TU WIEN Informatics

Setzen wir (nicht nur) unsere digitale Souveränität aufs Spiel?

Informationstechnische und rechtliche Aspekte eines Cloud-Betriebs kritischer Infrastruktur

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Software Engineering/Internet Computing

eingereicht von

David Eder, BSc
Matrikelnummer 01326201

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: Ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Wien, 18. März 2025

David Eder	Markus Haslinger

Technische Universität Wien
A-1040 Wien ▪ Karlsplatz 13 ▪ Tel. +43-1-58801-0 ▪ www.tuwien.at

TU WIEN Informatics

Is (not only) our digital sovereignty at stake?

IT and Legal Aspects of Cloud Services in Critical Infrastructures

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Software Engineering/Internet Computing

by

David Eder, BSc
Registration Number 01326201

to the Faculty of Informatics

at the TU Wien

Advisor: Ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Vienna, 18th March, 2025

David Eder | Markus Haslinger

Technische Universität Wien
A-1040 Wien ▪ Karlsplatz 13 ▪ Tel. +43-1-58801-0 ▪ www.tuwien.at

Erklärung zur Verfassung der Arbeit

David Eder, BSc

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.
Ich erkläre weiters, dass ich mich generativer KI-Tools lediglich als Hilfsmittel bedient habe und in der vorliegenden Arbeit mein gestalterischer Einfluss überwiegt. Im Anhang „Übersicht verwendeter Hilfsmittel“ habe ich alle generativen KI-Tools gelistet, die verwendet wurden, und angegeben, wo und wie sie verwendet wurden. Für Textpassagen, die ohne substantielle Änderungen übernommen wurden, haben ich jeweils die von mir formulierten Eingaben (Prompts) und die verwendete IT- Anwendung mit ihrem Produktnamen und Versionsnummer/Datum angegeben.

Wien, 18. März 2025

David Eder

Danksagung

Eine besondere Anerkennung gilt,

den Expert:innen, die sich für ein Interview bereit erklärt haben und ohne deren wertvollen Beitrag, der breite Praxiseinblick nicht möglich gewesen wäre,

meinem Betreuer für die Unterstützung bei der Umsetzung und die hilfreichen Hinweise im Laufe der Entwicklung dieser Arbeit,

meiner lieben Frau für den mentalen Rückhalt, das Korrektorat und die konstruktiven Gespräche zum Thema

und zu guter Letzt meiner gesamten Familie, die mir meine Ausbildung ermöglicht hat.

Danke!

Acknowledgements

Special recognition goes to,

the experts who agreed to be interviewed and without whose valuable contribution, the broad practical insight would not have been possible,

my supervisor for his support and helpful advice during the development of this thesis,

my dear wife for her mental support, proofreading and constructive discussions on the subject

and last but not least my entire family, who made my education possible.

Thank you!

Kurzfassung

Ziel dieser Thesis war die Beantwortung der Forschungsfrage, wie Betreiber der kritischen Infrastruktur Cloud-Dienste für Kernkomponenten ihrer Tätigkeiten einsetzen können und welche Risiken, aber auch Vorteile damit einhergehen. Der Fokus wurde dabei auf Österreich gerichtet.

Dabei wurde tiefgehend die aktuelle und zukünftige rechtliche Situation – insbesondere Entwicklungen innerhalb der EU – analysiert. Es wurden Unterstützungsangebote zur Compliance der marktdominierenden Public Cloud-Anbietern verglichen und wie diese mit rechtlichen Anforderungen kompatibel sein könnten. Um die aktuelle Cyber-Sicherheitslage zu beurteilen, fand eine Auswertung der medialen Berichterstattung über Sicherheitsvorfälle bei österreichischer kritischer Infrastruktur sowie bei großen internationalen Public Cloud-Dienstanbietern statt. Zur Erhebung des Status-Quo bei kritischer Infrastruktur in Österreich, kamen Interviews mit Expert:innen zum Einsatz.

Dabei wurden Probleme bei der sehr heterogenen europäischen Rechtslage mit unklaren und in der Praxis für Betreiber schwer umsetzbaren Anforderungen identifiziert. Gleichzeitig gibt es kaum Judikatur zu diesen ungeklärten Fragen, da manche Regulative noch nicht anwendbar sind. Ferner muss von einem Zugriff durch US-Behörden auf europäische Daten bei US-amerikanischen Cloud-Dienstleistern ausgegangen werden. Der Cloud-Betrieb kann die Aufsicht allerdings vereinfachen: Mit dem Einsatz eines Cloud-Dienstes durch mehrere beaufsichtigte Einrichtungen können sich Synergien ergeben, da mit der Überprüfung eines Cloud-Anbieters die Systeme aller relevanten Kund:innen gleich mitgeprüft werden können. Bei den Unterstützungsangeboten zur Compliance kündigen die Cloud-Dienstleister an, bei neuen rechtlichen Vorgaben unterstützen zu wollen. Bei der Adaption von Cloud-Lösungen herrscht bei der österreichischen kritischen Infrastruktur teilweise Zurückhaltung, was den Einsatz für Kernkomponenten angeht – mit Ausnahme des Finanzsektors.

Für Europa besteht die Gefahr, dass sich die massiv sinkende digitale Souveränität durch den Einsatz von Cloud-Diensten aus Drittstaaten auf andere Bereiche auswächst.

Abstract

The aim of this thesis was to answer the research question, how entities of the critical infrastructure can use cloud services for their core components and what advantages and risks this entails. The focus has been placed on Austria.

This involved in-depth analysis of the current and future legal situation, especially on developments taking place in the European Union. A comparison of the compliance offerings of the major public cloud service providers was performed, along with a validation of their compatibility with legal requirements. In order to assess the cybersecurity situation, an evaluation of media coverage regarding cybersecurity incidents in which Austrian critical infrastructure and public cloud providers were affected was carried out. To survey the status quo at Austrian critical infrastructure, interviews with experts in the fields took place.

Problems relating to the heterogeneous European legal framework with unclear requirements that are difficult for operators to implement in practice were identified. At the same time, there is hardly any case law on those unresolved issues, due to the fact, that many regulations are not applicable yet. Furthermore, access to European data by US authorities for US cloud providers must be assumed. However, cloud operations could simplify regulatory oversight, as the use of several operators can result in synergies: auditing the cloud provider could cover the systems of its customers as well. In respect to compliance offers, cloud providers announce support for their customers in regard to legal requirements. Austrian critical infrastructure is sometimes reluctant to adapt cloud solutions for their core components — except for the financial industry.

There is a risk for Europe that the massive decline in digital sovereignty going hand in hand with the usage of cloud services provided by third counties will spread to other areas as well.

Inhaltsverzeichnis

KAPITEL 1

Einführung

Über 77 % der großen Unternehmen in der EU nutzen mittlerweile Public Cloud-Dienste – Tendenz steigend[1] – gleichzeitig beträgt der Marktanteil europäischer Cloud-Dienstleister in Europa nur noch 13 %, mit einer stark sinkenden Tendenz[2]. Der Einsatz eines externen Cloud-Dienstleisters ist ein Spezialfall des Outsourcings, wobei ausschließlich Dienste der Informationstechnik (IT) betroffen sind. Somit geht eine Abgabe der Kontrolle der jeweiligen Einrichtung hin zum Cloud-Dienstleister mit den damit verbundenen Vor- und Nachteilen einher. Das Auslagerungsrisiko mag für klassische Unternehmen nur wirtschaftliche Aspekte treffen, für kritische Infrastruktur können im schlimmsten Fall Menschenleben oder das Funktionieren wichtiger gesellschaftlicher bzw. staatlicher Aufgaben auf dem Spiel stehen. Folglich hat die kritische Infrastruktur eine besonders große Verantwortung und Sorgfaltspflicht bei Auslagerungen an Dritte und damit auch an externe Cloud-Dienstleister. Damit einhergehend kommt es durch die Marktdominanz weniger großer US-amerikanischer Public Cloud-Anbieter zum Verlust der eigenen Souveränität im digitalen Umfeld. Dies kann sich durch die vermehrte Auslagerung von IT-Diensten der kritischen Infrastruktur, auf andere Bereiche auswachsen, bei denen wesentliche Aufgaben in eine informationstechnologische Abhängigkeit geführt wurden. Ein Staat kann dadurch Resilienz einbüßen und macht sich geopolitisch von Ländern abhängig, in denen seine IT-Dienstleister ihren Sitz haben.

Ein wichtiger Beweggrund für diese Arbeit waren persönliche Erfahrungen bzw. Beobachtungen im beruflichen Umfeld kritischer Infrastruktur. Die Frage nach dem Einsatz von Public Cloud-Diensten hat sich oft als eine schwierige erwiesen. Zuerst, ob derartige Auslagerungen überhaupt möglich sind und damit folgend – wenn ja – in welcher Form. Beim regen Austausch mit Kolleg:innen in anderen Branchen entstand der Eindruck, dass viele Einrichtungen vor ähnlichen Herausforderungen stehen und der persönliche Eindruck

[1] Statistisches Amt der Europäischen Union, *Enterprises buying cloud computing services by size class, EU, 2021 and 2023*.

[2] Synergy Research Group, *European Cloud Providers Continue to Grow but Still Lose Market Share*.

ein weit verbreitetes Phänomen betrifft – nicht nur in der kritischen Infrastruktur. So schrieb Hock Tan, Chief Executive Officer (CEO) von Broadcom, in einem Blogeintrag im August 2024 von den drei C der Public Cloud, mit denen viele Kund:innen zu kämpfen hätten: *„Cost, Complexity and Compliance“*[3].

Im Zuge einer Recherche in diversen wissenschaftlichen Arbeiten aus der rechtlichen und technischen Domäne, zeigte sich, dass besonders die neueren regulatorischen Entwicklungen für kritische Infrastruktur im Kontext Cloud-Computing noch nicht ausgiebig beleuchtet wurden. Eine Forschungslücke konnte bei einer Spezialisierung auf österreichische kritische Infrastruktur identifiziert werden. Ziel dieser Arbeit ist die Beantwortung der Forschungsfrage, in welcher Form Betreiber der kritischen Infrastruktur – mit besonderem Fokus auf Österreich – Cloud-Dienste für Kernkomponenten ihrer Tätigkeit nutzen können, was sie dabei beachten müssen und welches Wagnis sie damit eingehen. Das Endprodukt soll eine umfangreiche Entscheidungshilfe für „Cloud versus On-Premises“ im kritischen Infrastrukturbereich sein und Unterstützung beim Compliance-Management leisten.

Das Herzstück dieser Thesis ist die Analyse der rechtlichen Situation für Betreiber kritischer Infrastruktur in Hinblick auf Cloud-Computing und das Auffinden der Regulative, die für diese Problemstellung Relevanz haben. Jene rechtlichen Anforderungen umfassen zunächst internationale Abkommen, gefolgt von Regulatorik der EU hin zu nationalen Vorgaben in Österreich. Die Materie ist aktuell starkem Wandel unterworfen und noch nie wurden mehr Vorgaben in Hinblick auf Cybersicherheit ausgearbeitet wie in den letzten Jahren. Einen großen Teil der rechtlichen Analyse umfasst das Netz- und Informationssystemsicherheitsgesetz (NISG) bzw. die Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NISR) und deren Vergleich zur Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NISR2), wobei besonders die Unterschiede zwischen der älteren und neueren Richtlinie herausgearbeitet werden. Auch auf den Bericht des Rechnungshofes zur Koordination der Cyber–Sicherheit wird kurz eingegangen. Untersucht werden ferner die Vorgaben zur Resilienz aus der Richtlinie (EU) 2022/2557 über Resilienz kritischer Einrichtungen (CER), die für Produkthersteller relevante Verordnung (EU) über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (CRV) und Cybersicherheitszertifizierungen aus der Verordnung (EU) 2019/881 über die ENISA und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (CSA). Darüber hinaus werden sektorspezifische Vorgaben wie die Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA), die Leitlinien der Europäische Bankenaufsichtsbehörde (EBA) zu Auslagerungen, das österreichische Bundesgesetz über das Bankwesen (BWG) oder das Bundesgesetz über die Erbringung von Zahlungsdiensten 2018 (ZaDiG 2018) (im Zusammenhang mit der Richtlinie (EU) 2015/2366 über Zahlungsdienste im Binnenmarkt (PSD II)) analysiert. Abschließend

[3] Broadcom, *The Future of the Enterprise is Private.*

findet eine kritische Betrachtung der Datenzugriffe durch US-Behörden in der Europäische Union (EU) und deren Rechtsgrundlagen statt.

Unterstützend werden semistrukturierte qualitative Interviews mit Expert:innen, die mit oder im IT-Umfeld der kritischen Infrastruktur tätig sind, durchgeführt, um wertvolle Einblicke in die Praxis zu gewinnen. Dafür konnten IT-Berater:innen, Security Expert:innen und ein Teamleiter der sogenannten Computer-Notfallteams CERT Österreich gewonnen werden. Anhand einer Auswertung von Sicherheitsvorfällen bei kritischer Infrastruktur in Österreich und bei großen international tätigen Public Cloud-Anbietern, die im Zuge dieser Arbeit durchgeführt wird, soll die Bedrohungslage bewertet werden. Daraus ableitend wird eingeschätzt, wie wichtig IT-Sicherheit ist und ob entsprechende Vorgaben überhaupt notwendig sind, um ein hohes Sicherheitsniveau zu erreichen.

Daneben werden Compliance-Angebote, auch für regulatorische Vorgaben, zwischen den Public Cloud-Anbietern verglichen, um aufzuzeigen, welche für kritische Infrastruktur geeignet sein könnten und wie diese beim Cloud-Einsatz unterstützen können. Ferner werden die Verfügbarkeitsangebote verglichen und deren Tauglichkeit für kritische Infrastruktur untersucht. Anhand öffentlicher Informationen werden Datenzugriffe durch Behörden und deren potenzielle Auswirkungen beurteilt. Dabei wird auch auf das Problemfeld der digitalen Souveränität innerhalb der EU eingegangen und die weltweite Lage anhand von Marktstatistiken betrachtet.

Zu guter Letzt werden in den entsprechenden Kapiteln verschiedene Lösungsansätze für die ermittelten Probleme im Public Cloud-Computing gesucht. Von jenen Ansätzen stammen einige von Dienstleistern selbst, die offenbar ein Problemfeld erkannt haben, oder aber auch von Vertretern der Regierung, Wirtschaft oder Wissenschaft.

KAPITEL 2

Grundlagen des Cloud-Computing

Das amerikanische National Institute of Standards and Technology (NIST) definiert Cloud-Computing als Sammlung von Computing-Ressourcen, die bei Bedarf über Netzwerkdienste abrufbar, zwischen mehreren Kund:innen aufgeteilt und schnell provisionierbar bzw. wieder abbaubar sind[1]. Es können somit Dienste unterschiedlicher Benutzer:innen auf derselben Hardware ausgeführt werden. Inhaltlich orientieren sich auch europäische und österreichische Gesetzgeber weitgehend an dieser Begriffsbestimmung. Die Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NISR2) versteht unter Cloud-Computing:

> *„[. . .] einen digitalen Dienst, der auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind.“*[2]

Der Terminus Elastizität (bzw. elastischer Pool) beschreibt, dass benötigte Ressourcen je nach Bedarf automatisch angepasst werden[3]. Es können somit Lastspitzen bewältigt werden. Parallel kommt es in Zeiten geringen Bedarfs nicht zur Blockade ungenutzter Ressourcen. Ferner zeichnet sich Cloud-Computing durch Self-Service aus: Kund:innen können meist selbstständig und ohne Kontakt zu Administrator:innen oder Verkäufer:innen, Dienstleistungen bestellen und verwalten[4]. Üblicherweise kommt beim Cloud-Computing ein entsprechendes Quality of Service (QoS) zum Einsatz[5], das die Güte eines Service

[1] Mell und Grance, *The NIST definition of cloud computing*, S. 2.
[2] *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 6 Z 30.
[3] Mell und Grance, *The NIST definition of cloud computing*, S. 2.
[4] Ebd., S. 2.
[5] Wang u. a., „Cloud computing: a perspective study“, S. 141.

darstellt. Darin wird ein Leistungsniveau vereinbart, das mittels Service Level Agreement (SLA) durchgesetzt werden kann[6].

Nicht zu verwechseln ist Cloud-Computing mit dem sogenannten Grid-Computing, bei dem Ressourcen über mehrere Organisationen hinweg geteilt und zusammengefasst werden – meist mit dem Ziel, Computing Kapazitäten zu maximieren, also möglichst große Rechenleistung zu erreichen[7]. Anwendungsgebiete sind häufig wissenschaftlicher Natur und seltener im gewinnorientierten Umfeld[8]. Eine Erweiterung des Cloud-Computings ist Fog-Computing (siehe Abbildung 2.1), das sich ebenso der meteorologischen Analogie bedient. Dabei befinden sich die Computing-Komponenten zwischen den Cloud-Dienstanbietern und den Endgeräten. Wenn die Datenverarbeitung an der Datenquelle oder in direkter Nähe stattfindet (z. B. bei IoT Geräten), wird von Edge-Computing gesprochen[9]. Durch den Einsatz dieser Konzepte kann unter anderem die Latenz gering gehalten werden, Dezentralisierung erreicht werden und Echtzeitkommunikation stattfinden[10].

Als eines der ersten Unternehmen begann Salesforce in den 1990er-Jahren ein Customer Relationship Management (CRM) System als Software-as-a-Service (SaaS) anzubieten[11]. Im Jahr 2006 startete Amazon die EC2 und war damit Pionier im Bereich Infrastructure-as-a-Service (IaaS)[12]. 2010 kam Microsoft Azure auf den Markt und 2012 Googles Compute Engine[13]. Mittlerweile haben mit Stand 2023 laut Eurostat 45,2 % (mit einem Anstieg von 4,2 Prozentpunkten im Vergleich zu 2021) aller Unternehmen in der EU Cloud-Dienste erwerben, wobei der Großteil für E-Mail, Datenspeicherung und Büroanwendungen eingesetzt wurde[14]. Von diesen Unternehmen nutzten wiederum 75,3 % fortgeschrittene („sophisticated“) Cloud-Dienste, wie Sicherheitsanwendungen, Unternehmensdatenbanken oder Plattformen zur Softwareentwicklung[15]. Für einen Vergleich siehe Abbildung 2.3. Generell nimmt in der EU die Verbreitung von Cloud-Diensten mit der Größe der Unternehmen zu[16] – siehe Abbildung 2.2.

[6] Wang u. a., „Cloud computing: a perspective study“, S. 141.
[7] Dillon, Wu und Chang, „Cloud computing: issues and challenges“, S. 29–30.
[8] Ebd., S. 29–30.
[9] Sabireen und Neelanarayanan, „A review on fog computing: Architecture, fog with IoT, algorithms and research challenges“, S. 163–164.
[10] Ebd., S. 163–164.
[11] Surbiryala und Rong, „Cloud computing: History and overview“, S. 2.
[12] Ebd., S. 2.
[13] Ebd., S. 2.
[14] Statistisches Amt der Europäischen Union, *Cloud computing - statistics on the use by enterprises.*
[15] Ebd.
[16] Ebd.

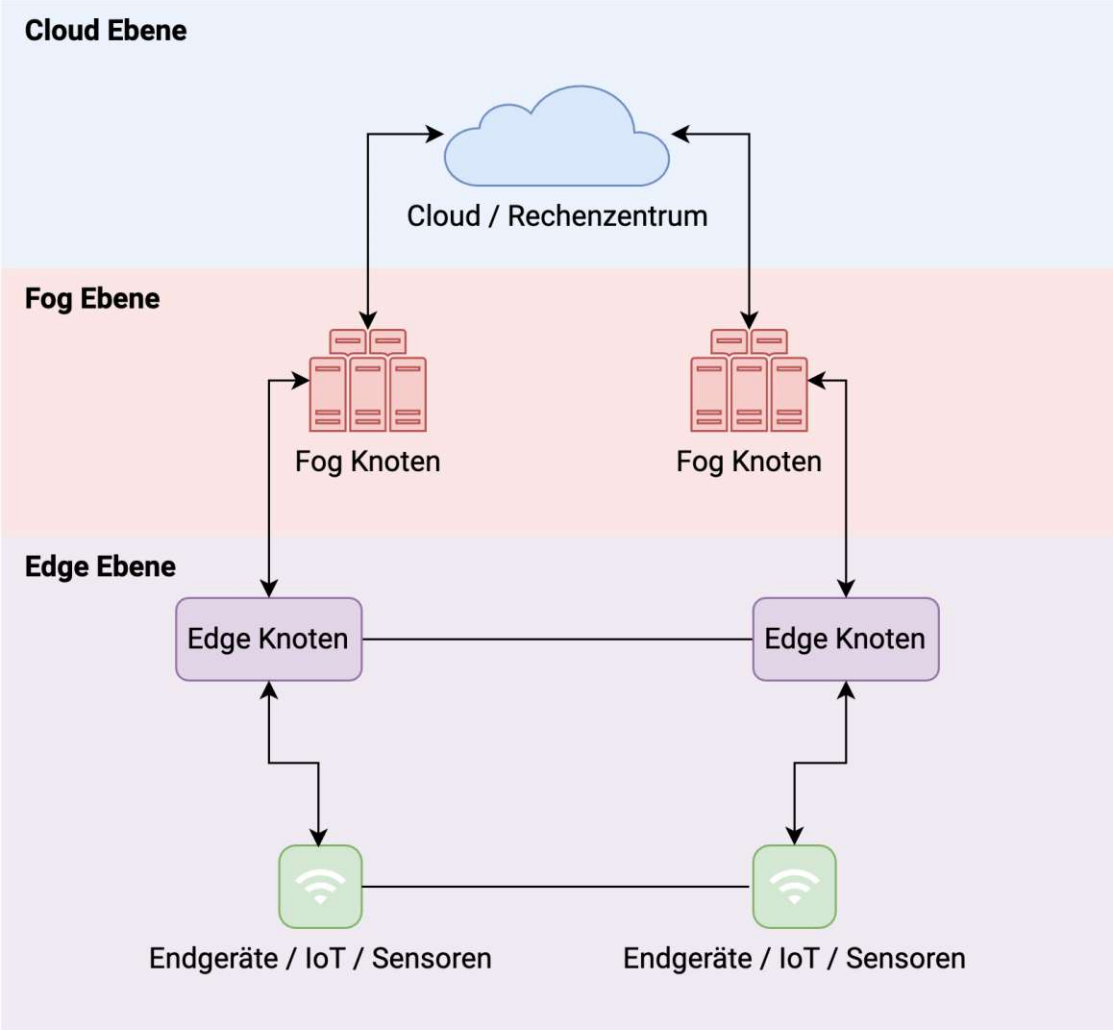

Abbildung 2.1: Fog-, Edge- und Cloud-Computing (basierend auf Sabireen und Neelanarayanan, „A review on fog computing: Architecture, fog with IoT, algorithms and research challenges“ IONOS, *Fog-Computing – Dezentraler Ansatz für IOT-Clouds*)

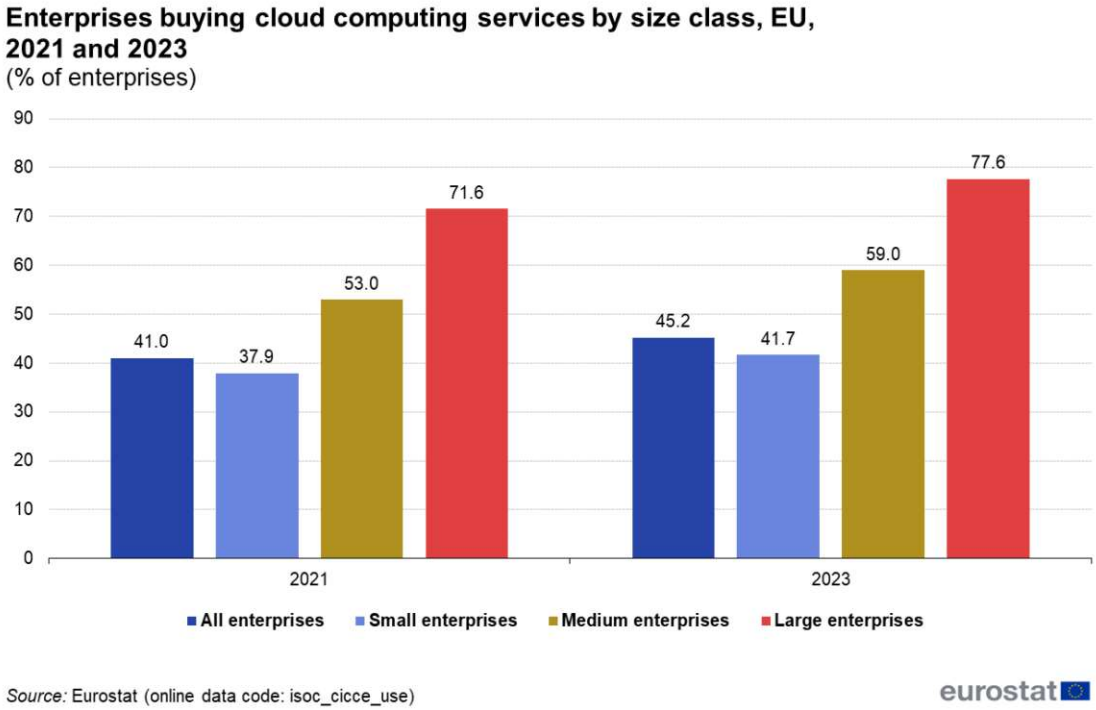

Abbildung 2.2: EU-Unternehmen, die Cloud-Dienste nutzen, nach Größe kategorisiert (Quelle: Statistisches Amt der Europäischen Union, *Enterprises buying cloud computing services by size class, EU, 2021 and 2023*)

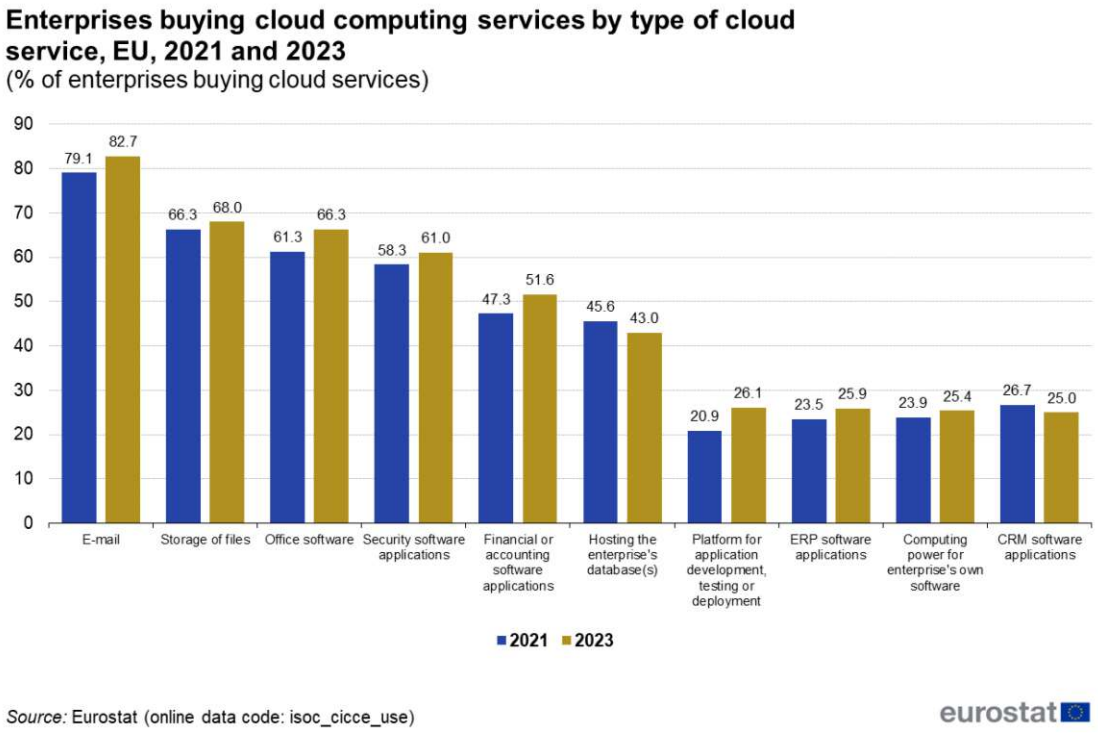

Abbildung 2.3: Einsatzarten von Cloud-Diensten bei EU-Unternehmen (Quelle: Statistisches Amt der Europäischen Union, *Enterprises buying cloud computing services by type of cloud service, EU, 2021 and 2023*)

2.1 Vorteile

Die doch recht großflächige Verbreitung von Cloud-Computing in den vergangenen Jahren beruht auf einigen Vorteilen gegenüber On-Premises-Installationen, die am häufigsten in einschlägiger Literatur genannten sind im Folgenden beschrieben:

- **Kosteneinsparungen:** Üblicherweise wird beim Cloud-Computing nur für tatsächlich genutzte Ressourcen bezahlt[17] und folgt dies dem Prinzip Pay as you go (PAYG). Damit können sich umfangreiche Kosteneinsparungen ergeben, da Hardware auch bei geringer Last insbesondere Strom verbraucht und abzuführende Wärme erzeugt. Ferner gibt es keine Anschaffungskosten für Hardware und keinen Wartungsaufwand[18]. Daher haben besonders Organisationen, die noch kein Rechenzentrum oder entsprechende Infrastruktur betreiben, eine Kostensenkung bei den Vorlaufkosten.

- **Skalierbarkeit:** Cloud-Umgebungen können automatisch oder mit wenig Aufwand von kleinen Deployments mit wenig Ressourcen zu vielen hunderten Servern umgestellt werden[19]. Passiert diese Skalierung in einem verteilten und großen Ausmaß, spricht man auch von Hyperscaling[20].

- **Agilität:** Für viele Unternehmen ist es wirtschaftlich unbedingt notwendig, kurzfristig auf Änderungen am Markt zu reagieren[21]. Mit dem Einsatz von Cloud-Computing können Prozesse, Produkte und Services schneller angepasst werden, als bei On-Premises-Infrastruktur[22]. Der Fokus kann auf Kernaufgaben gelegt werden, während keine Ressourcen in Verwaltung und Administration von Hardware und Software fließen müssen[23]. Gleichzeitig kümmert sich üblicherweise der Cloud-Provider um zumindest einen Teil der Software-Updates und Patches.

- **Resilienz:** Um in außergewöhnlichen Notsituationen (z. B. Überschwemmungen, Erdbeben, kriegerische Auseinandersetzungen, Stromausfälle usw.) Disaster Recovery betreiben zu können, müssen Server über zumindest zwei Standorte verteilt sein. Microsoft versucht etwa eine Entfernung von mindestens 300 Meilen (ca. 483 Kilometer) zwischen Rechenzentrumsregionen zu erreichen[24].

- **Umweltschutz:** Strom- und Kühlbedarf beim Betrieb von Rechenzentren ist teuer – besonders bei nicht optimaler Umsetzung. Cloud-Betreiber schaffen es

[17] Saini, Upadhyaya und Khandelwal, „Benefits of cloud computing for business enterprises: A review“, S. 1005–1006.
[18] Ebd., S. 1005–1006.
[19] Ebd., S. 1005–1006.
[20] Ebd., S. 1005–1006.
[21] Shayan u. a., „Identifying Benefits and risks associated with utilizing cloud computing“, S. 4–6.
[22] Ebd., S. 4–6.
[23] Ebd., S. 4–6.
[24] Microsoft, *Cross-region replication in Azure*.

meist beides kostengünstiger zu realisieren als On-Premises-Installationen[25]. Des Weiteren kommt es beim Betrieb eigener Hardware häufiger zu Leerläufen oder weniger Auslastung im Vergleich zu Cloud-Lösungen[26]. Die damit einhergehenden Einsparungen sind nicht nur ökonomischer, sondern leisten auch einen Beitrag zum Umweltschutz[27].

2.2 Risiken und Nachteile

Neben **Informationssicherheit** (siehe Abschnitt 2.6) und **rechtlichen Aspekten** (siehe Kapitel 4) birgt der Cloud-Betrieb weitere Risiken und Nachteile, die im Folgenden beschrieben werden:

- **Integration:** Die Integration von bestehenden Daten oder Systemen in Cloud-Umgebungen kann aufwendig sein, insbesondere wenn proprietäre Protokolle und Schnittstellen zum Einsatz kommen[28]. In einer Umfrage unter IT-Expert:innen, durchgeführt von Netwrix, gaben 41 % der Befragten an, dass die Integration sie beim Wechsel in Cloud-Dienste bremst[29].
- **Lock-in-Effekt:** Für Kund:innen besteht die Gefahr der Abhängigkeit von der Implementierung eines einzelnen Cloud-Anbieters (häufig auch Vendor Lock-in genannt). Ein Wechsel ist oft nicht ohne Kosten, technische Schwierigkeiten oder rechtliche Einschränkungen möglich[30]. Dieser Aufwand wird häufig von Cloud-Kund:innen unterschätzt oder findet im Vorhinein gar keine Betrachtung[31].
- **Kompetenz und Wissensverlust:** Mit dem Einsatz von Cloud-Computing beschäftigen sich Mitarbeiter:innen gelegentlich nicht mehr mit bestimmten – aber für On-Premises essenziellen – Technologien, da sie vor Ort nicht zur Anwendung kommen (z. B. Hardware, Netzwerk, Stromversorgung oder Klimasteuerung). Damit kann ein Kompetenz- oder Wissensverlust einhergehen[32], der in weiterer Folge die betroffenen Kund:innen stärker an externe Dienstleister bindet.
- **Multi Cloud:** Im Anwendungsgebiet von Multi Clouds (siehe Abschnitt 2.4) liegen die Problemstellungen darin, entsprechende Fähigkeiten als Unternehmen zu haben, um Umgebungen über mehrere Anbieter verteilt zu betreiben, bei gleichzeitigem Verständnis, wie die Lösungen zusammenarbeiten[33].

[25] Shayan u. a., „Identifying Benefits and risks associated with utilizing cloud computing“, S. 4–6.
[26] Ebd., S. 4–6.
[27] Ebd., S. 4–6.
[28] Dillon, Wu und Chang, „Cloud computing: issues and challenges“, S. 31.
[29] Netwrix, *Cloud Data Security Report*, S. 8.
[30] Opara-Martins, Sahandi und Tian, „Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective“, S. 2–3.
[31] Ebd., S. 9.
[32] Omar u. a., „An examination of the factors affecting the adoption of cloud enterprise resource planning systems in Egyptian companies“, S. 20.
[33] Check Point Software Technologies Ltd., *Cloud Security Report*, S. 6.

2.3 Verfügbarkeit und Hochverfügbarkeit

Um Ausfälle bei Cloud-Anbietern zu messen und auch vertraglich abzusichern (mit dem Einsatz von SLAs), etablierte sich der Begriff Verfügbarkeit. Diese ist üblicherweise einer der wichtigsten Parameter der Preisbildung. Grundsätzlich gibt es unterschiedliche Definitionen von Verfügbarkeit, häufig anzutreffen ist jedoch die folgende:

> *„[...] the degree to which a system is functioning and is accessible to deliver it's services during a given time interval.“*[34]

Zur Berechnung kann folgende Formel verwendet werden, wobei manche Anbieter andere Berechnungsmethoden verwenden:

$$A = MTTF/(MTTF + MTTR) \tag{2.1[35]}$$

Dabei bezeichnet A die Verfügbarkeit (engl. „availability“), MTTF die mittlere Betriebsdauer (engl. „mean time to failure“) und MTTR die mittlere Reparaturdauer (engl. „mean time to repair“)[36].

Daneben existiert der Terminus Hochverfügbarkeit, der einem System eine Verfügbarkeit von 99,999 % (entspricht einer gesamten Ausfalldauer von fünf Minuten und 15 Sekunden pro Jahr) abverlangt[37]. Erreicht wird dieses Ziel üblicherweise durch Redundanzen, Fault Tolerance oder Load Balancing bzw. Autoscaling[38].

Bei den Servicemodellen IaaS und PaaS gilt das Erreichen einer höheren Verfügbarkeit als einfacher, im Vergleich zu zustandsbasierten Applikationen. Ein Problem dabei ist das Erkennen von Fehlern[39]. Meist werden nur rudimentäre Monitoring-Aufgaben, wie Ping auf Hosts oder IP-Adressen, durchgeführt[40]. Für einen Vergleich zwischen Cloud-Anbietern in Bezug auf Verfügbarkeit siehe Kapitel 6.

2.4 Cloud-Liefermodelle

Aufgrund unterschiedlicher Anforderungen haben sich Typen von Liefermodellen am Cloud-Markt etabliert, wobei eine genaue Definition nicht immer möglich ist. Die Grenzen zwischen einzelnen Liefermodellen sind fließend und werden diese Modelle in unterschiedlichen Variationen eingesetzt. Die bekanntesten Vertreter sind im Folgenden beschrieben:

[34] Toeroe und Tam, *Service availability: principles and practice*, S. 36–40.
[35] Ebd., S. 36–40.
[36] Ebd., S. 36–40.
[37] Ebd., S. 36–40.
[38] Nabi, Toeroe und Khendek, „Availability in the cloud: State of the art“, S. 61.
[39] Ebd., S. 63.
[40] Ebd., S. 63.

- **Public Cloud:** Die Public Cloud ist für die breite Öffentlichkeit nutzbar und kann von jedem in Anspruch genommen werden. Die notwendige Hardware befindet sich beim Dienstanbieter[41]. Häufig ist die Region des Serverstandorts frei wählbar, aufgrund von (meistens gesetzlichen) Anforderungen mancher Kund:innen. Bekannte Public Cloud-Vertreter sind beispielsweise Google Cloud Platform (GCP), Amazon Web Services (AWS) und Microsoft Azure (Azure).

- **Private Cloud:** Private Clouds werden ausschließlich für eine einzelne Organisation zur Verfügung gestellt, wobei es intern unterschiedliche Nutzer:innen gibt (z. B. Abteilungen oder Business Units)[42]. Der Standort und die Verwaltung kann sowohl intern als auch extern sein: es gibt damit On-Premises und Off-Premises Private Clouds[43].

- **Community Cloud:** Community Clouds sind nur für eine bestimmte Benutzer:innengruppe nutzbar, die gemeinsame Interessen oder Anforderungen haben[44]. Als Beispiel kommen Banken infrage, die sich aufgrund derselben rechtlichen Vorgaben beim Betrieb der IT-Infrastruktur zusammenschließen.

- **Multi Cloud:** Bei Multi Clouds werden mehrere Cloud-Anbieter, üblicherweise desselben Liefermodells, genutzt, um so Redundanzen herzustellen[45].

- **Poly Cloud:** Poly Cloud beschreibt den Einsatz unterschiedlicher Anbieter für einzelne Applikationen oder Services[46]. Damit wird versucht, die Stärken der Provider gezielt zu nutzen[47].

- **Government Cloud:** Der Begriff wird meistens als ein Cloudservice beschrieben, das sich an staatliche Organisationen richtet. Vertreter sind unter anderem Microsofts Office 365 GCC, Office 365 GCC High und DoD (Department of Defense), womit das Unternehmen die Department of Defense Cloud-Computing Security Requirements Guide (SRG) erfüllt[48].

- **Hybrid Cloud:** Hybrid Clouds sind Kombinationen aus unterschiedlichen Liefermodellen, im Gegensatz zu Poly Clouds, wo nur Cloud-Dienste desselben Liefermodells genutzt werden.

[41] Mell und Grance, *The NIST definition of cloud computing*, S. 3.
[42] Ebd., S. 3.
[43] Ebd., S. 3.
[44] Ebd., S. 3.
[45] Petcu, „Multi-cloud: expectations and current approaches“.
[46] Panteli, *Examining Poly-Cloud in Enterprise Cloud Strategies: Differentiating Between Multi-Cloud and Hybrid Cloud Approaches*.
[47] Ebd.
[48] Microsoft, *Office 365 GCC - Service Descriptions — learn.microsoft.com*.

2.5 Cloud-Servicemodell

Je nach Bedarf können Kund:innen beim Kauf von Cloud-Diensten wählen, wie viel Kontrolle sie auslagern möchten. Dabei hat sich die Schreibweise *XaaS (X as a Service)* – wobei *X* für das entsprechende Service steht – etabliert. Das amerikanische National Institute of Standards and Technology (NIST) definiert drei Servicemodelle für Cloud-Dienste:

- **Infrastructure-as-a-Service (IaaS):** Hier beziehen die Kund:innen ausschließlich Computerressourcen und installieren darauf Betriebssysteme und Applikationen[49]. Damit besteht in diesem Servicemodell weitreichende Kontrolle über das System, abgesehen von der darunterliegenden Hardware (siehe Abbildung 2.5, zweite Spalte)[50].
- **Platform-as-a-Service (PaaS):** Im Gegensatz zu IaaS installieren Kund:innen eine beliebige Applikation basierend auf dem Betriebssystem, das der Cloud-Anbieter bereitstellt und haben volle Kontrolle über Applikation, Middleware und Zugriffskontrolle (siehe Abbildung 2.5, dritte Spalte)[51]. Die Konfigurationsmöglichkeiten am Betriebssystem sind jedoch stark eingeschränkt.
- **Software-as-a-Service (SaaS):** Bei SaaS wird den Nutzer:innen direkt eine Applikation des Cloud-Anbieters zur Verfügung gestellt, ohne Kontrollmöglichkeiten, mit Ausnahme der Zugriffskontrolle (siehe Abbildung 2.5, vierte Spalte)[52]. Bekannte Vertreter sind E-Mail, CRM oder Office-Produkte.

[49] Mell und Grance, *The NIST definition of cloud computing*, S. 3.
[50] Ebd., S. 3.
[51] Ebd., S. 2.
[52] Ebd., S. 2.

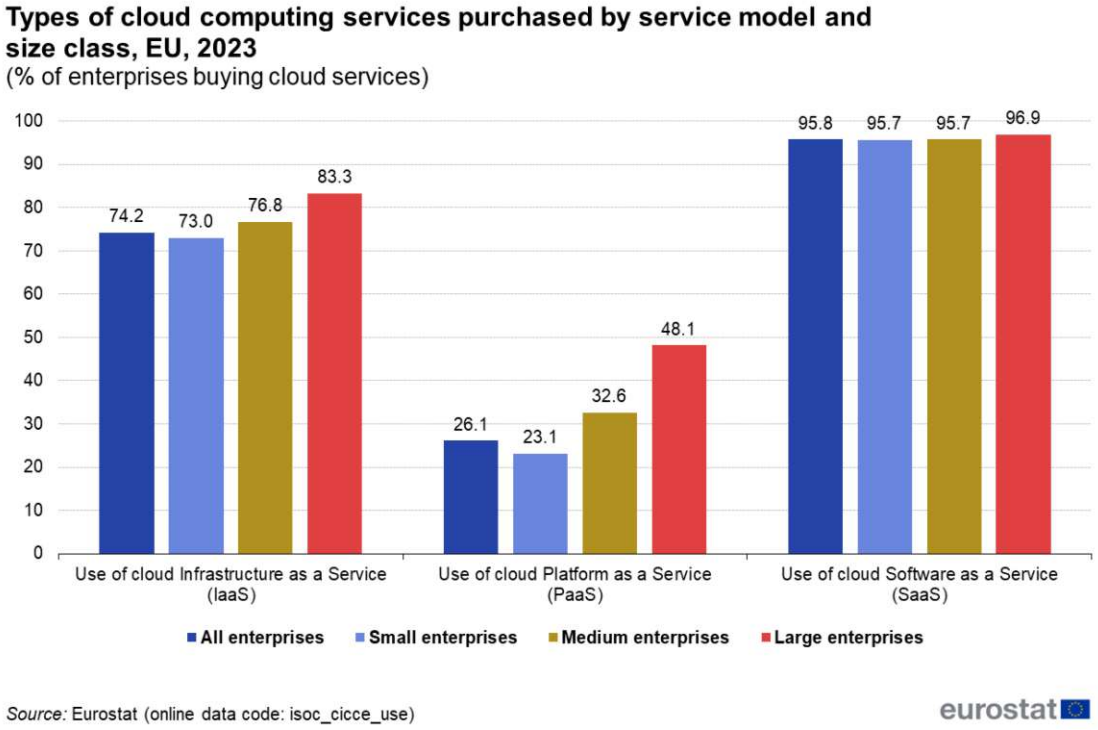

Abbildung 2.4: Einsatz der Servicemodelle in Unternehmen der EU (Quelle: Statistisches Amt der Europäischen Union, *Types of cloud computing services purchased by service model and size class, EU, 2023*)

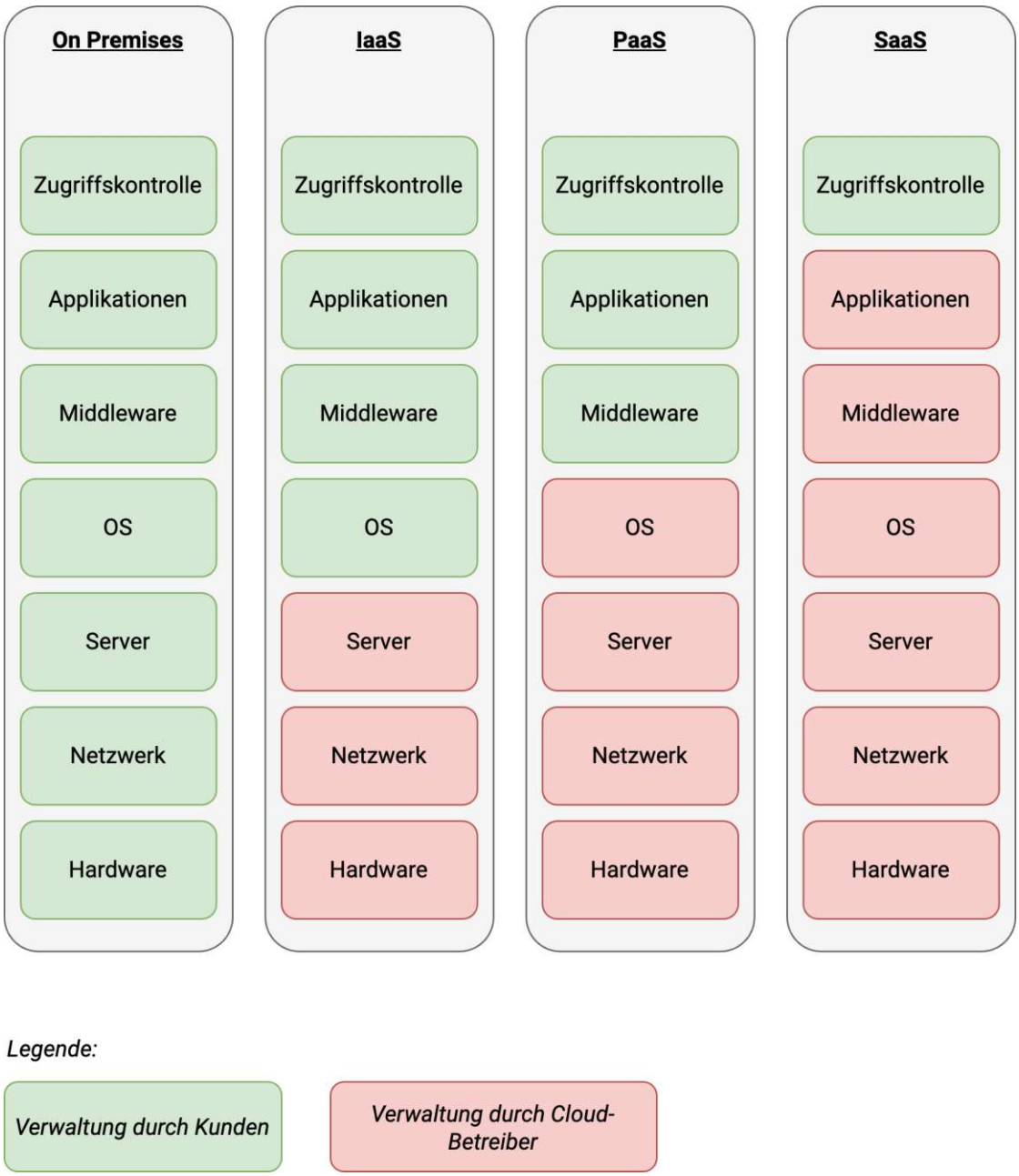

Abbildung 2.5: Kontrolle der Kund:innen in Servicemodellen (basierend auf Freet u. a., „Cloud forensics challenges from a service model standpoint: IaaS, PaaS and SaaS“ und Microsoft, *Get started guide for Azure IT operators — learn.microsoft.com*)

Nach einer Erhebung der Eurostat nutzten über 95,7 % aller Unternehmen in der EU, die Cloud-Services erworben haben, SaaS und je nach Unternehmensgröße zwischen 73 % und 83,3 % IaaS[53] (siehe Abbildung 2.4). Am wenigsten Anwendung findet PaaS mit 26,1 % (kleine Unternehmen) bis 48,1 % (große Unternehmen)[54].

Im Laufe der Zeit etablierten sich weitere Modelle, die häufig Mischformen oder Spezialisierungen der bereits vorgestellten Modelle sind. Eine Auswahl der mittlerweile bekanntesten Vertreter findet sich im Folgenden:

- **Function-as-a-Service (FaaS):** Hier wird von Kund:innen ausschließlich Code bereitgestellt, der auf einer Cloud-Plattform ausgeführt wird, ohne Zugriff oder Kenntnis darunterliegender Abstraktionsschichten[55]. Ein besonderes Merkmal ist dabei die Granularität: Die Ausführung findet nur in kleinen Teilen von Code statt[56]. Programmzustände werden nach Funktionsaufrufen wieder verworfen und können nicht von anderen Aufrufen weiterverwendet werden[57]. FaaS ist üblicherweise ereignisbasiert und benötigt einen Auslöser, um zur Ausführung zu gelangen[58].
- **Container-as-a-Service (CaaS):** Als Container wird ein selbstständig lauffähiges Softwarepaket beschrieben, das Code, Laufzeitumgebung, Bibliotheken und notwendige Abhängigkeiten bereits enthält[59]. Es ist damit plattformunabhängig und kann in jeder Container-lauffähigen Umgebung ausgeführt werden, die von Cloud-Dienstleitern angeboten werden. Bekannte Vertreter sind Google Container Engine und Amazon EC2 Container Service (ECS). Daneben kommen Tools zur Verwaltung von Containern zum Einsatz, wie Kubernetes, OpenShift oder Docker Swarm.
- **Database-as-a-Service (DBaaS):** Bei DBaaS werden unterschiedlichste Datenbanktechnologien zur Verfügung gestellt, beispielsweise relationale Datenbanken, wie Structured Query Language (SQL), nicht relationale Datenbanken (NoSQL) oder New SQL. Es gibt allerdings auch speziell für Cloud entwickelte Technologien wie Amazon RDS, Azure SQL Database und Google Cloud SQL.
- **Storage-as-a-Service (STaaS):** Üblicherweise wird bei STaaS Block- (meist für Applikationen und Datenbanken), Datei- oder Objektspeicherung (unstrukturierte Daten) bereitgestellt[60]. Häufig werden dabei auch Backup-Lösungen angeboten (Backup as a Service).

[53] Statistisches Amt der Europäischen Union, *Cloud computing - statistics on the use by enterprises.*
[54] Ebd.
[55] Shahrad, Balkind und Wentzlaff, „Architectural implications of function-as-a-service computing“, S. 1064.
[56] Ebd., S. 1064.
[57] Ebd., S. 1063.
[58] Ebd., S. 1063.
[59] Hussein, Mousa und Alqarni, „A placement architecture for a container as a service (CaaS) in a cloud environment“, S. 1.
[60] Kulkarni, Sutar und Gambhir, „Cloud computing-Storage as service“, S. 945.

- **Artifical-Intelligence-as-a-Service (AIaaS):** Künstliche Intelligenz (KI) Services, die von externen Anbietern zur Verfügung gestellt werden und bei denen Kund:innen keine eigene KI-Umgebung benötigen, werden als AIaaS bezeichnet[61].

2.6 Informationssicherheit

Bei der Informationssicherheit gilt es üblicherweise, die CIA Triade – also Confidentiality (Vertraulichkeit), Integrity (Integrität) und Availability (Verfügbarkeit) – sicherzustellen (siehe Abbildung 2.6). Vertraulichkeit beschreibt die Eigenschaft, dass Informationen nur für bestimmte Nutzer:innen zugänglich sind[62]. Integrität besagt, dass Informationen vertrauenswürdig und unverändert sind[63]. Verfügbarkeit ist die Garantie von verlässlich funktionierendem Zugriff auf Informationen[64].

In den vergangenen Jahrzehnten gab es immer wieder Bestrebungen, die CIA Triade zu erweitern. Eine dieser Erweiterungen ist Non-Repudiation: dabei können Teilnehmer:innen einer Kommunikation nicht abstreiten, dass dieselbige stattgefunden hat[65]. Daneben gibt es noch Authentizität (diese wird auch in der NISR2 verwendet – siehe Abschnitt 4.2), womit sichergestellt ist, dass eine behauptete Identität gültig und wahr ist[66]. Ein Beispiel dafür sind Zertifikate in Webanwendungen, die von Browsern automatisch überprüft werden, um sicherzustellen, dass der Server hinter dem DNS-Eintrag wirklich der behauptete Server ist.

2.6.1 Sicherheitsrisiken

In der Praxis ergeben sich konkrete Gefahren bzw. Angriffsvektoren, die die zuvor vorgestellten Eigenschaften (CIA Triade) und damit die Informationssicherheit von Systemen selbst bedrohen. In einschlägiger Literatur finden sich folgende bekannte Probleme, die anhand gleich gestalteter Angriffsmuster zusammengefasst werden können und auf Cloud-Dienste zutreffen (eine Zuordnung zur CIA Triade siehe Tabelle 2.1):

- **Fehlkonfiguration und unpassende Änderungskontrollen:** Falsche oder nicht optimale Einstellungen in Cloud-Computing Komponenten können diese anfällig für böswillige Aktivitäten oder unbeabsichtigte Schäden machen[67].
- **Identity and Access Management (IAM):** IAM ist eigentlich ein Feature der Cloud, aber aufgrund der Komplexität des Identitäts- und Zugriffsmanagements und

[61] Security Insider, *Was ist AI-as-a-Service (AIaaS)?*
[62] Tchernykh u. a., „Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability“, S. 4.
[63] Ebd., S. 4.
[64] Ebd., S. 4.
[65] Samonas und Coss, „The CIA strikes back: Redefining confidentiality, integrity and availability in security.“, S. 34.
[66] Ebd., S. 34.
[67] Cloud Security Alliance, *Top Threats to Cloud Computing 2024*, S. 9.

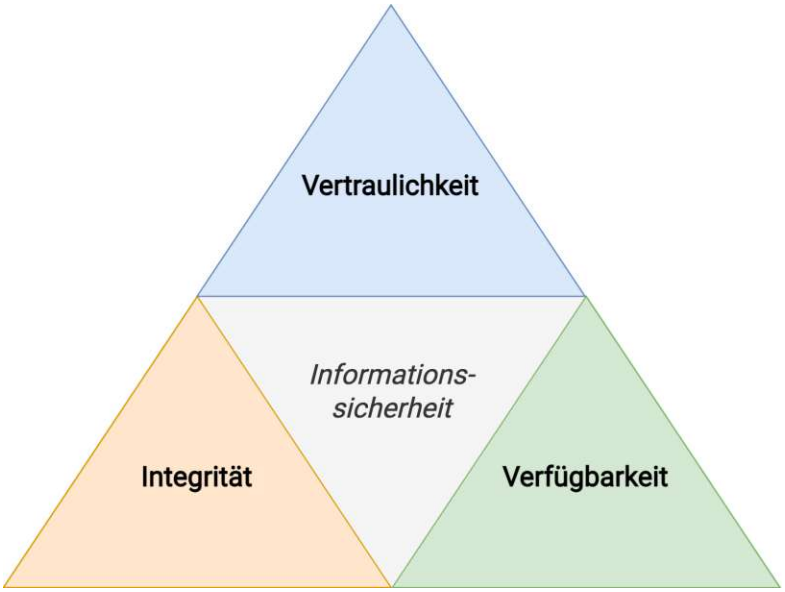

Abbildung 2.6: CIA Triade (basierend auf Samonas und Coss, „The CIA strikes back: Redefining confidentiality, integrity and availability in security.“)

fehlerhafter Implementierungen, Konfigurationen, Updates oder Überwachungen können neue Sicherheitslücken entstehen[68].

- **Phishing und Social Engineering:** Angreifer:innen versuchen durch verfälschte E-Mails, Webseiten oder Anrufen an Informationen (z. B. geheime Zugangsdaten) ihrer Opfer zu gelangen[69]. Die erbeutete Information wird dann missbräuchlich eingesetzt[70].
- **Böswilliger Insider:** Durch intransparente Einstellungsprozesse und Berechtigungsmaßnahmen von Cloud-Anbietern können Mitarbeiter:innen missbräuchlich mit Kundensystemen umgehen[71].
- **Virtualisierung und geteilte Ressourcen:** Mit dem Einsatz von Virtualisierungstechnologien teilen sich mehrere Kund:innen auf einem Hypervisor dieselbe Hardware. Dadurch gibt es die Gefahr, dass andere Kund:innen unerlaubten Zugriff auf fremde Daten bekommen, die im selben System oder auf derselben Hardware liegen[72].
- **Datenverlust:** Bei unzureichenden/fehlerhaften Disaster Recovery Verfahren im Rechenzentrum oder bei Fehlkonfigurationen bzw. -bedienungen, können Nut-

[68] Ebd., S. 14.
[69] Butt u. a., „Cloud security threats and solutions: A survey“, S. 399.
[70] Ebd., S. 399.
[71] Singh und Chatterjee, „Cloud security issues and challenges: A survey“, S. 96.
[72] Ebd., S. 97.

zer:innen Datenverlust erfahren[73]. Dazu kommen Ransomware-Angriffe, die Daten verschlüsseln und unbrauchbar machen können[74]. Derartige Attacken sind oft als Erpressungsversuch ausgestaltet, bei dem der Schlüssel zum Entschlüsseln der Daten erst nach einer Lösegeldzahlung übergeben wird.

- **Identitätsdiebstahl:** Beim Identitätsdiebstahl wird versucht, sich selbst für wahre Kund:innen auszugeben, um damit deren Ressourcen zu übernehmen[75].
- **Denial-of-Service (DOS):** Durch massenhaftes Versenden von Internetpaketen soll das Zielsystem überlastet und außer Betrieb gebracht werden. Damit kann sowohl dem Cloud-Dienst-Vertragsnehmer:innen als auch dessen Nutzer:innen der Zugang zum System verwehrt werden. Eine Erweiterung ist das sogenannte Distributed Denial-of-Service (DDOS), wobei eine große Anzahl unterschiedlicher und koordinierter Quellen für den Angriff genutzt wird[76].
- **Eingeschränkte Überwachung bzw. Sichtbarkeit:** Eingeschränkte Sichtbarkeit tritt auf, wenn Nutzer:innen nicht mehr effektiv analysieren und visualisieren können, ob ein Dienst sicher oder böswillig ist[77].
- **Supply Chain Attack:** (Software) Supply Chain Attacken versuchen Schadcode in ein Softwareprodukt einzuschleusen und Endnutzer:innen beziehen im Anschluss das manipulierte Produkt durch vertrauenswürdige Quellen[78]. Folglich kann derartiger Schadcode auch den Weg in eine Cloud-Umgebungen finden und eine Vielzahl von Kund:innen gleichzeitig betreffen.

Eine Gegenüberstellung von konkreten Sicherheitsvorfällen bei kritischer Infrastruktur und Cloud-Anbietern im Hinblick auf die vorgestellten Gefahren bzw. Angriffsvektoren findet sich in Kapitel 7 dieser Arbeit.

2.6.2 Sicherheitskonzepte

Um die Bedrohungsszenarien der Cloud zu bewältigen, entwickelten sich Sicherheitskonzepte für Betreiber und Nutzer:innen, die teils auch in anderen Domänen Anwendung finden[79]. Manche werden auch von rechtlichen Vorschriften für Betreiber wesentlicher Dienste gefordert (siehe Kapitel 4).

Das **Identity and Access Management (IAM)** soll die Identitäten der Dienst-Aufrufenden sicherstellen – dafür werden Passwörter, Multifaktor-Authentifizierung oder

[73] Singh und Chatterjee, „Cloud security issues and challenges: A survey“, S. 97.
[74] Sajjan und Ghorpade, „Ransomware attacks: Radical menace for cloud computing“, S. 1640.
[75] Singh und Chatterjee, „Cloud security issues and challenges: A survey“, S. 97.
[76] Butt u. a., „Cloud security threats and solutions: A survey“, S. 398.
[77] Cloud Security Alliance, *Top Threats to Cloud Computing 2024*.
[78] Ohm u. a., „Backstabber's knife collection: A review of open source software supply chain attacks“, S. 23.
[79] Kunduru, „THE PERILS AND DEFENSES OF ENTERPRISE CLOUD COMPUTING: A COMPREHENSIVE REVIEW“.

Sicherheitsgefahr	Vertraulichkeit	Integrität	Verfügbarkeit
Phishing und Social Engineering	✗	✗	✗
Böswilliger Insider	✗	✗	✗
Virt. und geteilte Ressourcen	✗	✗	✗
Datenverlust	✗	✗	✗
Identitätsdiebstahl	✗	✗	✗
Denial-of-Service			✗
Supply Chain Attack	✗	✗	✗
Fehlkonfiguration	✗	✗	✗
IAM	✗	✗	✗
Überwachung bzw. Sichtbarkeit	✗	✗	✗

Tabelle 2.1: Sicherheitsgefahren – CIA Triade (abgeleitet aus Singh und Chatterjee, „Cloud security issues and challenges: A survey“, Cloud Security Alliance, *Top Threats to Cloud Computing 2024*, Guilfoyle, Paige und McLaughlin, „The final frontier of cyberspace: The seabed beyond national jurisdiction and the protection of submarine cables“ und Butt u. a., „Cloud security threats and solutions: A survey“)

Single Sign-On eingesetzt. Zusätzlich wird damit die Zugriffsverwaltung realisiert, indem nur für die Identitäten freigegebenen Komponenten Zugriff gewährt wird. Dafür kommen folgende Mechanismen zur Anwendung:

- Mandatory Access Control (MAC): Die Kontrolle des Zugriffs erfolgt direkt in der Applikation, für die der Zugriff kontrolliert wird[80].
- Discretionary Access Control (DAC): Die Zugriffskontrolle erfolgt außerhalb in einer anderen Applikation[81].
- Role Based Access Control (RBAC): Zugriffsrechte werden in Rollen gebündelt[82].
- Attribute-based Access Control (ABAC): Anhand der Attribute der Benutzer:innen, des Systems oder zugegriffenen Ressourcen wird mittels Policies der Zugriff kontrolliert[83].

Aufgrund der Gefahren, die von kompromittierten – ursprünglich vertrauenswürdigen – Systemen ausgehen, etablierte sich das **Zero Trust**-Konzept. Es beruht auf der Idee, dass keiner Entität automatisch innerhalb eines Netzwerks vertraut wird[84]. Ein Merkmal eines

[80] Indu, Anand und Bhaskar, „Identity and access management in cloud environment: Mechanisms and challenges“.
[81] Ebd.
[82] Ebd.
[83] Ebd.
[84] Sarkar u. a., „Security of Zero Trust Networks in Cloud Computing“, S. 1.

Zero Trust-Netzwerks ist unter anderem Micro Segmentation[85], also die netzwerktechnische Trennung pro Knoten, anstatt der bloßen Differenzierung zwischen internen und externen Netzen. Ferner wird der Datenverkehr vollständig verschlüsselt, auch wenn die Kommunikation nur im eigenen Netzwerk stattfindet[86]. Authentifizierung wird laufend durchgeführt und nicht nur beim initialen Verbindungsaufbau[87]. Sicherheitsrichtlinien müssen granular und anpassbar sein[88].

Ein vergleichsweise neuer Ansatz ist das **Cloud Security Posture Management (CSPM)**. Dabei wird der Sicherheitsstatus von IaaS und PaaS durchgehend durch das Verhindern, Erkennen und Reagieren auf Bedrohungen geschützt[89]. Es werden Cloud-Konfigurationen anhand von Unternehmensrichtlinien, regulativer Vorgaben und Frameworks überprüft sowie entsprechende Vorschläge zur Korrektur erstellt[90]. Ähnliches bietet auch das **Cloud Infrastructure Entitlements Management (CIEM)**, ein automatisches Tool, das die Wahrscheinlichkeit von Datenpannen in Public Cloud-Umgebungen durch das Überwachen von Rechten und Benutzer:innenaktivitäten reduzieren soll[91]. CIEM erkennt zu weitreichende Rechtevergaben und schränkt sie automatisch auf das notwendige Maß ein[92]. Zur Reaktion auf Sicherheitsvorfälle (Incident Response) gibt es Tools der Produktkategorie **Cloud Investigation and Response Automation (CIRA)**[93]. Damit können forensische Daten über mehrere Cloud-Umgebungen hinweg gesammelt bzw. analysiert werden und helfen folglich bei der Aufarbeitung[94].

Um die Verantwortlichkeiten von Kund:innen und Cloud-Anbietern zu regeln, wird das **Shared Responsibility Model** genutzt, das auch bei den größten Public Cloud-Anbietern anzutreffen ist[95]. Ferner findet das Modell Eingang in NIST-Standards und in den Payment Card Industry Data Security Standard (PCI DSS)[96].

2.7 Cloud-Repatriation

Unter Cloud-Repatriation wird die Migration von Diensten bei Public Cloud-Anbietern hin zu On-Premises verstanden[97]. Ein Hauptgrund für Cloud-Repatriation ist dabei häufig der hohe monetäre Aufwand für Kund:innen in Public Cloud-Umgebungen, auch

[85] Sarkar u. a., „Security of Zero Trust Networks in Cloud Computing“, S. 9.
[86] Ebd., S. 9.
[87] Ebd., S. 9.
[88] Ebd., S. 9.
[89] Gartner, *Definition of Cloud Security Posture Management*.
[90] Ebd.
[91] Ahir und Shaikh, „A Systematic Survey on Cloud Security Threats, Impacts and Remediation“, S. 6.
[92] Ebd., S. 6.
[93] Gartner, *Emerging Tech: Security — Cloud Investigation and Response Automation Offers Transformation Opportunities*.
[94] CADO, *Why is CIRA (Gartner) all the Hype for Cloud Incident Response?*
[95] Lane, Shrestha und Ali, „Managing the risks of data security and privacy in the cloud: a shared responsibility between the cloud service provider and the client organisation“, S. 4.
[96] Ebd., S. 4.
[97] Jewargi, „Public Cloud to Cloud Repatriation Trend“, S. 1.

wenn die Betreiber besonders mit Kosteneffizienz werben[98]. Daneben werden als Gründe interne Richtlinien, Speicherbedarf und bessere Kontrolle auf eigenen Umgebungen angeführt[99]. Der File-Hosting-Dienst Dropbox hat beispielsweise im Jahr 2017 seine Dienste in eigene Rechenzentren verlagert[100]. Damit konnten im ersten Jahr 20 Millionen eingespart und in den folgenden zwei bis drei Jahren sollten ca. 75 Millionen US-Dollar an Einsparungen erreicht werden[101]. Auch das Social-Media-Unternehmen X (vormals Twitter) hat Teile seines Datenspeichers auf eigene Infrastruktur übertragen und soll dadurch eine Kostensenkung von 60 Millionen US-Dollar pro Jahr erreicht haben[102].

In einer online durchgeführten Umfrage von Netwrix zum Thema Cloud-Sicherheit aus dem Jahr 2022 gaben 66 % der 720 befragten IT-Expert:innen weltweit an, sensible Informationen von Public Cloud-Dienstanbietern wieder entfernt zu haben, wenngleich 78 % angaben, mit der Cloud-Sicherheit zufrieden zu sein[103]. Ferner gaben 20 % an, gar keine sensiblen Informationen bei Public Cloud-Anbietern zu speichern.[104]. Im genannten Bericht wurde gemutmaßt, dass manche Einrichtungen meinen, Dateien seien On-Premises sicherer aufgehoben[105].

[98] Murugesan, „Cloud Services—Boon or Bane: A Comprehensive Review“, S. 2.
[99] Ebd., S. 2.
[100] TechCrunch, *Why Dropbox decided to drop AWS and build its own infrastructure and network.*
[101] Murugesan, „Cloud Services—Boon or Bane: A Comprehensive Review“, S. 2.
[102] Ebd., S. 2.
[103] Netwrix, *Cloud Data Security Report*, S. 25.
[104] Ebd., S. 25.
[105] Ebd., S. 25.

KAPITEL 3

Forschungsstand

Im Zeitraum von 2013 bis 2015 gab es ein von der EU finanziertes Forschungsprojekt mit dem Titel „SECCRIT- SEcure Cloud computing for CRitical infrastructure IT“, koordiniert durch das Austrian Institute of Technology (AIT). Erklärtes Projektziel war es, Cloud-Computing-Technologien mit Hinblick auf Sicherheitsrisiken für sensible Bereiche zu analysieren. Gleichzeitig sollten Methoden, Technologien und Best Practices für Cloud-Computing in kritischer Infrastruktur erarbeitet werden[1]. Aus dem Projekt resultierten laut Projektbericht wertvolle Einblicke und Empfehlungen, um besonders die Sicherheit vor Cyberangriffen zu erhöhen[2]. Eine ihm Rahmen des Forschungsprojekts entsprungene Arbeit untersuchte die Auswirkungen der Anforderungen auf die kritische Infrastruktur sowie deren Einfluss auf Cloud-Migrationsrichtlinien[3]. Dabei zeigte sich im Zuge einer Umfrage, dass für Dienstleister der kritischen Infrastruktur der Server- bzw. Datenstandort (besonders in Hinblick auf die rechtliche Domäne) wichtiger ist als für reine Industrieunternehmen[4]. Auf Basis dieser Erkenntnisse wurde eine Richtlinie für die Cloud-Migration von Software vorgestellt, die sich in fünf Phasen teilt: Analyse (auch der rechtlichen Rahmenbedingungen und Implikationen der Migration), Design der Software-Architektur, Implementierung, Verifikation und Deployment[5]. Besonders auf den ersten Punkt wird im Zuge dieser Arbeit eingegangen.

In einem Artikel zum Thema Risiko durch die US-Überwachung für den öffentlichen Sektor im Cloud-Bereich und deren Mitigation wurde auf die massiven rechtlichen Herausforderungen hingewiesen, die sich ergeben, sobald mehr als bloßer Speicherplatz bei US-Cloud-Dienstleistern genutzt wird (eine Begrenzung auf reines Datenspeichern

[1] European Commission, *SEcure Cloud computing for CRitical infrastructure IT*.
[2] Ebd.
[3] Wagner u. a., „Impact of critical infrastructure requirements on service migration guidelines to the cloud“, S. 1.
[4] Ebd., S. 7–8.
[5] Ebd., S. 7.

schränkt jedoch den Funktionsumfang stark ein)[6]. Der Autor diskutierte die Frage, ob nach schwedischem Recht das bloße Hochladen von vertraulichen Informationen bei US-Cloud-Anbietern bereits eine gesetzeswidrige Weitergabe darstellt[7]. Als einer der kritischsten Punkte wurde ermittelt, dass der Oberste Gerichtshof der Vereinigten Staaten Nicht-US-Staatsbürgern außerhalb der USA fundamentale Rechte bis dato nicht zuerkannte[8]. Ferner habe die EU als Datenstandort keinen Effekt, da US-Unternehmen auch bei Serverstandorten außerhalb der USA den Aufforderungen von US-Behörden Folge leisten müssen[9]. Einen ähnlichen Fokus legte Lawrence Siry in seiner Arbeit zur grenzüberschreitenden Beweissicherung, im Hinblick auf den Clarifying Lawful Overseas Use of Data Act (CLOUD Act) und die Auswirkungen auf die Rechte von EU-Bürger:innen[10]. Darin wurde das Problem – für international tätige Unternehmen – der Verpflichtung, gesetzliche Anforderungen eines Landes zu befolgen, mit denen gleichzeitig die eines anderen Landes verletzt werden, beleuchtet[11]. In seiner Arbeit hielt er fest, dass Industrievertreter:innen die Notwendigkeit von Rechtssicherheit auf dem Gebiet der grenzüberschreitenden Beweissicherung sehen[12]. Jene Erkenntnisse werden als Inspiration genutzt, um im Zuge dieser Thesis die neueren rechtlichen Entwicklungen beim Datenzugriff von US-Behörden zu beleuchten.

Ariana Polyviou und Nancy Pouloudi haben die Entscheidungsfindung bei Public Cloud-Betrachtungen im öffentlichen Sektor untersucht, indem sie die Ergebnisse von 21 Interviews, die in sechs europäischen Ländern durchgeführt wurden, analysiert haben[13]. Die Interviewten kamen aus den öffentlichen Sektoren Bildung, Regierungsbehörden, Regionalverwaltungen und IT-Dienstleister[14]. Dabei zeigte sich eine positive Einstellung beim Umstieg auf Cloud-Dienste, wobei die meisten Barrieren außerhalb der Kontrolle der Organisation lagen[15]. Diese umfassten: Kompatibilität, Bürokratie, politische bzw. juristische Probleme und Verständnis für die Komplexität der Technologie[16].

Eine Analyse zum Netz- und Informationssystemsicherheitsgesetz (NISG) wurde im Buch „Netz- und Informationssystemsicherheitsgesetz (NISG): Kurzkommentar“ von Axel Anderl, Vinzenz Heußler, Sylvia Mayer und Bernhard Müller dargelegt. Darin wurden die wesentlichen Aspekte der Umsetzung der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NISR) dargestellt, bei gleichzeitiger Abdeckung

[6] Hildén, „Mitigating the risk of US surveillance for public sector services in the cloud“, S. 18.
[7] Ebd., S. 14.
[8] Ebd., S. 18.
[9] Ebd., S. 18.
[10] Siry, „Cloudy days ahead: Cross-border evidence collection and its impact on the rights of EU citizens“, S. 227.
[11] Ebd., S. 247.
[12] Ebd., S. 247.
[13] Polyviou und Pouloudi, „Understanding cloud adoption decisions in the public sector“, S. 2085.
[14] Ebd., S. 2088.
[15] Ebd., S. 2093–2094.
[16] Ebd., S. 2094.

anwaltlicher und behördlicher Praxis[17]. Der Kommentar befasst sich zwar nicht explizit mit Cloud-Computing, jedoch können die im Text aufgezeigten rechtlichen Anforderungen für den Einsatz von Cloud-Computing bei kritischer Infrastruktur relevant sein. Er dient dieser Thesis damit besonders bei der Analyse der rechtlichen Situation in Österreich als Stütze.

Donald David Stewart Ferguson hat im Jahr 2023 die Wirksamkeit der Risikomanagement-Maßnahmen der Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NISR2) für wichtige und wesentliche Einrichtungen gegen Cyberangriffe mittels Rechtsauslegung und einer Cyber Kill Chain Modellanalyse untersucht[18]. Dabei kam der Autor zum Schluss, dass die Wirksamkeit sehr eingeschränkt sein könnte, da der Fokus nicht auf das Verhindern von Cyberangriffen liege, sondern auf die Eingrenzung der Auswirkungen von Angriffen auf Widerstandsfähigkeit der Netz- und Informationssysteme sowie die Empfänger:innen der jeweiligen Dienste[19]. Die wichtigste Beobachtung der Modellanalyse war, dass Bedrohungsakteure weitgehend von Risikomanagement- und Incident-Response-Maßnahmen ungehindert in der Frühphase eines Cyberangriffs fortschreiten könnten und damit ein massiver Schaden bei Einrichtungen verursacht werden könnte[20]. Der Autor identifizierte Maßnahmen, wie beispielsweise Schwachstellen-Scans interner Ressourcen oder tiefgehende Penetrationstests, die nicht explizit von Risikomanagement- und Incident-Response-Maßnahmen gefordert sind und daher in Durchführungsbestimmungen zur NISR2 Beachtung finden sollten[21]. Ob die österreichische Umsetzung der NISR2 in Form des NISG 2024 diese Punkte berücksichtigt, wird in Abschnitt 4.5 erörtert.

Philipp Eckhardt und Anastasia Kotovskaia haben in ihrer Arbeit das Zusammenspiel zwischen der NISR2 und dem Entwurf der Verordnung (EU) über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (CRV) untersucht. Dabei kamen sie zum Schluss, dass die Cybersicherheitsanforderungen in der CRV helfen könnten, Risikomanagementanforderungen aus der NISR2 im Hinblick auf Lieferketten zu erfüllen[22]. Daneben soll die in der CRV geforderte Transparenz bei digitalen Elementen von Produkten leichtere Vergleichbarkeit herstellen[23]. Es wurde allerdings der mögliche Bedarf einer Angleichung der Meldepflicht zwischen den beiden Regulativen festgestellt[24].

[17] Anderl u. a., *Netz-und Informationssystemsicherheitsgesetz (NISG): Kurzkommentar*, S. VII.
[18] Ferguson, „The outcome efficacy of the entity risk management requirements of the NIS 2 Directive“, S. 371.
[19] Ebd., S. 384.
[20] Ebd., S. 384.
[21] Ebd., S. 384.
[22] Eckhardt und Kotovskaia, „The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive“, S. 163.
[23] Ebd., S. 163.
[24] Ebd., S. 163.

Im Dezember 2023 hat die Europäische Kommission (EK) ein Projekt mit dem Namen Important Project of Common European Interest Next Generation Cloud Infrastructure and Services (IPCEI CIS) zu fortgeschrittenen Cloud- und Edge-Computing-Technologien genehmigt mit dem Ziel, Forschung, Entwicklung und ein erstes Deployment über mehrere Anbieter in Europa hinweg zu unterstützen[25]. Sieben Mitgliedstaaten stellen dafür 1,2 Milliarden Euro bereit, bei gleichzeitiger Erwartung, dass weitere 1,4 Milliarden aus privaten Investments finanziert werden[26]. Das Projekt soll dazu beitragen, mehrere Ziele der EU für die Wirtschaft zu erreichen, wie Resilienz, Sicherheit und Souveränität[27]. Vor allem der letzte Punkt lässt vermuten, dass auch die Abhängigkeit von US-amerikanischen Cloud-Dienstleistern reduziert werden soll.

Die Cloud Security Alliance (CSA), eine Verbindung aus vielen großen Public Cloud-Anbietern (wie Google, Amazon und Microsoft)[28], hat für das Jahr 2024 einen Bericht zu Sicherheitsproblemen in der Cloud-Industrie herausgegeben. Dabei wurden über 500 Expert:innen aus der Industrie befragt, elf Gefahren ermittelt und nach Wichtigkeit sortiert[29]. Ferner erfolgte eine Business-Impact-Analyse, zugehörige Sicherheitskontrollen wurden angeführt und die Ergebnisse jenen von 2022 gegenübergestellt[30]. Die Autor:innen empfehlen im Bericht fortlaufende Investitionen in die neuesten Sicherheitslösungen, wie Cloud Security Posture Management (CSPM) (siehe Unterabschnitt 2.6.2) und Endpoint Detection and Response (EDR) Tools[31]. Aufbauend auf einem ähnlichen Bericht im Jahr 2016 haben Ashish Singh und Kakali Chatterjee in ihrer Arbeit „Cloud security issues and challenges: A survey“ das Design einer integrierten Sicherheitslösung gefordert, die alle großen Sicherheitsanforderungen der Cloud adressiert[32].

In einer Untersuchung zum aktuellen Status von Cloud-Computing in der kritischen Infrastruktur wurden Literaturrecherchen und Expert:inneninterviews im Jahr 2018 in Deutschland durchgeführt[33]. Dabei zeigte sich, dass Cloud-Computing nur zum Teil eingesetzt wird, Zurückhaltung vorherrscht und meist Cloud-Computing nur für nicht kritische Systeme Anwendung findet[34]. Für Betreiber sind oft regulative Vorgaben und ungeklärte rechtliche Fragen Hemmnisse für den Wechsel auf derartige Dienste[35]. Obwohl steigender Bedarf feststellbar ist, herrscht auch beim Risikomanagement vielerorts noch Unklarheit[36]. Die Autoren merkten an, dass weitere Interviews vorzugsweise mit allen Sektoren kritischer Infrastruktur wünschenswert sind, da sie selbst nur einen kleinen Bereich an Unternehmen

[25] European Commission, *Common European Interest in computing technologies*.
[26] Ebd.
[27] Ebd.
[28] Cloud Security Alliance, *Current Corporate Members*.
[29] Cloud Security Alliance, *Top Threats to Cloud Computing 2024*, S. 5.
[30] Ebd.
[31] Ebd., S. 57.
[32] Singh und Chatterjee, „Cloud security issues and challenges: A survey“, S. 111.
[33] Adelmeyer und Teuteberg, „Cloud Computing Adoption in Critical Infrastructures-Status Quo and Elements of a Research Agenda“, S. 1346–1347.
[34] Ebd., S. 1354.
[35] Ebd., S. 1354.
[36] Ebd., S. 1354.

erfassen konnten[37]. Zusätzlich wurde der Bedarf weiterer Forschung in den Kernfunktionen kritischer Infrastruktur für Cloud-Computing angemerkt[38]. Im Forschungsstand wurden Lücken in den Kategorien „technisch“, „juristisch“, „organisatorisch“ und „vertraglich“ identifiziert[39]. In Teilen schließt nun diese Thesis an jene Expert:inneninterviews in Deutschland an, mit dem Unterschied, dass der Fokus auf österreichischer kritischer Infrastruktur liegt und mehrheitlich auf IT-Unternehmensberater:innen, die für unterschiedliche Einrichtungen der kritischen Infrastruktur tätig sind, zurückgegriffen wird.

[37] Ebd., S. 1354.
[38] Ebd., S. 1354.
[39] Ebd., S. 1352.

KAPITEL 4

Rechtliche Analyse

In den vergangenen Jahren hat die EU begonnen, Informationssicherheit immer stärker zu regulieren und zahlreiche Vorgaben bzw. Vorhaben veröffentlicht. Vieles davon ist noch im Entwurfsstadium oder entsprechende Richtlinien müssen erst in nationale Gesetze überführt werden. Ferner hat im Jahr 2020 die EK und der Hohe Vertreter der EU für Außen- und Sicherheitspolitik die neue EU Cybersicherheitsstrategie vorgestellt, deren Ziel es ist, die Sicherheit von wesentlichen Diensten zu gewährleisten[1]. Auf Betreiber von kritischer Infrastruktur im weitesten Sinne und Public Cloud-Dienstanbieter kommen wohl in Bälde weitere massive Anforderungen zu, sei es durch Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA) für Finanzdienstleister, Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NISR2) ganz allgemein oder durch Cloud Services Schema (EUCS) für Cloud-Betreiber, die eine potenziell notwendige Zertifizierung anstreben. Gleichzeitig gab es beispielsweise mit dem Bundesgesetz über das Bankwesen (BWG) für den Finanzsektor schon früher österreichische nationalstaatliche spezifische Vorgaben in Hinblick auf Cloud-Computing, während für Finanzunternehmen die Leitlinien der EBA hinzukommen. Einen Überblick zur aktuellen regulatorischen Arbeit auf europäischer und österreichischer Seite bzw. deren Beziehungen und Abhängigkeiten liefert die Abbildung 4.1. Ferner wird auf die Entwicklung in den USA eingegangen, wo praktisch alle großen Public Cloud-Anbieter ihren Sitz haben und in den Gebotsbereich des US-Rechts fallen.

Methodisch werden im Zuge dieser Arbeit, beginnend bei österreichischen nationalen Gesetzen, über EU-Vorgaben, bis zu US-amerikanischen Regularien entsprechend relevante gesetzliche Anforderungen für in Österreich ansässige kritische Infrastruktur in einer weiter gefassten Definition ermittelt. Dabei werden die rechtlichen Aspekte für einen Public Cloud-Einsatz dieser Organisationen herausgearbeitet und wird untersucht welche Konflikte bzw. Schwierigkeiten dabei entstehen können.

[1] Europäische Kommission, *Gestaltung der digitalen Zukunft Europas.*

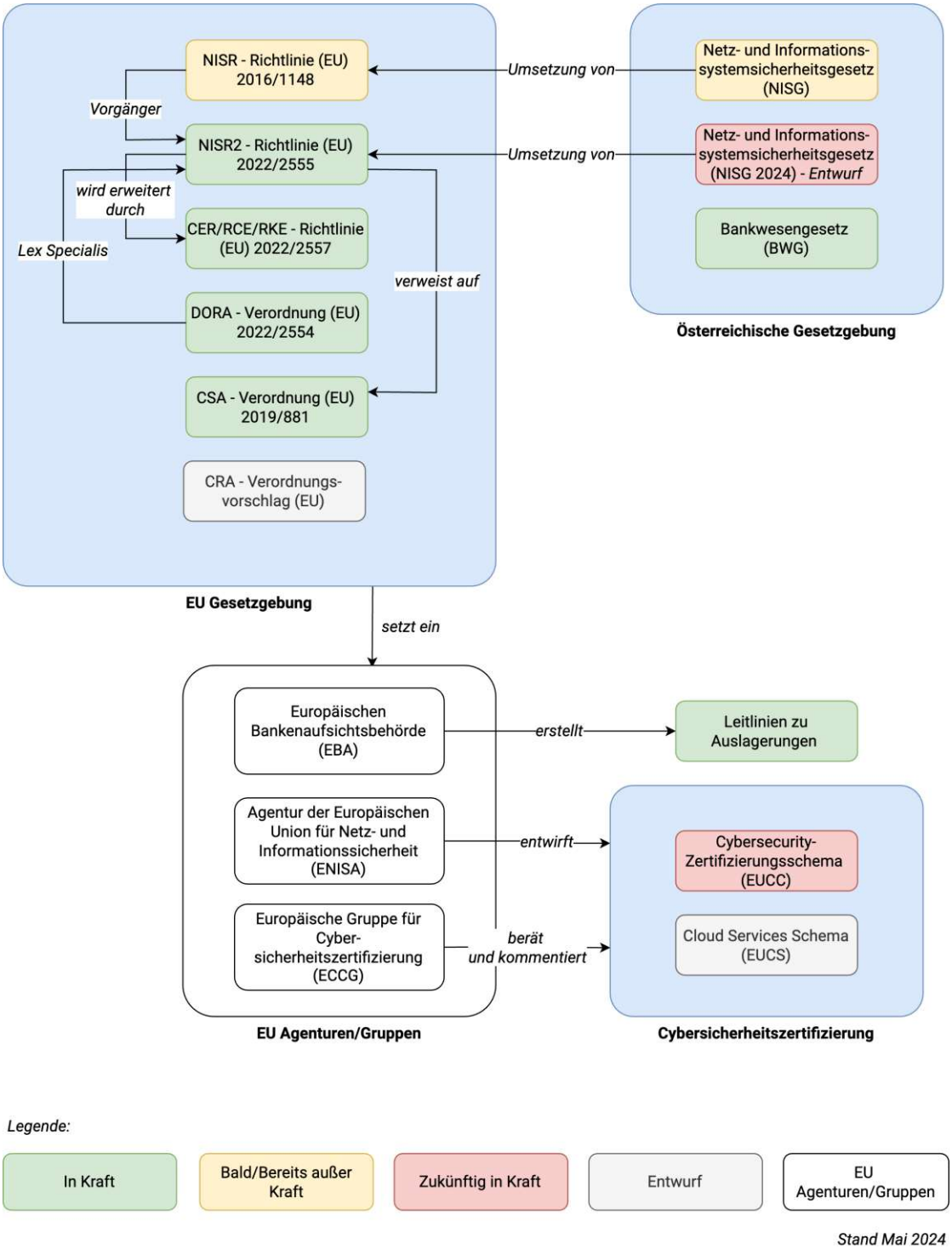

Abbildung 4.1: Überblick zu europäischen und österreichischen Regulativen (eigene Grafik)

4.1 Netz- und Informationssystemsicherheitsgesetz (NISG)

Mit dem Netz- und Informationssystemsicherheitsgesetz (NISG) setzt Österreich seit Ende 2018 die Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NISR) um. Es ist für kritische Infrastruktur in Österreich eines der relevantesten Regulative und stellt an unterschiedliche Einrichtungen teils sehr konkrete Anforderungen. Daher wird das Gesetz in diesem Kapitel tiefgehender beleuchtet. Für kritische Infrastruktur selbst gibt es keine einheitliche Definition, allerdings hat der Gesetzgeber im NISG den Begriff *wesentlicher Dienst* wie folgt definiert:

> *„ein Dienst, der in einem der in §2 genannten Sektoren [siehe unten] erbracht wird und der eine wesentliche Bedeutung insbesondere für die Aufrechterhaltung des öffentlichen Gesundheitsdienstes, der öffentlichen Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, des öffentlichen Verkehrs oder die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie hat und dessen Verfügbarkeit abhängig von Netz- und Informationssystemen ist“*[2]

Um als Betreiber wesentlicher Dienste zu gelten, muss die Einrichtung eine Niederlassung in Österreich haben[3]. Jene Sektoren, in denen der Dienst erbracht werden muss, um überhaupt in die Anwendbarkeit des NISG zu fallen, umfassen die folgenden:

1. *Energie*
2. *Verkehr*
3. *Bankwesen*
4. *Finanzmarktinfrastrukturen*
5. *Gesundheitswesen*
6. *Trinkwasserversorgung*
7. *Digitale Infrastruktur*

(Obenstehende Aufzählung vollständig übernommen aus *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*, §2)

[2] *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*, §3 Z 9.
[3] Ebd., §3 Z 10.

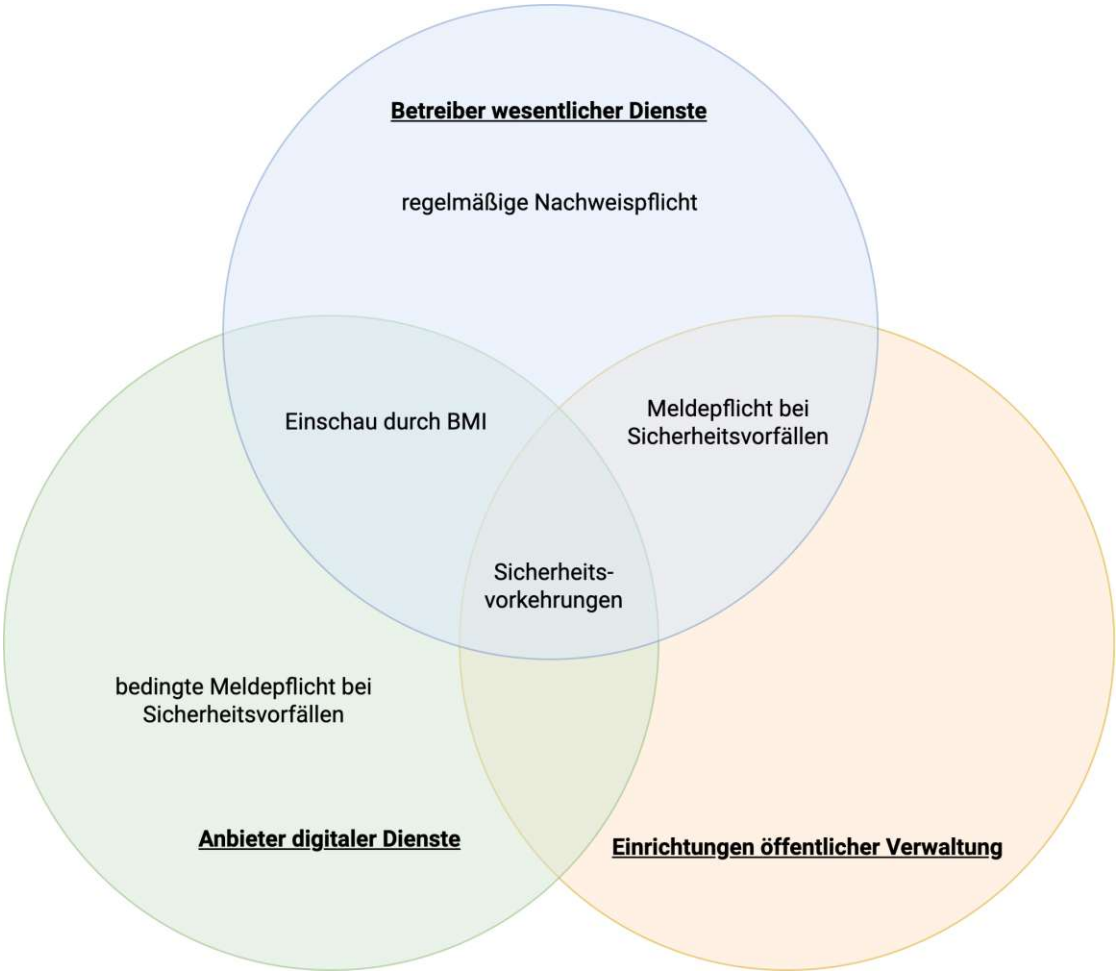

Abbildung 4.2: Verpflichtungen nach dem NISG (basierend auf *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*)

Neben Betreibern wesentlicher Dienste kennt das NISG noch zwei weitere Adressaten, nämlich Anbieter digitaler Dienste und Einrichtungen der öffentlichen Verwaltung[4]. Für beide gibt es gesonderte Verpflichtungen. Einen vergleichenden und allgemeinen Überblick zu den Verpflichtungen zwischen den betroffenen Einrichtungen nach dem NISG liefert Abbildung 4.2.

[4] *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*, §21 und §22.

4.1.1 Betreiber wesentlicher Dienste

Die Ermittlung der Betreiber wesentlicher Dienste wird in Österreich durch das Bundeskanzleramt (BKA) durchgeführt[5], erfolgt also proaktiv durch den Staat. Im Gegensatz dazu müssen sich beispielsweise in Deutschland Betreiber selbst ermitteln[6]. Dies geschieht anhand von Kriterien in der BSI-Kritisverordnung, die von Betroffenen selbstständig geprüft werden müssen[7]. Eine Auflistung der vom BKA konkret erfassten Dienste in Österreich ist aktuell nicht öffentlich zugänglich. Bei einer parlamentarischen Anfragebeantwortung wurde auf den Geheimnisschutz verwiesen[8]. Aus der Anfragebeantwortung geht allerdings hervor, dass zum 7. Februar 2020 37 Einrichtungen ermittelt wurden[9]. Jedoch kann durch die Auflistung von Kategorien im Gesetzestext bereits auf einige Betreiber mutmaßend geschlossen werden.

Daneben veröffentlichen das Bundeskanzleramt (BKA) sowie das Bundesministerium für Inneres regelmäßig sogenannte NIS Fact Sheets. Mit Dezember 2023 finden sich auf der Website des Innenministeriums fünf derartige Dokumente[10]. Zweck der NIS Fact Sheets ist es, betroffenen Unternehmen Unterstützungsmaterial zur Befolgung des Gesetzes zur Verfügung zu stellen. Darin finden sich teilweise konkret ausformulierte Empfehlungen, wie dem Gesetz entsprochen werden kann.

Die erste Anforderung an Betreiber wesentlicher Dienste ist das Treffen von *„geeignete[n] und verhältnismäßige[n] technische[n] und organisatorische[n] Sicherheitsvorkehrungen“*[11], diese müssen folgende Kategorien umfassen und wurden in den NIS Fact Sheets näher erläutert bzw. in der Netz- und Informationssystemsicherheitsverordnung (NISV) genauer spezifiziert:

1. **Governance und Risikomanagement:** Es sind Netz- und Informationssysteme zu identifizieren, potenzielle Risiken einzuschätzen und regelmäßig zu überprüfen[12]. Ferner muss eine Sicherheitsrichtlinie aufgesetzt und ein Informationssicherheitsmanagementsystem regelmäßig geprüft werden[13]. Es müssen auch ausreichend Ressourcen zum Betrieb des Dienstes zur Verfügung gestellt werden und eingesetztes Personal muss vertrauenswürdig, geschult und qualifiziert sein[14].

2. **Umgang mit Dienstleistern, Lieferanten und Dritten:** Risiken und Abhängigkeiten, die sich durch Beziehungen zu Dritten ergeben, sind festzustellen und zu

[5] *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*, §16 Z 1.
[6] Anderl u. a., *Netz-und Informationssystemsicherheitsgesetz (NISG): Kurzkommentar*, S. 103.
[7] Ebd., S. 103.
[8] *Liste der "Betreiber wesentlicher Dienste"gem § 16 Abs 4 Z 3 NIS-Gesetz | Parlament Österreich.*
[9] Ebd.
[10] *Rechtliches und Dokumente — nis.gv.at.*
[11] *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*, §17 Z 1.
[12] *NIS Fact Sheet 9/2022*, S. 6.
[13] Ebd., S. 7.
[14] Ebd., S. 7–9.

bewerten[15]. Entsprechende Leistungsvereinbarungen müssen geprüft und überwacht werden[16].

3. **Sicherheitsarchitektur:** Netz- und Informationssysteme müssen dokumentiert und sicher konfiguriert werden. Vermögenswerte sind zu analysieren und zu dokumentieren[17]. Netzwerke müssen nach Schutzbedarf segmentiert und sicher gestaltet werden[18]. Vertraulichkeit, Authentizität und Integrität sind durch Kryptografie sicherzustellen[19].

4. **Systemadministration:** Es müssen privilegierte Zugänge mit den nur unbedingt notwendigen Rechten zur Administration eingerichtet werden, die ausschließlich für diesen Zweck verwendet werden dürfen[20]. Zugriffe und Zugänge müssen protokolliert und regelmäßig geprüft werden[21]. Systeme, von denen aus administrative Tätigkeiten vorgenommen werden, dürfen ausschließlich zu diesem Zweck eingesetzt werden und müssen sicher konfiguriert sein[22]. Dezidiert verboten ist der Zugriff auf das Internet von diesen Systemen[23].

5. **Identitäts- und Zugriffsmanagement:** Benutzer:innen und Dienste müssen authentifiziert und identifiziert werden[24]. Nicht mehr benötigte Accounts sind zu deaktivieren[25]. Zwei-Faktor-Authentifizierung muss vorangetrieben werden[26]. Zugriffsrechte müssen mindestens einmal pro Jahr überprüft werden[27]. Sämtliche Änderungen an privilegierten Accounts müssen kontrolliert werden[28].

6. **Systemwartung und Betrieb:** Versionen der eingesetzten Systeme müssen aktuell gehalten und die Software auf Integrität geprüft werden[29]. Gleichzeitig muss die Herkunft der Systeme kontrolliert werden[30]. Wartungsintervalle sind einzuhalten und deren Umsetzung ist zu protokollieren[31]. Schwachstellen und entsprechende Korrekturen in Systemen müssen erfasst und mitigiert werden[32]. Für Fernzugrif-

[15] *NIS Fact Sheet 9/2022*, S. 10–12.
[16] Ebd., S. 10–12.
[17] Ebd., S. 12–13.
[18] Ebd., S. 13–15.
[19] Ebd., S. 15–16.
[20] Ebd., S. 16–17.
[21] Ebd., S. 16–17.
[22] Ebd., S. 16–17.
[23] Ebd., S. 16–17.
[24] Ebd., S. 18.
[25] Ebd., S. 18.
[26] Ebd., S. 18.
[27] Ebd., S. 19.
[28] Ebd., S. 19.
[29] Ebd., S. 20–21.
[30] Ebd., S. 20–21.
[31] Ebd., S. 20–21.
[32] Ebd., S. 20–21.

fe ist die Zwei-Faktor-Authentifizierung zu verwenden[33]. Jene Zugriffe müssen aufgezeichnet werden und unter Kontrolle der Systemverantwortlichen erfolgen[34].

7. **Physische Sicherheit:** Physische Zugänge zu Netz- und Informationssystemen sind zu schützen[35].

8. **Erkennung von Vorfällen:** Durch Sensoren müssen Systeme überwacht werden, um Beeinträchtigungen des Dienstes zu erkennen; dazu sind auch Korrelationen und Analysen der gesammelten Daten durchzuführen[36]. Mindestens zu kontrollieren ist der Datenaustausch zu Lieferanten und Dienstleistern[37].

9. **Bewältigung von Vorfällen:** Für die Reaktion auf Vorfälle müssen Prozesse erstellt werden; diese beinhalten auch das Meldewesen und die Analyse sowie die kontinuierliche Verbesserung[38].

10. **Betriebskontinuität:** Nach einem Sicherheitsvorfall hat der Betreiber den Dienst auf einem festgelegten Niveau wiederherzustellen[39]. Daneben müssen auch Notfallpläne etabliert sein[40].

11. **Krisenmanagement:** Auch vor und während eines Sicherheitsvorfalls muss der Betreiber entsprechende Abläufe haben, um den Betrieb aufrechtzuerhalten[41].

Ferner gibt es für betroffene Betreiber eine Nachweispflicht über die Umsetzung der Anforderungen, die zumindest alle drei Jahre erfüllt werden muss[42]. Dazu muss entweder der Nachweis über eine Überprüfung durch eine Qualifizierte Stelle (QUASTE) (im Sinne von §18 NISG, siehe Abschnitt QUASTE) oder entsprechende Zertifizierungen an den Bundesminister für Inneres (BMI) erbracht werden[43]. Für den BMI gibt es die Möglichkeit einer Einschau zur Kontrolle der Sicherheitsvorkehrungen[44]. Es ist folglich möglich, dass der BMI Zugriff auf sensible Daten, auch von Kund:innen entsprechender Betreiber, erhält. Die Sicherheitsanforderungen und Meldepflichten gelten unabhängig davon, ob betroffene Systeme durch die Einrichtungen selbst betrieben werden oder an Dritte ausgelagert sind[45]. Die Einhaltung im Falle von Ausgliederungen muss vom Betreiber wesentlicher Dienste sichergestellt werden, üblicherweise durch Verträge mit

[33] Ebd., S. 21.
[34] Ebd., S. 21.
[35] *Netz- und Informationssystemsicherheitsverordnung*, Anlage 1.
[36] *NIS Fact Sheet 9/2022*, S. 23–24.
[37] Ebd., S. 23–24.
[38] *Netz- und Informationssystemsicherheitsverordnung*, Anlage 1.
[39] Ebd., Anlage 1.
[40] Ebd., Anlage 1.
[41] Ebd., Anlage 1.
[42] *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*, §17 Abs 3.
[43] Ebd., §17 Abs 3.
[44] Ebd., §17 Abs 4.
[45] *Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016*, ErwG 52.

den entsprechenden Dienstleistern. Verwehrt dies der jeweilige Dienstanbieter, kann dieser folglich nicht für den Betreiber wesentlicher Dienste tätig werden. Gleichzeitig geht auch die Einschaumöglichkeit durch den BMI bei Drittanbietern einher[46]. Unter Drittanbietern ist auch der Einsatz bestimmter Cloud-Computing-Dienste durch Betreiber wesentlicher Dienste gemeint. Wenn also von §17 NISG erfasste Organisationen Dienste wie Amazon Web Services (AWS), Microsoft Azure (Azure), Google Cloud Platform (GCP) oder auch Anbieter ohne Niederlassung in Österreich oder gar Europa in Anspruch nehmen, darf der BMI zumindest theoretisch trotzdem Einsicht nehmen[47].

Bei einem Sicherheitsvorfall haben Betreiber wesentlicher Dienste umgehend eine Meldung an das relevante Computer-Notfallteam zu erstatten, von dem aus die Meldung an den BMI weitergeleitet wird[48]. Auch bei der Inanspruchnahme von Anbietern digitaler Dienste besteht eine Meldepflicht für Betreiber wesentlicher Dienste, wenn es beim digitalen Dienst zu Sicherheitsvorfällen mit erheblicher Auswirkung auf die Verfügbarkeit kommt[49]. Theoretisch müsste die Meldepflicht auch Sicherheitsvorfälle betreffen, die vor dem Inkrafttreten des NISG aufgetreten sind, aber erst nach dem Inkrafttreten entdeckt wurden. Aus dem Gesetz geht allerdings nicht hervor, ob auch alle alten, bereits bekannten Sicherheitsvorfälle gemeldet hätten werden müssen.

4.1.2 Einrichtungen der öffentlichen Verwaltung

Einrichtungen der öffentlichen Verwaltung sind nach dem NISG grundsätzlich Einrichtungen des Bundes, die Begriffsbestimmung kann aber durch Landesgesetze auch auf Einrichtungen der Länder erweitert werden[50]. Einrichtungen der öffentlichen Verwaltung haben am wenigsten konkrete Sicherheitsvorkehrungen umzusetzen (siehe Abbildung 4.2 – gelber Kreis). So fordert das NISG:

> *Zur Gewährleistung der NIS haben Einrichtungen des Bundes in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung wichtiger Dienste nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen für [sic!] zu treffen. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein.“*[51]

Es gibt auch keine Möglichkeiten für eine Einschau durch den BMI und keine Strafbestimmungen[52]. Im Gegensatz zu Anbietern digitaler Dienste und Betreibern wesentlicher Dienste

[46] *Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016*, ErwG 52.
[47] Anderl u. a., *Netz-und Informationssystemsicherheitsgesetz (NISG): Kurzkommentar*, S. 123–124.
[48] *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*, §19 Z 1.
[49] Ebd., §19 Abs 1 und Abs 4.
[50] Ebd., §22 Abs 5.
[51] Ebd., §22 Abs 1.
[52] Ebd., §22 Abs 1.

kann es damit bei Einrichtungen der öffentlichen Verwaltung auch zu keinem Zugriff auf Systeme oder Daten durch den BMI bei Dienstleistern (z. B. Cloud-Computing-Diensten) kommen, die von der öffentlichen Verwaltung eingesetzt werden.

Im NIS-Fact Sheet von 2019 weist das BKA darauf hin, dass die Sicherheitsvorkehrungen aus der NISV auch für Einrichtungen der öffentlichen Verwaltung geeignet sind, um dem NISG zu entsprechen[53]. Es ist damit empfehlenswert, dass sich auch diese daran orientieren.

Die von §22 NISG erfassten Einrichtungen der öffentlichen Verwaltung haben Sicherheitsvorfälle umgehend an das Computer-Notfallteam der öffentlichen Verwaltung (GovCERT) zu melden, wobei analog zu anderen Betreibern die Meldung an den BMI weitergeleitet wird[54]. Eine Ausnahme bilden Einrichtungen, die Teil des Inneren Kreises der Operativen Koordinationsstruktur (IKDOK) sind: in diesem Fall erfolgt die Meldung innerhalb von IKDOK[55].

4.1.3 Anbieter digitaler Dienste

Als Anbieter digitaler Dienste definiert das NISG nur jene österreichischen Dienste, die unter §3 Z 1 E-Commerce-Gesetz (ECG) fallen, gleichzeitig ein Online-Marktplatz, eine Online-Suchmaschine oder ein Cloud-Computing-Dienst sind und kein Kleinstunternehmen oder kleines Unternehmen sind[56]. Die wesentlichen Kriterien, damit ein Dienst unter §3 Z 1 ECG fällt, sind die Entgeltlichkeit, elektronische Erbringung, individuelle Abrufbarkeit und der Fernabsatz (also gleichzeitige Abwesenheit von Nutzer und Anbieter)[57]. Es sind damit auch dezidiert Cloud-Computing-Dienste vom NISG erfasst, sofern sie die oben genannten Anforderungen erfüllen. Der Begriff Cloud-Computing-Dienst ist nach dem NISG folgendermaßen definiert:

> *„[. . .] ein[. . .] digital[er] Dienst, der den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht“*[58]

Werden Cloud-Computing-Dienste nur innerhalb eines Unternehmens erbracht, also beispielsweise für andere Abteilungen, fallen sie folglich damit nicht unter die Definition von Anbietern digitaler Dienste, da kein Entgelt verlangt wird. Dies ist insbesondere für das Liefermodell Private Cloud (siehe Punkt Private Cloud) oder Community Cloud (siehe Punkt Communiy Cloud) – im Falle der Unentgeltlichkeit – relevant.

[53] *Umsetzungsleitfaden für Einrichtungen des Bundes*, S. 21.
[54] *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*, §22 Abs 2.
[55] Ebd., §22 Z 2.
[56] Ebd., §3 Abs 12 und Abs 13.
[57] Anderl u. a., *Netz-und Informationssystemsicherheitsgesetz (NISG): Kurzkommentar*, S. 19–21.
[58] *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*, §3.

Die NISR schätzt Anbieter digitaler Dienste weniger wichtig für die Aufrechterhaltung kritischer gesellschaftlicher und wirtschaftlicher Tätigkeiten ein als Betreiber wesentlicher Dienste. Das spiegelt sich auch in den Anforderungen wider (siehe Abbildung 4.2 – grüner Kreis). Es sollen Durchführungsrechtsakte die Spezifikation und Umsetzung der Maßnahmen erleichtern[59,60]. Das NISG fordert von Anbietern digitaler Dienste konkret folgende Sicherheitsmaßnahmen, die aus der NISR[61] übernommen wurden und in der Durchführungsverordnung (EU) 2018/151 genauer spezifiziert sind:

a) **Sicherheit der Systeme und Anlagen:** Netz- und Informationssysteme müssen systematisch verwaltet werden, also entsprechend dokumentiert und die Informationssicherheit gemanagt werden[62]. Auch Vorkehrungen zum physischen Schutz der Systeme sind zu treffen[63]. Für unentbehrliche Güter oder Vorleistungen, die zum Betrieb unbedingt notwendig sind, muss Versorgungssicherheit gewährleistet sein[64]. Daneben ist der Zugang zu Netz- und Informationssystemen zu kontrollieren[65].

b) **Bewältigung von Sicherheitsvorfällen:** Mit dem Einsatz von entsprechenden Verfahren sollen ungewöhnliche Ereignisse rechtzeitig erkannt und eingeordnet werden[66]. Daneben muss es Vorgaben für Meldungen von Vorfällen sowie das Erkennen von Schwachstellen geben[67]. Bei Sicherheitsvorfällen müssen daraus resultierende Erkenntnisse dokumentiert werden[68].

c) **Betriebskontinuitätsmanagement:** Es sind Notfallpläne und Wiederherstellungskapazitäten zu entwickeln und regelmäßig, beispielsweise im Zuge von Übungen, zu prüfen[69].

d) **Überwachung, Überprüfung und Erprobung:** Es sind regelmäßige Kontrollen durchzuführen, ob Systeme funktionieren[70]. Mängel in Sicherheitsmechanismen müssen über einen Prozess feststellbar sein und die Befolgung von Normen oder Leitlinien muss kontrolliert werden[71].

[59] *Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016*, ErwGr 49.
[60] Anderl u. a., *Netz-und Informationssystemsicherheitsgesetz (NISG): Kurzkommentar*, S. 155.
[61] *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*, §21 Abs 1.
[62] *Durchführungsverordnung (EU) 2018/151 der Kommission vom 30. Januar 2018*, Art 2 Abs 1 lit a.
[63] Ebd., Art 2 Abs 1 lit b.
[64] Ebd., Art 2 Abs 1 lit c.
[65] Ebd., Art 2 Abs 1 lit d.
[66] Ebd., Art 2 Abs 2 lit a.
[67] Ebd., Art 2 Abs 2 lit b.
[68] Ebd., Art 2 Abs 2 lit d.
[69] Ebd., Art 2 Abs 3.
[70] Ebd., Art 2 Abs 4.
[71] Ebd., Art 2 Abs 4.

e) **Einhaltung der internationalen Normen:** Anbieter digitaler Dienste können auch internationale, europäische oder national anerkannte Normen und Spezifikationen für die Sicherheit ihrer Systeme anwenden[72].

Für einen Vergleich und eine Gegenüberstellung von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste betreffend die Sicherheitsmaßnahmen siehe Abbildung 4.3. Bei Betreibern wesentlicher Dienste sind die Sicherheitsmaßnahmen deutlich konkreter und umfangreicher.

Im Gegensatz zu Betreibern wesentlicher Dienste darf der BMI Kontrollen oder Einschaurechte nur wahrnehmen, wenn er Kenntnis erlangt, dass ein Anbieter digitaler Dienste sich nicht an die geforderten Sicherheitsvorkehrungen hält[73,74].

Bei einem Sicherheitsvorfall betreffend einen ihrer digitalen Dienste haben Anbieter eine unmittelbare Meldepflicht beim nationalen Computer-Notfallteam oder GovCERT[75]. Letztere nehmen eine Weiterleitung an den BMI vor[76]. Die Meldepflicht gilt für Anbieter digitaler Dienste allerdings nur, wenn diese Informationen besitzen, die zum Bewerten eines Sicherheitsvorfalles benötigt werden[77]. Sie sind damit seltener zu Meldungen verpflichtet als Betreiber wesentlicher Dienste oder Einrichtungen der öffentlichen Verwaltung.

Mitgliedstaaten der EU dürfen nach Artikel 16, Absatz 10 NISR keine zusätzlichen Sicherheitsvorkehrungen oder Meldepflichten für Anbieter digitaler Dienste festlegen[78,79].

4.1.4 Qualifizierte Stelle (QUASTE)

Zu Nachweis über die Sicherheitsvorkehrungen haben Betreiber wesentlicher Dienste eine Überprüfung durch eine Qualifizierte Stelle (QUASTE) durchführen zu lassen (sofern sie nicht auf andere Nachweismöglichkeiten zurückgreifen können)[80]. Die Qualifikation einer solchen Stelle kann auch nur auf bestimmte Sicherheitsvorkehrungen/Kategorien eingeschränkt sein[81]. Auch bei der QUASTE kann der BMI Einschau nehmen, jedoch nicht in deren Daten in Bezug auf durchgeführte Überprüfungen[82]. Dazu müsste der BMI sich direkt an Betreiber wesentlicher Dienste wenden.

[72] Ebd., Art 1 Abs 5.
[73] *Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016*, Art 17.
[74] Anderl u. a., *Netz-und Informationssystemsicherheitsgesetz (NISG): Kurzkommentar*, S. 155.
[75] *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*, §21 Z 2.
[76] Ebd., §21 Abs 2.
[77] Ebd., §21 Abs 2.
[78] *Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016*, Art 16, Absatz 10.
[79] Anderl u. a., *Netz-und Informationssystemsicherheitsgesetz (NISG): Kurzkommentar*, S. 148.
[80] *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*, §17 Z 3.
[81] Anderl u. a., *Netz-und Informationssystemsicherheitsgesetz (NISG): Kurzkommentar*, S. 125.
[82] Ebd., S. 129.

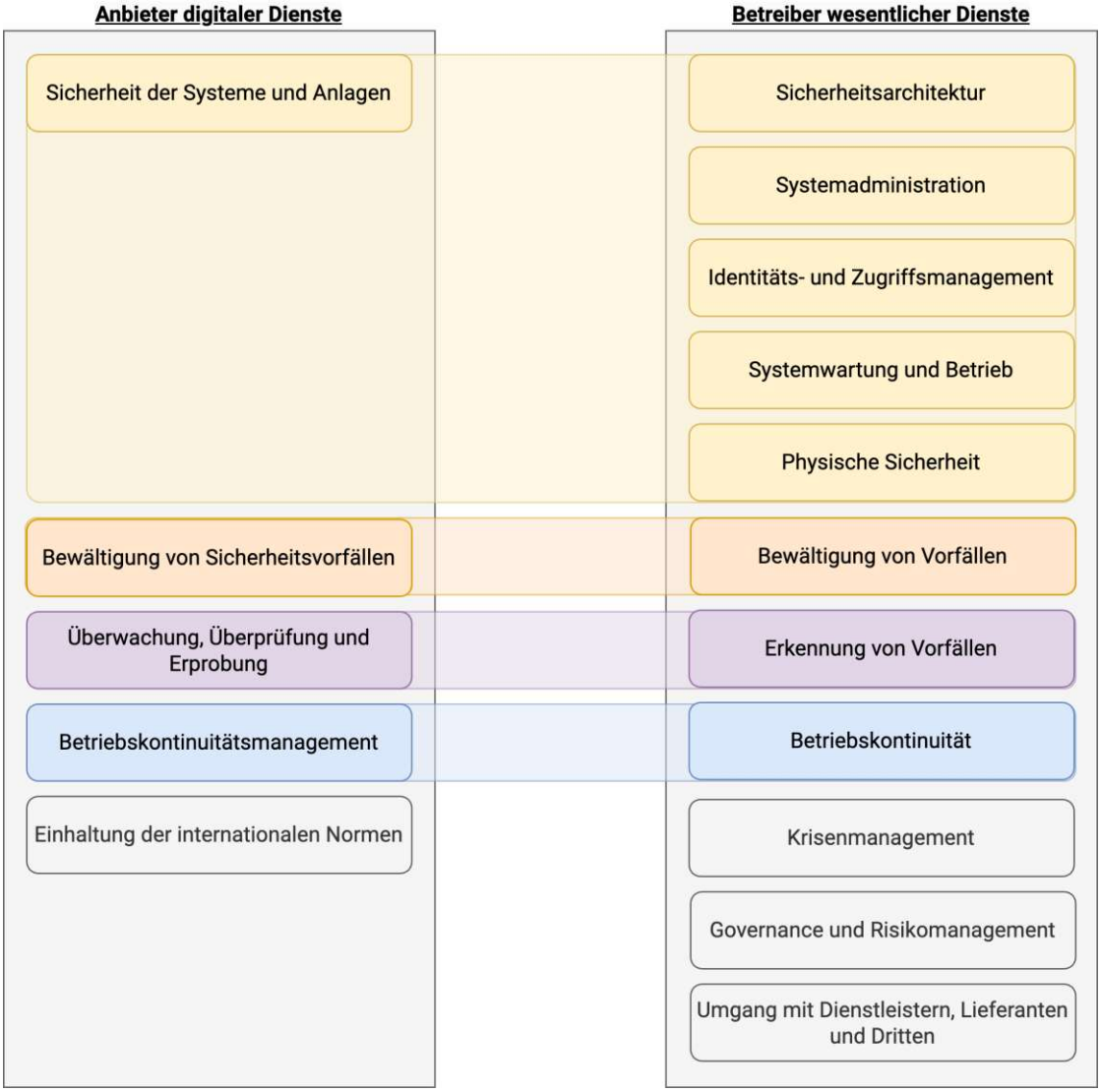

Abbildung 4.3: Vergleich von Sicherheitsmaßnahmen zwischen Betreibern wesentlicher Dienste und Anbietern digitaler Dienste (basierend auf *Netz- und Informationssystemsicherheitsverordnung*, Anlage 1 und *Durchführungsverordnung (EU) 2018/151 der Kommission vom 30. Januar 2018*, Art 1)

Für Cloud-Computing-Anbieter sind Überprüfungen durch QUASTEn nur sekundär relevant, da sie als Anbieter digitaler Dienste nicht erfasst sind. Jedoch können ihre Kund:innen Betreiber wesentlicher Dienste sein, und damit auch Teile des Cloud-Computing-Anbieters auditiert werden.

Eine Auflistung von QUASTEn stellt der BMI Betreibern wesentlicher Dienste zur

Verfügung[83]. Eine offizielle und öffentlich zugängliche Liste findet sich nicht. Bei einer Internetrecherche geben jedoch elf Unternehmen auf ihrer Homepage an, eine QUASTE in allen Kategorien im Sinne des NISG zu sein.

4.1.5 Bericht des Rechnungshofes

Im Bericht „Koordination der Cyber–Sicherheit“ hat der österreichische Rechnungshof im Jahr 2021 – also zur Zeit der Anwendbarkeit des NISG – die Koordination der Cyber–Sicherheit in der Bundesverwaltung untersucht[84]. Dabei wurde angemerkt, dass nicht alle Bundesministerien notwendige Audits durchgeführt haben und es wird eine Regelmäßigkeit, ähnlich zu Betreibern wesentlicher Dienste, von drei Jahren empfohlen[85]. Nachdem derartige Vorgaben sich nicht im Entwurf zum NISG 2024 finden, wurde dieser Punkt wohl auch zukünftig zumindest vom Gesetzgeber nicht erfasst. Der Rechnungshof kritisierte, dass die operative NIS–Behörde im Innenministerium keine Klassifizierung von Sicherheitsvorfällen nutzt[86]. Damit besteht insbesondere die Gefahr, dass beim Einsatz desselben Public Cloud-Services durch viele beaufsichtigte Einrichtungen die NIS-Behörde im Falle vieler gleichzeitiger Meldungen zum selben Vorfall beim Cloud-Service, ohne entsprechende Klassifizierung, nur schwer den Überblick behält. Im Zuge der wirkungsorientierten Folgeabschätzung zum Entwurf des NISG wurden deutlich mehr Vollbeschäftigungsäquivalente geplant, als im Jahr 2021 tatsächlich eingesetzt wurden[87]. So ergibt sich eine Differenz der Vollbeschäftigungsäquivalente von 5,3 im Bundeskanzleramt und 16 im Innenministerium[88]. Beide hielten fest, dass die Personalressourcen für einen optimalen Vollzug des NISG nicht ausreichend waren[89]. Folglich könnten sich durch diese unzureichende Besetzung Sicherheitsgefahren für Österreich ergeben und vom NISG adressierte Einrichtungen werden möglicherweise nicht mit dem gebotenen Nachdruck zur Beachtung angehalten.

4.2 Richtlinie (EU) 2022/2555 (NISR2) über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NISR2)

Ende des Jahres 2022 trat die Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NISR2) in Kraft und löste damit die Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NISR) ab.

[83] *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*, §18 Abs 4.
[84] Rechnungshof Österreich, *Koordination der Cyber–Sicherheit*, S. 9.
[85] Ebd., S. 32.
[86] Ebd., S. 75.
[87] Ebd., S. 92.
[88] Ebd., S. 92.
[89] Ebd., S. 92.

Zweitere wurde durch die europäischen Mitgliedstaaten sehr unterschiedlich umgesetzt, teils sogar mit widersprüchlichen Regeln[90]. Folglich wurde damit die grenzüberschreitende Erbringung von Diensten erschwert. Diese Probleme sollen mit der NISR2 behoben werden[91]. Ferner sollen Defizite bei der Unterscheidung von Anbietern digitaler Dienste und Betreibern wesentlicher Dienste korrigiert werden[92]. Die Anzahl der erfassten Einrichtungen wurde durch NISR2 massiv erweitert. Beim Verfassen dieses Kapitels ist Österreich gerade in einer Übergangszeit zwischen der NISR und der NISR2.

4.2.1 Wesentliche und wichtige Einrichtungen

NISR2 unterscheidet weniger granular als die Vorgängerrichtlinie und damit nur noch zwischen wesentlichen und wichtigen Einrichtungen. Als Ersteres definiert sind *große* Unternehmen, die in den folgenden Sektoren tätig sind:

1. *Energie*
2. *Verkehr*
3. *Bankwesen*
4. *Finanzmarktinfrastrukturen*
5. *Gesundheitswesen*
6. *Trinkwasser*
7. *Abwasser*
8. *Digitale Infrastruktur*
9. *Verwaltung von IKT-Diensten (Business-to-Business)*
10. *öffentliche Verwaltung*
11. *Weltraum*

(Obenstehende Aufzählung vollständig übernommen aus *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Anhang 1)

Erläuternd sei dabei angemerkt, dass große Unternehmen die Definitionsbestimmungen von mittelgroßen Unternehmen übersteigen. Mittelgroße Unternehmen beschäftigen unter 250 Personen und erwirtschaften entweder einen Jahresumsatz von höchstens 50 Millionen Euro oder haben eine Jahresbilanzsumme von höchstens 43 Millionen Euro[93]. Mittelgroße Unternehmen, die in den zuvor angeführten Sektoren tätig sind, gelten als wichtige

[90] *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, ErwGr 4.
[91] Ebd., ErwGr 5.
[92] Ebd., ErwGr 6.
[93] *Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen*, Art 1 Z 1.

Einrichtungen[94]. Im Vergleich zur NISR wurde die Liste um *Abwasser*, *Verwaltung von IKT-Diensten* und *Weltraum* erweitert. Die öffentliche Verwaltung hatte in der alten NISR einen Sonderstatus, da für sie spezielle Anforderungen galten. Sie war aber grundsätzlich bereits erfasst. Ferner gelten nun mittlere und große Unternehmen in folgenden Sektoren als wichtige Einrichtungen:

1. *Post- und Kurierdienste*
2. *Abfallbewirtschaftung*
3. *Produktion, Herstellung und Handel mit chemischen Stoffen*
4. *Produktion, Verarbeitung und Vertrieb von Lebensmitteln*
5. *Verarbeitendes Gewerbe/Herstellung von Waren*
6. *Anbieter digitaler Dienste*
7. *Forschung*

(Obenstehende Aufzählung vollständig übernommen aus *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Anhang 2)

Daneben gelten größenunabhängig DNS-Diensteanbieter, qualifizierte Vertrauensdiensteanbieter, TLD-Namenregister oberster Stufe, Einrichtungen der öffentlichen Verwaltung der Zentralregierung und mittelgroße Anbieter öffentlicher elektronischer Kommunikationsnetze/Dienste als wesentliche Einrichtungen[95]. Mitgliedstaaten können eine Einstufung nach NISR in der Kategorie „wesentlich“ für eine Einrichtung auch nach NISR2 beibehalten[96]. Cloud-Computing-Dienste finden sich im Sektor *Digitale Infrastruktur* konkret angeführt und sind nur bei entsprechender Unternehmensgröße (mittel oder groß) als wesentlicher Dienst betroffen. Sie müssen sich also den strengeren Regeln unterwerfen. Ferner können Unternehmen – auch kleinere Cloud-Anbieter – indirekt über die Lieferkette von der NISR2 betroffen sein[97].

4.2.2 Mindestmaßnahmen und Durchsetzung

NISR2 fordert von den Mitgliedstaaten sicherzustellen, dass wichtige und wesentliche Einrichtungen die Risiken für die Sicherheit der Netz- und Informationssysteme minimieren, indem sie entsprechende Maßnahmen umsetzen. NISR2 definiert folgende Mindestmaßnahmen:

a) *Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme*

[94] *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 2 Z 3.
[95] Ebd., Art 2 Abs 2 und Art 3 Abs 1.
[96] Ebd., Art 3 Abs 1 lit g.
[97] Ebd., Art 21 Abs 2 lit d.

b) Bewältigung von Sicherheitsvorfällen

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement

d) Sicherheit der Lieferkette, einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit

h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung

i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen

j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

(Obenstehende Aufzählung vollständig übernommen aus *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 21 Abs 2)

Im Gegensatz zu den in Österreich bereits bestehenden Anforderungen aus dem NISG und der NISV für Betreiber wesentlicher Dienste sind mit der NISR2 insbesondere die geforderten Schulungen für Cybersicherheit, gesicherte Kommunikation, die Multi-Faktor-Authentifizierung/kontinuierliche Authentifizierung – in den NIS Fact Sheets war erst vom „Vorantreiben“ die Rede – und Notfallkommunikationssysteme neu. Überdies soll es für betroffene Einrichtungen Meldepflichten bei erheblichen Sicherheitsvorfällen an ihr Computer Security Incident Response Team bzw. Computer-Notfallteam (CSIRT) oder an die zuständige Behörde geben[98]. Ein Sicherheitsvorfall ist dabei eine Beeinträchtigung von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Daten innerhalb eines Netz- und Informationssystems ist[99]. Zu einem „erheblichen Sicherheitsvorfall“ nach NISR2 kommt es bei schwerwiegenden Betriebsstörungen oder wenn durch den Vorfall finanzielle Verluste für die betroffene Einrichtung entstehen[100]. Auch erhebliche Schäden

[98] *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 23 Abs 1.

[99] Ebd., Art 6 Abs 6.

[100] Ebd., Art 23 Abs 3.

bei anderen natürlichen/juristischen Personen sind dabei erfasst[101]. Schon die bloße Möglichkeit des Schadens ausreicht, um eine Meldepflicht auszulösen, unabhängig davon, ob er wirklich eingetreten ist[102]. Durch das Erfassen von gar nicht wirklich eingetreten Vorfällen in der NISR2 scheint die Meldepflicht hier recht uferlos und in der Praxis schwer beurteilbar.Bei Cloud-Computing Diensten ist es für Kund:innen oft nicht transparent, ob es zu einem Sicherheitsvorfall hätte kommen können, beispielsweise aufgrund von neu veröffentlichten Schwachstellen in eingesetzten Systemen, da die dahinterliegenden Technologien für die Dienstkonsument:innen nicht einsehbar sind. Besonders bei Verletzungen der Vertraulichkeit von Daten ist es für kritische Einrichtungen, die Informationssysteme an Dritte ausgelagert haben, nicht überprüfbar, ob ein Datenabfluss in andere als dafür vorgesehene Richtungen erfolgt ist.

Die Sicherheit der Lieferketten bestimmter kritischer IKT-Produkte, -Dienste oder -Systeme kann durch dafür vorgesehene Organisationen (Kooperationsgruppe, ENISA und EK) risikobewertet werden[103]. Mitgliedstaaten sollen sicherstellen, dass wesentliche und wichtige Einrichtungen diese Risikobewertung berücksichtigen müssen[104]. Folglich könnte eine negative Bewertung dazu führen, dass bestimmte Cloud-Dienste von wesentlichen und wichtigen Einrichtungen nicht mehr genutzt werden dürfen. Überdies können wesentliche und wichtige Einrichtungen von Mitgliedstaaten zur Verwendung von zertifizierten (nach den europäischen Schemata für Cybersicherheitszertifizierung – siehe Abschnitt 4.3) IKT-Diensten, -Produkten oder -Prozessen verpflichtet werden[105]. Damit kann ebenfalls die Wahl von Cloud-Computing Anbietern für betroffene Unternehmen eingeschränkt werden und damit eventuell auch die Wettbewerbsfähigkeit im internationalen Vergleich.

Für einen Überblick und Vergleich zu den in der NISR2 vorgesehenen Aufsichts- und Durchsetzungsmaßnahmen zwischen wesentlichen und wichtigen Einrichtungen siehe Abbildung 4.4. Ein grundlegender Unterschied bei den Maßnahmen ist der nachträgliche und gezielte Charakter bei wichtigen Einrichtungen[106]. Die Maßnahmen für wesentliche Einrichtungen sollen eher von Regelmäßigkeit und Proaktivität gekennzeichnet sein[107].

Eine besondere Pflicht trifft TLD-Namenregister und Domänennamen-Registrierungsdienste, diese müssen Kontakt- und Metainformationen von Domäneinhaber:innen bzw. der betroffenen Domäne sammeln[108]. Um die Genauigkeit und Vollständigkeit der Daten zu gewährleisten, müssen die Mitgliedstaaten sicherstellen, dass Registrierungsdienste Überprüfungsverfahren etablieren und diese Verfahren veröffentlichen[109]. Ferner müssen nicht personenbezogene Daten zu den Domänen öffentlich einsehbar sein[110].

[101] Ebd., Art 23 Abs 3.
[102] Ebd., Art 23 Abs 3.
[103] Ebd., Art 22.
[104] Ebd., Art 21 Abs 3.
[105] Ebd., Art 24 Abs 1.
[106] *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 33.
[107] Ebd., Art 32.
[108] Ebd., Art 28 Abs 1.
[109] Ebd., Art 28 Abs 2.
[110] Ebd., Art 28 Abs 4.

Abbildung 4.4: Vergleich von Aufsichts- und Durchsetzungsmaßnahmen zwischen wesentlichen und wichtigen Einrichtungen (basierend auf *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 32 und Art 33)

Die in der NISR2 definierten Maßnahmen stellen nur eine Untergrenze dar. Nationale Gesetzgeber können auch strengere oder detailliertere Anforderungen verlangen[111]. Die Mitgliedstaaten der EU haben bis 17. Oktober 2024 Zeit, die Umsetzungsregelungen zur Richtlinie zu erlassen und müssen sie ab dem 18. Oktober 2024 anwenden[112].

4.2.3 Entwurf für einen Durchführungsrechtsakt zur NISR2

Im Juni 2024 wurde der Entwurf der EK für einen Durchführungsrechtsakt zur NISR2 veröffentlicht[113]. Darin wurden technische und methodische Anforderungen nach der NISR2 dargelegt und spezifiziert, welche Vorfälle als signifikant gelten[114]. Der Rechtsakt nimmt Bezug auf folgende Dienste:

1. *DNS-Diensteanbieter*

[111] *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 32 und Art 33.
[112] Ebd., Art 41.
[113] *DRAFT - COMMISSION IMPLEMENTING REGULATION (EU) laying down rules for the application of Directive (EU) 2022/2555*.
[114] Ebd., Art 1.

2. *TLD-Namenregister*
3. *Cloud-Computing Dienstanbieter*
4. *Rechenzentrumsdienstanbieter*
5. *CDN-Anbieter*
6. *Managed Service Dienstleister*
7. *Managed Security Dienstleister*
8. *Online-Marktplätze*
9. *Suchmaschinen*
10. *Soziale Netzwerke*
11. *Vertrauensdiensteanbieter*

(Obenstehende Aufzählung vollständig übernommen und übersetzt aus *DRAFT - COMMISSION IMPLEMENTING REGULATION (EU) laying down rules for the application of Directive (EU) 2022/2555*, Art 1)

Im Hinblick auf signifikante Vorfälle wurden generelle Kriterien festgelegt, wie finanzieller Verlust von mindestens 100.000 EUR oder mindestens 5 % Jahresumsatz, Reputationsschaden, Exfiltration von Geschäftsgeheimnissen, potenziell oder wirklich eingetretener Todesfall oder Gesundheitsschaden einer Person, erfolgreicher vermutlich böswilliger Zugriff auf Netz- und Informationssysteme[115] oder auch wenn der Sicherheitsvorfall öfter als zweimal in den vergangenen sechs Monaten aufgetreten ist oder mehrere Vorfälle dieselbe Ursache haben[116]. Für die zuvor aufgezählten Bereiche wurden ferner spezielle Anforderungen an die Meldepflichten definiert. So sind für Cloud-Computing-Dienstleister vollständige Ausfälle eines Services für mehr als zehn Minuten bereits signifikante Sicherheitsvorfälle[117], was jedoch etwas praxisfern wirkt, da Cloud-Dienstleister wohl auch nicht zeitkritische Services anbieten. Es kann auch SLAs mit Kunden geben, wo deutlich größere Schwellenwerte vereinbart wurden, eben weil Kund:innen keine entsprechend hohe Verfügbarkeit benötigen. Die Zehn-Minuten-Grenze findet sich ebenso in den Vorgaben für die anderen genannten Dienstleister. Wenn es zu einer SLA-Verletzung kommt, müssen 5 % oder mehr als eine Million Benutzer:innen in der EU für eine Dauer von mehr als einer Stunde betroffen sein, damit ein signifikanter Sicherheitsvorfall vorliegt[118]. Selbiges gilt im Fall von fehlenden SLAs bei Verfügbarkeitsbeeinträchtigungen[119]. Bei Verletzungen von Integrität, Vertraulichkeit oder Authentizität aufgrund vermuteter böswilliger Aktionen oder mehr als 5 % Betroffenen in der EU liegt ebenso ein signifikanter Sicherheitsvorfall vor[120].

[115] Ebd., Art 3 Abs 1.
[116] Ebd., Art 4.
[117] Ebd., Art 7 lit a.
[118] Ebd., Art 7 lit b.
[119] Ebd., Art 7 lit c.
[120] Ebd., Art 7 lit c.

4.3 Verordnung (EU) 2019/881 über die ENISA und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (CSA)

Mit der Verordnung (EU) 2019/881 über die ENISA und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (CSA) wurde die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) sowie die Europäische Gruppe für Cybersicherheitszertifizierung (ECCG) eingesetzt[121]. Erstere soll Mitgliedstaaten, Organe und Einrichtungen der Union beim Thema Cybersicherheit unterstützen, um damit die Cybersicherheit insgesamt zu erhöhen[122]. Darüber hinaus soll auch jeder Mitgliedstaat in seinem Hoheitsgebiet nationale Behörden für die Cybersicherheitszertifizierung benennen, die für die jeweilige Aufsicht zuständig sind[123]. In Österreich soll die Rolle dieser nationalen Behörde entsprechend dem Ministerialentwurf betreffend Bundesgesetz zur Einrichtung einer nationalen Behörde für die Cybersicherheitszertifizierung - Cybersicherheitszertifizierungs-Gesetz (CSZG) der Bundeskanzler wahrnehmen[124]. Die ECCG soll eine beratende Rolle einnehmen und Stellungnahmen zu den Entwürfen der Schemata der ENISA abgeben[125].

Ein weiteres Ziel von CSA ist die Beauftragung der ENISA mit der Erstellung und Evaluation möglicher europäischer Schemata für die Cybersicherheitszertifizierung von IKT-Prozessen, -Diensten und -Produkten[126]. Nationale Schemata für Cybersicherheitszertifizierung, die schon von einem europäischen Schema erfasst sind, werden damit abgelöst[127]. Diese Schemata finden auch in europäischen Regulativen direkte Anwendung, beispielsweise in NISR2 (siehe Abschnitt 4.2). Wesentliche und wichtige Einrichtungen können verpflichtet werden, zertifizierte IKT-Produkte, -Dienste und -Prozesse zu verwenden[128]. Eine solche Zertifizierung ist das Cybersecurity-Zertifizierungsschema der Europäischen Union (EUCC), das mit der Durchführungsverordnung (EU) 2024/482 in Kraft gesetzt wurde und mit 27. Februar 2025 gelten wird[129]. EUCC gilt insbesondere für IKT-Produkte wie Hardware, Software und Komponenten[130]. Daneben wird an einem Entwurf mit dem Titel European Cybersecurity Certification Scheme for 5G (EU5G)

[121] *Verordnung (EU) 2019/881 über die ENISA und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik*, Art 1 Abs 1 und Art 62 Abs 1.
[122] Ebd., Art 3 Abs 1.
[123] Ebd., Art 58 Abs 1.
[124] *Ministerialentwurf Gesetz: Bundesgesetz zur Einrichtung einer nationalen Behörde für die Cybersicherheitszertifizierung (Cybersicherheitszertifizierungs-Gesetz – CSZG)*, §2 Abs 1.
[125] *Verordnung (EU) 2019/881 über die ENISA und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik*, Art 62 Abs 4.
[126] Ebd., Art 8 Abs 1.
[127] Ebd., Art 57.
[128] *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 24 Abs 1.
[129] *Durchführungsverordnung (EU) 2024/482 mit Durchführungsbestimmungen zur Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates hinsichtlich der Annahme des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC)*, Art 50.
[130] *Developing Certification Schemes - European Union.*

gearbeitet, der auf 5G-Technologie ausgerichtet ist, aber aktuell nicht veröffentlicht ist[131]. Ein bereits veröffentlichter Entwurf ist das Cloud Services Schema (EUCS), das sich besonders an Cloud-Dienste richtet[132]. In jenem Schema sollen sich Cloud-Anbieter in den Assurance Levels „Basic“, „Substantial“ und „High“ zertifizieren können[133]. Eine Selbstbewertung, wie es die CSA möglich macht, soll es in EUCS nicht geben[134]. In folgenden Kategorien schreibt das EUCS Maßnahmen vor:

1. *Organisation of Information Security*
2. *Information Security Policies*
3. *Risk Management*
4. *Human Resources*
5. *Asset Management*
6. *Physical Security*
7. *Operational Security*
8. *Identity, Authentication and Access Control Management*
9. *Cryptography and Key Management*
10. *Communication Security*
11. *Portability and Interoperability*
12. *Change and Configuration Management*
13. *Development of Information Systems*
14. *Procurement Management*
15. *Incident Management*
16. *Business Continuity*
17. *Compliance*
18. *User Documentation*
19. *Dealing with Investigation Requests from Government Agencies*
20. *Product Security*

(Obenstehende Aufzählung vollständig übernommen aus den Kategorien „SECURITY OBJECTIVES AND REQUIREMENTS FOR CLOUD SERVICES“ *EUCS – Cloud Services Scheme*, Annex A)

[131] Ebd.
[132] Ebd.
[133] *EUCS – Cloud Services Scheme*, S. 19.
[134] Ebd., S. 27.

Besonders interessant ist dabei Punkt 11 „Portability and Interoperability“, der vertragliche Vereinbarungen vorschreibt, wie die Migration von Daten bei einer Beendigung des Vertrages mit dem Cloud-Anbieter vonstattengeht[135], also gerade im Hinblick auf Vendor Lock-in. Ähnliche Vorgaben finden sich nur in DORA[136], nicht aber in NISR2 oder NISR. Ferner gibt es für das Löschen von Daten ab Assurance Level „Substantial“ das Erfordernis, dass Daten auch durch forensische Maßnahmen nicht wiederherstellbar sein sollen[137]. Das EUCS lässt offen, was genau unter forensischen Maßnahmen zu verstehen ist. Für Assurance Level „Basic“ könnten demzufolge die zu löschenden Daten gegebenenfalls wiederherstellbar sein.

Das EUCS ist eine umfangreiche Sammlung von teils konkreten Anforderungen und auch detailreicher als europäische Regulative im Zusammenhang mit Informationssicherheit für kritische Infrastruktur. Unbekannt ist, wann, ob und in welcher Form das EUCS das Entwurfsstadium verlässt. Aktuell ist der nächste Schritt, dass die ECCG eine Meinung dazu abgeben soll, danach kommt der Entwurf zur EK[138].

4.4 Verordnung (EU) über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (CRV)

Mit 10. Dezember 2024 ist der Verordnung (EU) über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (CRV) in Kraft getreten und ist ab 11. Dezember 2027 anwendbar[139]. Die Verordnung ist auch unter dem Namen Cyber Resilience Act (CRA) bekannt.

Die CRV sieht vor, dass Produkte mit digitalen Elementen nur am Markt bereitgestellt werden dürfen, wenn sie bestimmte Anforderungen erfüllen[140]. Dabei wird zwischen nicht kritischen und kritischen Produkten unterschieden, wobei es für letztere Klasse I und II gibt[141]. Die Zuordnung von Produkten erfolgt gemäß Anhang III der CRV. Die von Cloud-Anbietern eingesetzten Technologien würden wohl zu einem großen Teil unter die erfassten Produktkategorien (z.B. „Hypervisoren und Container-Runtime-Systeme“, „Allzweck-Mikroprozessoren“, „Betriebssysteme für Server“) fallen und folglich damit die Anforderung der Verordnung erfüllen müssen. Bis auf wenige Ausnahmen sind SaaS-Dienste allerdings von CER explizit nicht erfasst[142]. Die grundlegenden Sicherheitsanforderungen der CRV spalten sich in zwei Teile, nämlich einerseits in Bezug auf die

[135] *EUCS – Cloud Services Scheme*, S. 126.
[136] *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 30 Abs 3 lit f.
[137] *EUCS – Cloud Services Scheme*, S. 127.
[138] *Developing Certification Schemes - European Union.*
[139] Directorate-General for Communications Networks und Technology, *Cyber Resilience Act.*
[140] *Vorschlag für eine VERORDNUNG über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen*, Art 6.
[141] Ebd., Art 6 Abs 1.
[142] Ebd., ErwGr 9.

Eigenschaften der Produkte und andererseits in Bezug auf die Behandlung von Schwachstellen[143]. Letztere müssen innerhalb der Produktlebensdauer oder während fünf Jahren ab Inverkehrbringen (wobei jeweils die kürzere Dauer gilt) entsprechend der Verordnung behandelt werden[144]. Jene Schwachstellen müssen vom Hersteller, sobald er über deren aktive Ausnutzung oder deren Auswirkungen auf die Produktsicherheit Kenntnis erlangt hat, innerhalb 24 Stunden an die ENISA gemeldet werden[145]. Die EK kann Kategorien hochkritischer Produkte mit digitalen Elementen festlegen, für die ein europäisches Cybersicherheitszertifikat erlangt werden muss, insbesondere wenn diese Produkte von wesentlichen Einrichtungen nach NISR2 verwendet werden oder abhängig davon sind[146]. Für Hersteller besteht folglich die Gefahr, von dieser Zertifizierungspflicht erfasst zu werden, selbst wenn nur ein sehr kleiner Teil ihrer Kunden wesentliche Einrichtungen sind.

Mit den Anforderungen der CRV können jedoch nur einzelne Teile der Regulative für kritische Infrastrukturen, die unter NISR, NISR2 oder DORA fallen, abgedeckt werden. Damit ist es für eine von den genannten Regulativen erfassten Einrichtung wohl nicht ausreichend, sich auf eine derartige Zertifizierung bei eigenen oder ausgelagerten IT-Systemen zu berufen. Die Anforderungen der CRV könnten jedoch helfen, Risikomanagementanforderungen aus der NISR2 im Hinblick auf Lieferketten zu erfüllen[147].

4.5 Begutachtungsentwurf Netz- und Informationssystemsicherheitsgesetz 2024 (NISG 2024)

Am 03.04.2024 begann die Begutachtungsfrist für das Netz- und Informationssystemsicherheitsgesetz 2024 (NISG 2024) und diese endete am 01.05.2024[148]. Mit dem NISG 2024 soll die Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NISR2) in österreichisches nationales Bundesrecht umgesetzt werden[149]. Ein konkreter Zeitplan für das Inkrafttreten des Entwurfs findet sich nicht. Nachdem der Entwurf Änderungen unterworfen sein kann, wird als Stichtag zur Betrachtung für diese Arbeit der 1. Mai 2024 festgelegt. Es wird in diesem Kapitel auf Besonderheiten im Vergleich zur NISR2 eingegangen (für einen detaillierten Einblick zu NISR2 siehe Abschnitt 4.2).

Wesentliche oder wichtige Unternehmen können zusätzlich per Bescheid durch die Cybersicherheitsbehörde größenunabhängig eingestuft werden (sofern bestimmte Kriterien

[143] Ebd., Anhang 1.
[144] Ebd., Art 10 Abs 6.
[145] Ebd., Art 11 Abs 1.
[146] Ebd., Art 6 Abs 2.
[147] Eckhardt und Kotovskaia, „The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive", S. 163.
[148] *RIS - NISG 2024 - Begutachtungsentwürfe.*
[149] *Begutachtungsentwurf: Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024)*, §48 1.

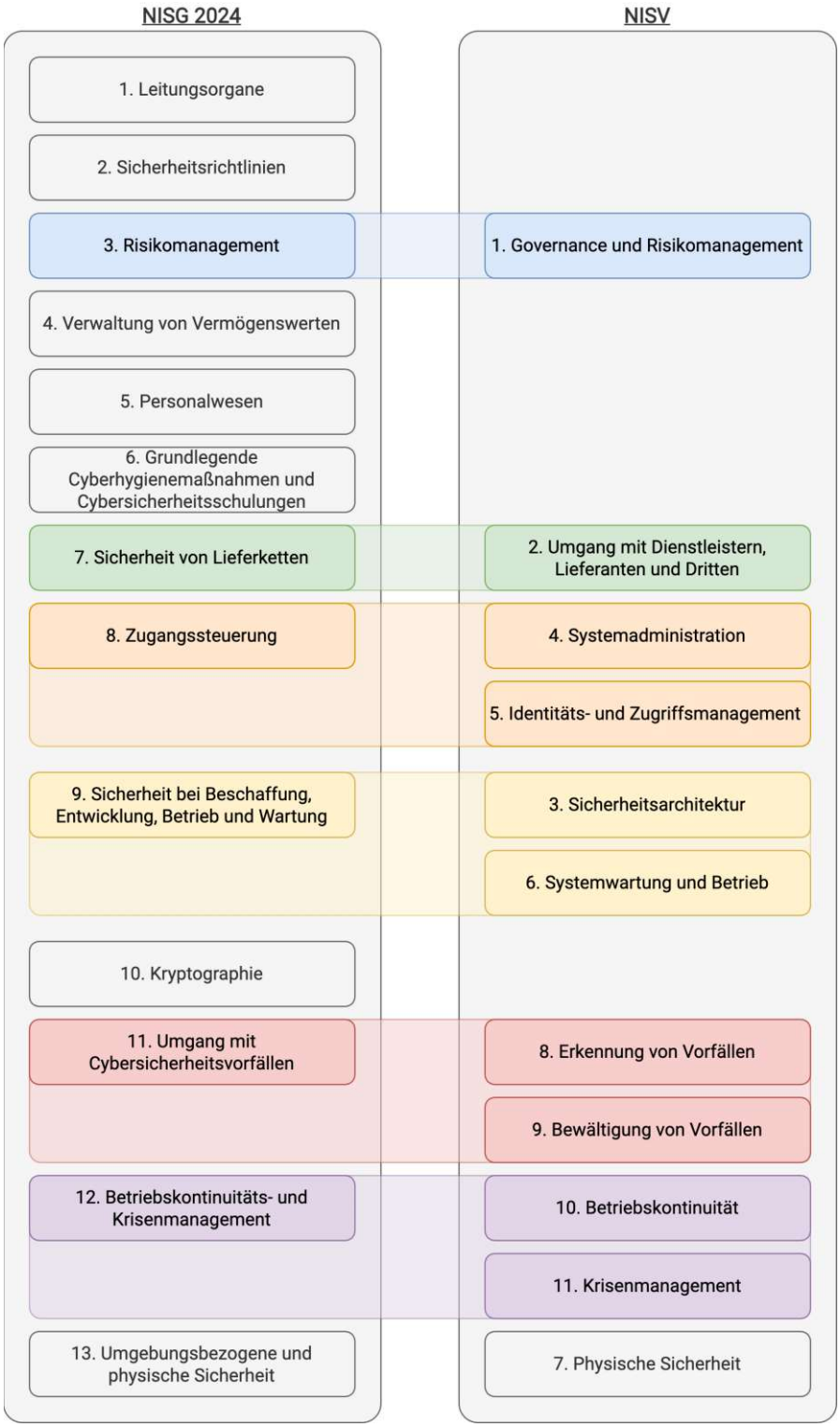

Abbildung 4.5: Gegenüberstellung Risikomanagementmaßnahmen nach NISG 2024 und Sicherheitsmaßnahmen nach NISV (basierend auf *Anlage 3 - Begutachtungsentwurf: Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024)* und *Netz- und Informationssystemsicherheitsverordnung*, Anlage 1)

erfüllt sind)[150], auch wenn sie nach NISR2 eigentlich nicht erfasst oder anders eingestuft wären. Wenn Einrichtungen vom NISG 2024 betroffen sind, aber durch sektorspezifische unionsrechtliche Rechtsakte ein gleichwertiges Cybersicherheitsniveau benötigen, ersetzen diese die Bestimmungen des NISG 2024 für die jeweilige Einrichtung, allerdings nur, wenn die Gleichwertigkeit durch den BMI mittels Verordnung festgelegt wurde[151].

4.5.1 Maßnahmen

Eine Gegenüberstellung der Risikomanagementmaßnahmen nach dem NISG 2024 und der Sicherheitsmaßnahmen der NISV findet sich in Abbildung 4.5. Besonders die Unterpunkte der Maßnahmen aus dem NISG 2024 (Anlage 3 NISG 2024) sind deutlich konkreter und umfangreicher als das vorhergehende NISG bzw. die begleitende Verordnung NISV. Selbiges trifft auch für die NISR2 zu (siehe Artikel 21 Absatz 2 NISR2). Beispielsweise fordert folgende Punkte NISR2 nicht explizit, wohl aber NISG 2024:

- *Schutz vor umgebungsbezogenen Gefährdungen*
- *Schutz vor bösartiger und unautorisierter Software*
- *Sichere Softwareentwicklung*
- *Lieferantenverzeichnis*
- *Hintergrundüberprüfung*

(Obenstehende Aufzählung übernommen aus *Anlage 3 - Begutachtungsentwurf: Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024)*)

Folglich kann von einer Übererfüllung der europäischen Richtlinie durch den österreichischen Gesetzgeber gesprochen werden. Besonders das geforderte Lieferantenverzeichnis und die Hintergrundüberprüfung kann für den Public Cloud-Betrieb relevant sein. So wären auch beim Personal von Cloud-Anbietern Hintergrundüberprüfungen durchzuführen.

Verwaltungsstrafbestimmungen, die in §45 NISG 2024 festgelegt sind (Geldstrafen bis zu 10.000.000 EUR oder bis zu 2 % des weltweiten Umsatzes für wesentliche Einrichtungen bzw. bis zu 7.000.000 EUR oder bis zu 1,4 % für wichtige Einrichtungen), gelten nicht für Einrichtungen der öffentlichen Verwaltung[152]. Allerdings hat die Bezirksverwaltungsbehörde bei nicht fristgerechter Einhaltung durch eine Stelle der öffentlichen Verwaltung, einen möglichst breiten Personenkreis darüber zu informieren[153].

[150] *Begutachtungsentwurf: Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024)*, §26 Abs 1.
[151] Ebd., §27 Abs 1.
[152] Ebd., §45 Abs 5.
[153] Ebd., §46 Abs 2.

Umsetzungsempfehlungen

In einer wissenschaftlichen Veröffentlichung aus dem Jahr 2023 zur NISR2 mit dem Titel „The outcome efficacy of the entity risk management requirements of the NIS 2 Directive“ wurden folgende Punkte identifiziert, die für einen sinnvollen Schutz in eine nationale Umsetzung Eingang finden sollten:

1. *Bewertung des Aufklärungsbedarfs*
2. *Schwachstellenscans der internen Ressourcen*
3. *Tiefgehende Penetationstests*
4. *Überprüfungen interner und externer Bedrohungsdaten*
5. *Bedrohungsmodellierung*

(Obenstehende Aufzählung übernommen und übersetzt aus Ferguson, „The outcome efficacy of the entity risk management requirements of the NIS 2 Directive“, S. 384)

Im Hinblick auf Punkt 2 und Punkt 3 können diese Aspekte mit den in Anlage 3 NISG 2024 genannten Maßnahmen („Sicherheitstests“ und eventuell „Umgang mit Schwachstellen und deren Offenlegung“) als abgedeckt betrachtet werden. Die anderen Punkte scheinen selbst bei weitreichender Interpretation nicht erfasst zu sein.

4.5.2 Ausblick

Entsprechend einer Parlamentskorrespondenz zur 270. Sitzung des Nationalrats vom 3. Juli 2024 wollten die Regierungsparteien Österreichische Volkspartei (ÖVP) und Grüne das NISG 2024 beschließen, erreichten jedoch nur eine einfache Mehrheit und keine aufgrund von betroffenen Verfassungsbestimmungen notwendige Zweidrittelmehrheit[154]. Nennenswert sei hier jene Verfassungsbestimmung, die festlegt, dass auch Vorgaben des NISG 2024 Bundessache sind, für die das Bundes-Verfassungsgesetz (B-VG) etwas anderes bestimmt[155] und folglich nicht Bundeskompetenz wären. Ferner ist die Feststellung der Nichteinhaltung der Verpflichtungen durch öffentliche Stellen und deren Sanktionierung (in Form von Veröffentlichung) als Verfassungsbestimmung ausgewiesen[156]. Es hätte dazu entsprechend der Mandatsverteilung[157] die Stimmen der SPÖ oder FPÖ benötigt. Kritisiert am Entwurf wurde von der SPÖ, dass das Innenministerium zu viel Macht

[154] Parlament Österreich, *Nationalrat: Absage für Informationssystemsicherheitsgesetz (PK0785/04.07.2024)*.

[155] *Begutachtungsentwurf: Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024)*, §1 Abs 1.

[156] Parlament Österreich, *Nationalrat: Absage für Informationssystemsicherheitsgesetz (PK0785/04.07.2024)*, §46 Abs 2.

[157] Parlament Österreich, *Informationen über den Nationalrat*.

ohne Kontrolle bekäme und eine Vorratsdatenspeicherung zu befürchten sei[158]. Die FPÖ führte aus, dass sie aufgrund der fehlenden Einbindung der Opposition nicht zustimme und bezeichnete die Ansiedelung der nationalen Cybersicherheitsbehörde beim Innenministerium als „Konstruktionsfehler“[159].

Das Gesetz wurde nicht innerhalb der in der NISR2 festgelegten Frist (17. bzw. 18. Oktober 2024) beschlossen. Theoretisch kann Österreich bei nicht fristgerechter Umsetzung die Zahlung eines Pauschalbetrags oder eines Zwangsgelds drohen[160].

4.6 Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen (CER/RCE/RKE)

Komplementär zur Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NISR2) trat die Richtlinie (EU) 2022/2557 über Resilienz kritischer Einrichtungen (CER) – auch bekannt unter den Abkürzungen RCE bzw. RKE – in Kraft. Bei CER geht es weniger um direkte Sicherheitsmaßnahmen, sondern mehr um das Bewältigen von bzw. das Wiederherstellen der Betriebsfähigkeit nach Sicherheitsvorfällen. Die Richtlinie hat in der Definition von Resilienz auch eine gewisse Proaktivität erfasst und spricht zusätzlich von der Verhinderung und vom Schutz vor Vorfällen[161].

4.6.1 Kritische Einrichtungen

Die CER zielt konkret auf kritische Einrichtungen ab, die im Gegensatz zur NISR2 von den Mitgliedstaaten selbst ermittelt werden müssen. Dies entspricht mehr dem Charakter des NISG. Die dafür vorgesehene Frist läuft bis zum 17. Juli 2026[162]. Jene Ermittlung greift in folgenden Sektoren, die leicht von denen in der NISR2 abweichen:

1. *Energie*
2. *Verkehr*
3. *Bankwesen*
4. *Finanzmarktinfrastrukturen*
5. *Gesundheit*
6. *Trinkwasser*
7. *Abwasser*

[158] Parlament Österreich, *Nationalrat: Absage für Informationssystemsicherheitsgesetz (PK0785/04.07.2024).*
[159] Ebd.
[160] *Vertrag über die Arbeitsweise der Europäischen Union*, Art 260.
[161] *Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 2 Abs 2.
[162] Ebd., Art 6 Abs 1.

8. *Digitale Infrastruktur*
9. *öffentliche Verwaltung*
10. *Weltraum*
11. *Produktion, Verarbeitung und Vertrieb von Lebensmitteln*

(Obenstehende Aufzählung vollständig übernommen aus *Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Anhang)

Zusätzlich erbringen die ermittelten Einrichtungen zumindest einen wesentlichen Dienst, sind im betroffenen Mitgliedstaat mit kritischer Infrastruktur tätig und ein Sicherheitsvorfall hätte eine erhebliche Störung des wesentlichen Dienstes zur Folge[163]. Der Begriff wesentlicher Dienst ist in den Definitionen der CER wie folgt festgehalten:

> *„[...] [ein] Dienst, der für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, wichtiger wirtschaftlicher Tätigkeiten, der öffentlichen Gesundheit und Sicherheit oder der Erhaltung der Umwelt von entscheidender Bedeutung ist.“*[164]

Damit unterscheidet sich die Definition in der CER von der im NISG (siehe Abschnitt 4.1). Erstere ist deutlich allgemeiner gehalten und schließt im Gegensatz zum NISG explizit die Erhaltung Umwelt mit ein.

4.6.2 Maßnahmen für kritische Einrichtungen

Kritische Einrichtungen müssen mindestens im Vier-Jahres-Rhythmus alle Risiken, die Einfluss auf die Erbringung des wesentlichen Dienstes haben, bewerten[165]. Die Risiken umfassen unter anderem Naturkatastrophen, gesundheitliche Notlagen, feindliche Bedrohungen und terroristische Straftaten[166]. Die Mitgliedstaaten der EU müssen sicherstellen, dass kritische Einrichtungen Maßnahmen ergreifen, um zumindest folgende Punkte abzudecken:

a) *Verhinderung von Sicherheitsvorfällen*
b) *angemessenen physischen Schutz*
c) *Abwehr und Schadensbegrenzung von Sicherheitsvorfällen*
d) *Gewährleistung der Wiederherstellung nach Sicherheitsvorfällen*

[163] *Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 6.
[164] Ebd., Art 2 Abs 5.
[165] Ebd., Art 12.
[166] Ebd., Art 12.

> *e) Sicherheitsmanagement der Mitarbeiter, insbesondere Zuverlässigkeitsüberprüfungen*
>
> *f) Sensibilisierung des entsprechenden Personals zu den zuvor genannten Punkten unter gebührender Berücksichtigung von Schulungen, Informationsmaterial und Übungen*
>
> (Obenstehende Aufzählung vollständig bezogen und zusammengefasst aus *Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 13 Abs 1)

Ausschließlich die Zuverlässigkeitsüberprüfungen stellen eine bereits sehr konkrete Anforderung in der Richtlinie dar, im Gegensatz zu den anderen Punkten, die eher allgemeiner Natur sind. Zuverlässigkeitsüberprüfungen haben sich zumindest auf Personen zu beziehen, die sensible Funktionen erfüllen oder Zugriff auf Räumlichkeiten, Informationen oder Kontrollsystemen haben[167]. Sie sollen im Hinblick auf die Risikobewertung und in begründeten Fällen durchzuführen sein[168]. Dieser Punkt ist beim Einsatz von Cloud-Computing Diensten durch kritische Einrichtungen, die sie von Unternehmen beziehen, die nicht von der CER erfasst sind, relevant. Kritische Einrichtungen müssen sicherstellen, dass auch alle Mitarbeiter:innen des Cloud-Computing-Anbieters mit Zugriff auf kritische Komponenten einer entsprechenden Zuverlässigkeitsüberprüfung unterzogen wurden. Im Zuge einer Zuverlässigkeitsüberprüfung muss mindestens die Identität der zur prüfenden Person verifiziert werden und eine Strafregisterprüfung für Straftaten mit Relevanz für die spezifische Position ist durchzuführen[169].

Hinsichtlich der Aufsicht über kritische Einrichtungen müssen Mitgliedstaaten gewährleisten, dass die zuständigen Behörden die Möglichkeit haben, Kontrollen vor Ort vorzunehmen[170]. Zusätzlich können entsprechende Audits auferlegt werden, um die Erfüllung der Verpflichtungen zu prüfen[171]. Kritische Einrichtungen trifft auch eine Informations- und Nachweispflicht gegenüber der Behörde bezüglich der umgesetzten Maßnahmen[172]. Ferner sind sie von einer Meldepflicht bei Sicherheitsvorfällen gegenüber der Behörde erfasst[173]. Analog zur NISR2 wurden in der CER auch bloße potenzielle Störungen in diese Verpflichtung aufgenommen[174].

[167] *Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 14.
[168] Ebd., Art 14.
[169] Ebd., Art 14 Abs 3 lit a–b.
[170] Ebd., Art 21 Abs 1.
[171] Ebd., Art 21 Abs 1.
[172] Ebd., Art 21 Abs 2.
[173] Ebd., Art 15 Abs 1.
[174] Ebd., Art 15 Abs 1.

4.7 Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA)

Am 17. Jänner 2023 trat die Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA) in Kraft und sie gilt ab dem 17. Januar 2025[175]. Für einen Überblick zu DORAs zeitlichen Entwicklung siehe Abbildung 4.6. Nachdem es sich dabei im Gegensatz zur NISR und NISR2 um eine Verordnung und nicht um eine Richtlinie handelt, ist sie direkt anwendbar und muss nicht erst durch Mitgliedstaaten in nationales Recht umgesetzt werden. DORA stellt allerdings eine stärkere Harmonisierung der Anforderungen aus NISR2 dar und ist damit eine sogenannte Lex Specialis zur NISR2[176].

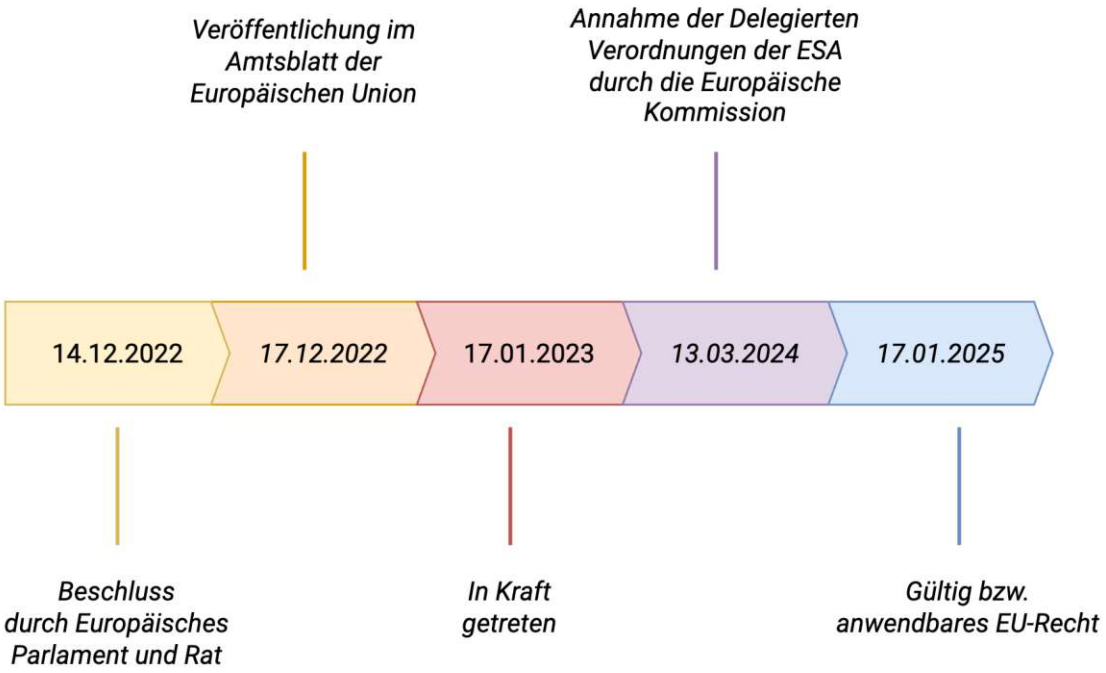

Abbildung 4.6: DORAs zeitliche Entwicklung (basierend auf *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*)

Von der Verordnung erfasst ist eine Vielzahl von Unternehmen im Finanzsektor, wie Kreditinstitute, Zahlungsinstitute, Anbieter von Krypto-Dienstleistungen, Handelsplätze, Versicherungsvermittler etc.[177]. Eine vollständige Liste findet sich in Artikel 2 von DORA.

[175] *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 64.
[176] Ebd., ErwGr 16.
[177] *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 2 Abs 1.

Für betroffene Unternehmen gibt es fünf relevante Kapitel, die zur Umsetzung der digitalen operationalen Resilienz notwendig sind (siehe Abbildung 4.7).

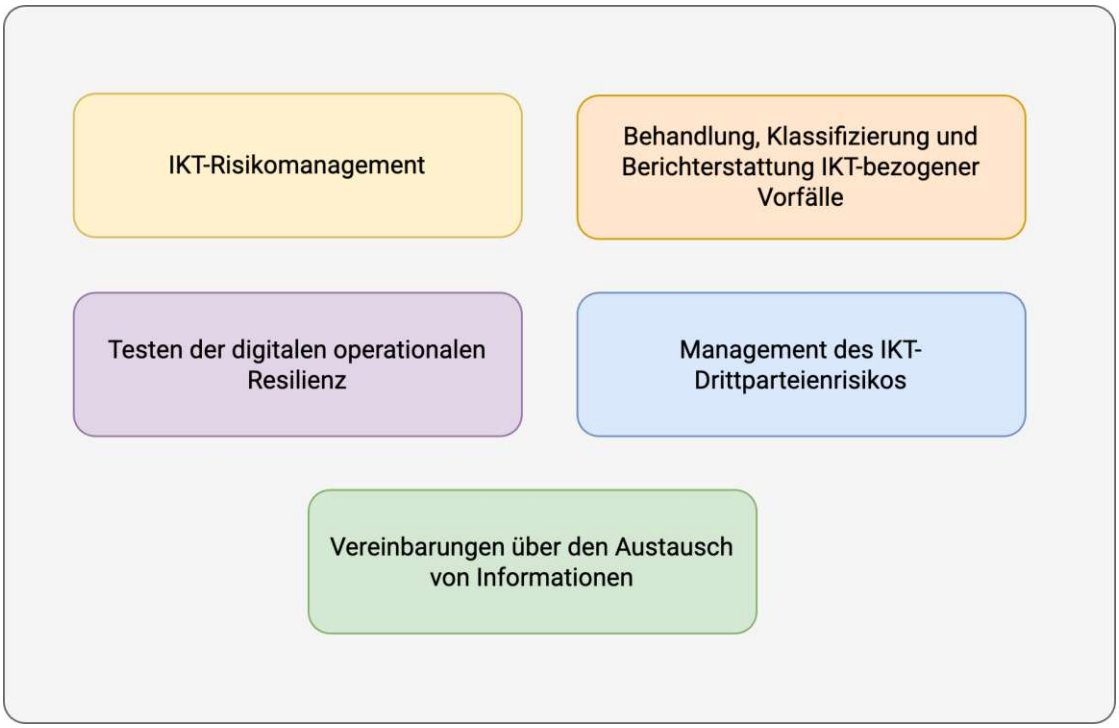

Abbildung 4.7: Für betroffene Unternehmen relevante Kapitel in DORA (basierend auf *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*)

4.7.1 IKT-Risikomanagement

Zur Überwachung von Vereinbarungen mit IKT-Drittdienstleistern (dazu zählen wohl auch Cloud-Anbieter) müssen von DORA betroffene Finanzunternehmen jemanden bestimmen, der diese Aufgabe und die entsprechende Dokumentation dazu wahrnimmt[178]. Mitglieder der Leitungsorgane müssen auch regelmäßig an speziellen Schulungen teilnehmen, damit sie einen aktuellen Kenntnisstand haben, um IKT-Risiken bewerten zu können[179]. IKT-Systeme, -Protokolle und -Tools müssen aktuell gehalten werden[180]. Diese Anforderung scheint allgemein zu gelten, unabhängig davon, ob Systeme abgeschottet betrieben werden oder fehlende Aktualität durch andere Maßnahmen mitigiert wird. Ferner sind regelmäßige (mindestens jährliche) Überprüfungen und Bewertungen der Risikoszenarien

[178] *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 5 Abs 3.
[179] Ebd., Art 5 Abs 4.
[180] Ebd., Art 7.

im Zusammenhang mit Cyberbedrohungen und IKT-Schwachstellen durchzuführen[181]. Selbige sind auch bei wesentlichen Änderungen der IT-Infrastruktur und Verfahren durchzuführen[182]. Für IKT-Altsysteme muss eine spezifische Bewertung des Risikos vorgenommen werden[183]. Interessanterweise dürften Betroffene aber laut Artikel 7 DORA gar keine nicht aktuellen Systeme (also Altsysteme) haben. Ob jene Bewertungspflicht auch bei Änderungen an Systemen von externen Cloud-Diensten maßgeblich ist, geht aus der Verordnung nicht hervor. Betroffene Einrichtungen müssen IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -tools aufbauen, die die Sicherheit der Systeme gewährleisten[184]. Konkret sind folgende Punkte zum Schutz und zur Prävention umzusetzen:

> *a) Die Verfassung einer Informationssicherheitsleitlinie zum Schutz von Confidentiality (Vertraulichkeit), Integrity (Integrität), Authenticity (Authentizität) und Availability (Verfügbarkeit) (CIAA).*
>
> *b) Die Einrichtung einer soliden Struktur für Netzwerk- und Infrastrukturmanagement.*
>
> *c) Die Beschränkung des physischen oder logischen Zugangs zu Informations- und IKT-Assets auf ein notwendiges Niveau, inklusive der Einrichtung von dazugehörigen Verfahren und Kontrollen.*
>
> *d) Der Einsatz starker Authentifizierungsmechanismen, Schutzmaßnahmen für kryptografische Schlüssel und die Datenverschlüsselung anhand von Datenklassifizierungs- und IKT-Risikobewertungsprozessen.*
>
> *e) Die Implementierung eines IKT-Änderungsmanagements in Bezug auf Software, Hardware, Firmware-Komponenten, den Systemen oder Sicherheitsparametern.*
>
> *f) Für Patches und Updates müssen angemessene und umfassend dokumentierte Richtlinien existieren.*
>
> (Obenstehende Aufzählung vollständig bezogen und zusammengefasst aus *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 9 Abs 4 lit a–f)

Interessanterweise fordert DORA allgemein nur starke Authentifizierung (Punkt d)), ohne zu definieren, was darunter genau zu verstehen ist. NISR2 wiederum verlangt dezidiert Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung (siehe Abschnitt 4.2).

[181] *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 8 Abs 2.
[182] Ebd., Art 8 Abs 3.
[183] Ebd., Art 8 Abs 7.
[184] Ebd., Art 9 Abs 1.

Daneben müssen Finanzunternehmen in der Lage sein, anomale Aktivitäten zu erkennen und Schwachstellen zu ermitteln[185]. Sollte es zu IKT-bezogenen Vorfällen kommen, müssen wichtige und kritische Funktionen aufrechterhalten werden bzw. wiederhergestellt werden[186]. Dafür müssen sie IKT-Geschäftsfortführungspläne, IKT-Reaktions- und Wiederherstellungspläne etablieren[187], besonders auch für wichtige/kritische Funktionen, die an Dritte ausgelagert wurden[188]. Dazu zählen auch Business-Impact-Analyses (BIA) der vorherrschenden Risiken[189]. Aus diesen Anforderungen schließend, müssten damit beim Einsatz externer Cloud-Dienste auch die Auswirkungen bei Vorfällen dieser Dienstleister betrachtet und mitigiert werden.

4.7.2 Vorfallsmanagement

DORA fordert von erfassten Organisationen konkret drei Punkte beim Auftreten von Vorfällen mit IKT Bezug: erkennen, behandeln und melden[190]. Als schwerwiegend eingestufte Vorfälle müssen an die zuständige nationale Behörde gemeldet werden und diese werden, sofern sie von als bedeutend eingestuften Kreditinstituten (nach *Verordnung (EU) Nr. 1024/2013 des Rates vom 15. Oktober 2013*, Art 6 Abs 4) gemeldet wurden, an die Europäische Zentralbank (EZB) weitergeleitet[191]. Ergänzend dazu können Cyberbedrohungen freiwillig gemeldet werden[192]. Wenn ein schwerwiegender IKT-Vorfall die finanziellen Interessen von Kund:innen betrifft, müssen auch diese umgehend informiert werden[193]. Ebenso müssen Kund:innen bei erheblichen Cyberbedrohungen über Maßnahmen, die diese ergreifen können, unterrichtet werden[194]. Von DORA betroffene Unternehmen können diese genannten Melde- und Informationspflichten zwar an Dienstleister auslagern, nicht jedoch ihre Verantwortlichkeit bei der Erfüllung[195].

4.7.3 Systemtests in Bezug auf IKT-Vorfälle

DORA verlangt die Durchführung regelmäßiger Tests von Finanzunternehmen (mit der Ausnahme von Kleinstunternehmen), um die digitale Resilienz zu prüfen[196]. Die Tests können von internen oder externen Tester:innen vorgenommen werden[197] und müssen für kritische/wichtige Systeme zumindest einem jährlichen Zyklus folgen[198]. Alle

[185] *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 10 Abs 1.
[186] Ebd., Art 11 Abs 2.
[187] Ebd., Art 11 Abs 3, Abs 4.
[188] Ebd., Art 11 Abs 4.
[189] Ebd., Art 11 Abs 5.
[190] Ebd., Art 17 Abs 1.
[191] Ebd., Art 17 Abs 1.
[192] Ebd., Art 17 Abs 2.
[193] Ebd., Art 17 Abs 3.
[194] Ebd., Art 17 Abs 3.
[195] Ebd., Art 17 Abs 5.
[196] Ebd., Art 24 Abs 1.
[197] Ebd., Art 24 Abs 4.
[198] Ebd., Art 24 Abs 6.

während dieser Tests aufgedeckten Punkte müssen vollständig „*angegangen*“ werden[199]. Interessant dabei ist, dass das bloße Bearbeiten des Problems reicht und eine Lösung nicht innerhalb einer vorgegebenen Frist in DORA vorgesehen ist. Betroffene Unternehmen könnten damit die Umsetzung entsprechend hinauszögern, bis sich der Mangel anderweitig löst, beispielsweise durch eine System-Ablöse. Unter dem Begriff *Testen* versteht die Verordnung:

> *„[...] wie etwa Schwachstellenbewertung und -scans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfungen soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests“*[200]

Die zuvor genannte Aufzählung scheint jedoch eher beispielhaften Charakter zu haben und ist wohl nicht zwingend vollständig umzusetzen. Allerdings sind gewisse Penetrationstests, nämlich das sogenannte Threat-Led Penetration Testing (TLPT), für gewisse Unternehmen mindestens alle drei Jahre durchzuführen[201]. Die zuständige Behörde kann das Intervall verringern oder erhöhen[202]. Die Tests umfassen entweder alle oder zumindest Teile der kritischen/wichtigen Funktionen eines Finanzunternehmens und sind an Live-Produktionssystemen durchzuführen[203], was insbesondere die Gefahr eines Ausfalls oder einer Störung bergen kann. In diesem Zusammenhang kann speziell der Einsatz von Cloud-Anbietern relevant sein, da von der Testpflicht explizit IKT-Drittdienstleister, auch wenn diese nur unterstützend wirken, miterfasst sind[204]. Finanzunternehmen müssen sicherstellen, dass diese Dienstleister in TLPTs eingebunden werden[205]. Kommen interne Tester:innen zum Einsatz, muss die zuständige Behörde überprüfen, dass keine Interessenkonflikte in der Konzeptions- und Durchführungsphase entstehen und das Unternehmen genügend Mittel für derartige Tests hat[206]. Ferner darf die für TLPT notwendige Bedrohungsanalyse nur durch externe Anbieter durchgeführt werden[207].

4.7.4 Drittparteienrisiko

In DORA widmet sich ein ganzes Kapitel dem sogenannten Management des IKT-Drittparteienrisikos, von dem auch Cloud-Computing ein Teil ist. Die Verordnung legt dabei folgenden Grundsatz fest:

[199] *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 24 Abs 5.
[200] Ebd., Art 25 Abs 1.
[201] Ebd., Art 26 Abs 1.
[202] Ebd., Art 26 Abs 1.
[203] Ebd., Art 26 Abs 2.
[204] Ebd., Art 26 Abs 2.
[205] Ebd., Art 26 Abs 3.
[206] Ebd., Art 27 Abs 2 lit a, b.
[207] Ebd., Art 26 Abs 2 lit c.

> *„Finanzunternehmen, die vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen für die Ausübung ihrer Geschäftstätigkeit getroffen haben, bleiben jederzeit in vollem Umfang für die Einhaltung und Erfüllung aller Verpflichtungen nach dieser Verordnung und nach dem anwendbaren Finanzdienstleistungsrecht verantwortlich“*[208]

Dazu müssen betroffene Unternehmen eine Strategie zur Prüfung des IKT-Drittparteienrisikos erstellen[209] und informieren die zuständigen Behörden mindestens jährlich über die genutzten IKT-Drittdienstleister[210]. Ferner dürfen nur Dienstleister beauftragt werden, die angemessene Standards zur Informationssicherheit einhalten[211]. Die Verordnung lässt aber offen, welche Standards genau damit gemeint sind. DORA schreibt implizit auch eine Auditpflicht ausgehend von den Finanzunternehmen vor und verlangt dabei einen risikobasierten Ansatz[212]. Wenn durch den Einsatz des Drittdienstleisters eine wirksame Aufsicht durch die zuständige Behörde nicht mehr möglich ist, muss das Finanzunternehmen sicherstellen, dass es eine Kündigungsmöglichkeit gibt[213]. Allerdings gibt es keine explizit formulierte Verpflichtung, den Vertrag dann wirklich kündigen zu müssen.

Für kritische oder wichtige IKT-Drittdienstleistungen müssen Finanzunternehmen Ausstiegsstrategien entwickeln, um dem Risiko von Ausfällen, Fehlern oder Serviceverschlechterungen Rechnung zu tragen[214]. Der Ausstieg muss praktisch ohne Servicebeeinträchtigung vonstattengehen[215]. Nachdem bei Cloud-Anbietern Vendor Lock-in ein häufiges Problem ist[216] (siehe auch Abschnitt 2.2), muss der Einsatz von Public Clouds aus der Warte von DORA besonders betrachtet werden. Ein Ansatz, dem Problem des Vendor Lock-in zu begegnen, ist die Multi Cloud, also die Nutzung unterschiedlicher Anbieter desselben Liefermodells, um somit Redundanzen herzustellen[217]. Artikel 29 von DORA führt dies auch in verallgemeinerter Form beispielhaft mit „Nutzung verschiedener IKT-Drittdienstleister“ explizit an[218]. Bei der Wahl eines Dienstleisters mit Sitz in einem Drittland muss von den jeweiligen Finanzunternehmen sichergestellt werden, dass einschlägige Rechtsvorschriften (insbesondere auch die Datenschutzvorschriften) in diesem Land durchsetzbar sind[219].

Finanzunternehmen sind verpflichtet, in den Vertrag mit IKT-Dienstleistern mehrere Punkte aufzunehmen. So müssen IKT-Drittdienstleister das Finanzunternehmen bei

[208] Ebd., Art 28 Abs 1 lit a.
[209] Ebd., Art 28 Abs 2.
[210] Ebd., Art 28 Abs 3.
[211] Ebd., Art 28 Abs 5.
[212] Ebd., Art 28 Abs 6.
[213] Ebd., Art 28 Abs 6.
[214] Ebd., Art 28 Abs 8.
[215] Ebd., Art 28 Abs 8.
[216] Opara-Martins, Sahandi und Tian, „Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective“.
[217] Hong u. a., „An overview of multi-cloud computing“.
[218] *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 29 Abs 1.
[219] Ebd., Art 29 Abs 2.

IT-Vorfällen kostenlos oder zu vorab vereinbarten Kosten unterstützen[220]. Ferner muss der Dienstanbieter mit den für das Finanzunternehmen zuständigen Behörden zusammenarbeiten[221] und sich an TLPTs beteiligen[222]. Dem Finanzunternehmen müssen uneingeschränkte Zugangs- und Auditrechte zugesichert werden, die nicht durch andere vertragliche Vereinbarungen eingeschränkt werden dürfen[223]. Ein Public Cloud-Anbieter müsste dann folglich seinen Kund:innen, die von DORA erfasst sind, weitgehend Zugang zu seinen Systemen gewähren. Gleichzeitig basiert aber das Geschäftsmodell vieler Cloud-Betreiber darauf, dass Systeme mehrerer Kund:innen parallel auf derselben Plattform laufen (um damit Synergien zu schaffen) und ein granularer Zugang für einzelne Kund:innen möglicherweise nur schwer durchführbar ist. Außerdem müssen Ausstiegsstrategien mit dem Dienstleister vereinbart werden[224], also wie der Finanzdienstleister den IKT-Dienstleister wechseln kann (siehe dazu auch Punkt f)).

Die Europäischen Aufsichtsbehörden (ESA) stufen IKT-Drittdienstleister anhand von verschiedenen Kriterien als kritisch für Finanzdienstleister ein[225] und ernennen eine sogenannte federführende Überwachungsbehörde[226]. Die Einstufung erfolgt allerdings erst, nach dem die EK einen delegierten Rechtsakt erlassen hat, der die Einstufungskriterien genauer beschreibt[227]. Die Einstufung kann jedoch keine IKT-Unternehmen treffen, die selbst Finanzunternehmen sind oder nur in einem einzigen Mitgliedstaat tätig sind[228]. Um ihre Aufgabe zu erfüllen, bewertet die federführende Überwachungsbehörde folgende Punkte bei den von ihrer Zuständigkeit erfassten Finanzunternehmen:

a) *Gewährleistung von Sicherheit, Verfügbarkeit, Kontinuität, Skalierbarkeit, Qualität der Dienste und hoher Standards für Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der Daten*
b) *Physische Sicherheit*
c) *Risikomanagementprozesse*
d) *Governance-Regelungen*
e) *Ermittlung, Überwachung und unverzügliche Meldung wesentlicher IKT-bezogener Vorfälle an die Finanzunternehmen sowie den Umgang und die Lösung dieser Vorfälle*
f) *Mechanismen für Datenübertragbarkeit, Übertragbarkeit von Anwendungen und Interoperabilität, die eine wirksame Wahrnehmung von Kündigungsrechten durch die Finanzunternehmen gewährleisten*

[220] *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 30 Abs 2 lit f.
[221] Ebd., Art 30 Abs 2 lit g.
[222] Ebd., Art 30 Abs 3 lit d.
[223] Ebd., Art 30 Abs 3 lit e.
[224] Ebd., Art 30 Abs 3 lit f.
[225] Ebd., Art 31 Abs 1 lit a.
[226] Ebd., Art 31 Abs 1 lit b.
[227] Ebd., Art 31 Abs 6, 7.
[228] Ebd., Art 31 Abs 8.

g) Tests von IKT-Systemen, Infrastrukturen und Kontrollen

h) IKT-Audits

i) Übernahme entsprechender Normen

(Obenstehende Aufzählung vollständig bezogen und zusammengefasst aus *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 33 Abs 3)

Als Besonderheit der Anforderungen ist hier Punkt f) zu nennen, da jene Mechanismen zur Übertragbarkeit in anderen rechtlichen Vorgaben wie NISR oder NISR2 nicht vorkommt. Der IKT-Dienstleister wird damit folglich gezwungen, vom Vendor Lock-in Abstand zu nehmen und möglicherweise Technologien nicht einzusetzen, auch wenn sie wirtschaftliche oder technologische Vorteile bringen könnten. Ferner kann die federführende Behörde empfehlen, von einer Auftragsvergabe abzusehen, wenn der Auftragnehmer in einem Drittland sitzt, eine kritische/wichtige Funktion betroffen ist und die federführende Überwachungsbehörde von einem ernsten Risiko für die Finanzstabilität ausgeht[229]. Die Durchsetzbarkeit dieser Anforderung mit Zwangsgeldern ist nicht eindeutig formuliert, da Artikel 35 Absatz 1 DORA (verwiesen von Artikel 35 Absatz 6) nur eine Berichtspflicht der Finanzunternehmen gegenüber der federführenden Aufsichtsbehörde in Bezug auf die Empfehlungen verlangt[230], aber keine explizite Verpflichtung zur Umsetzung im Verordnungstext aufgenommen wurde. Wenn allerdings bei kritischen IKT-Drittdienstleistern Risiken festgestellt werden, können die zuständigen Behörden von Finanzunternehmen verlangen, den Bezug vom jeweiligen Dienstleister vorübergehend teilweise oder vollständig auszusetzen[231].

Die federführende Überwachungsbehörde hat umfassende Untersuchungsrechte bei kritischen IKT-Drittdienstleistern[232]. Sie kann unter anderem Dateneinsicht nehmen, Vertreter des IKT-Drittdienstleisters vorladen und Aufzeichnungen von Telefongesprächen bzw. Datenübermittlungen erheben[233]. Daneben sind Vor-Ort-Inspektionen möglich[234]. Zur Durchsetzung können Zwangsgelder verhängt werden[235]. Folglich müssen sich auch in diesem Fall große Cloud-Dienstanbieter von der federführenden Überwachungsbehörde durchleuchten lassen, wenn sie als kritische IKT-Drittdienstleister eingestuft werden. Interessanterweise muss die Aufsicht durch die federführende Überwachungsbehörde von den kritischen IKT-Drittdienstleistern in Form von Gebühren selbst bezahlt werden[236].

[229] *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 35 Abs 1 lit d iv.
[230] Ebd., Art 35 Abs 1 lit c.
[231] Ebd., Art 42 Abs 6.
[232] Ebd., Art 38 Abs 1.
[233] Ebd., Art 38 Abs 2.
[234] Ebd., Art 39 Abs 1.
[235] Ebd., Art 38 Abs 3.
[236] Ebd., Art 43 Abs 1.

4.7.5 Austausch von Informationen

Finanzunternehmen wird das Recht eingeräumt, Informationen über Cyberbedrohungen unter bestimmten Voraussetzungen untereinander auszutauschen[237], bei gleichzeitiger Mitteilungspflicht gegenüber ihrer zuständigen Behörde über dazugehörige Vereinbarungen[238]. Unklar ist, ob ein Austausch ausschließlich zu den in Artikel 45 genannten Bedingungen stattfinden darf. Die Bedingungen umfassen, dass damit die digitale operationale Resilienz von Finanzunternehmen gestärkt wird, der Empfängerkreis nur aus vertrauenswürdigen Gemeinschaften von Finanzunternehmen bestehen darf und entsprechende Vereinbarungen zum Schutz der Information getroffen werden[239]. In jenen Vereinbarungen sind auch Voraussetzungen über die Einbindung von IKT-Drittdienstleistern, also auch Public Cloud-Diensten, festzulegen[240], wobei diese nach Artikel 45 Absatz 1 DORA nicht Teil der Gemeinschaften von Finanzunternehmen sein können, es sei denn, sie sind auch als Finanzunternehmen tätig.

4.7.6 Delegierte Rechtsakte und Durchführungsstandards

Die drei Teile der ESA, bestehend aus Europäische Bankenaufsichtsbehörde (EBA), Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA) und Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA), haben im Jänner 2024 Entwürfe zu technischen Implementierungs- und Regulierungsstandards veröffentlicht[241] in Form von delegierten Verordnungen. Delegierte Verordnungen im Allgemeinen gehen auf den Vertrag über die Arbeitsweise der Europäischen Union (AEUV) zurück, die Möglichkeit einräumt, im Rahmen von Sekundärrechtsakte der EK Befugnisse zu übertragen, um Rechtsakte zur Ergänzung oder Änderung bestimmter Regularien zu erlassen[242]. Ziel der Standards ist, zu konkretisieren, wie DORA anzuwenden ist[243]. Die EK hat die Entwürfe mit 13. März 2024 angenommen und sie werden die nächsten drei Monate geprüft[244]. Diese umfassen:

- **Delegierte Verordnung (EU) 2024/1772:** Klassifizierung, Wesentlichkeitsschwellen und Einzelheiten zu IKT-bezogenen Vorfällen[245]
- **Delegierte Verordnung (EU) 2024/1773:** Leitlinien zu Vereinbarungen mit IKT-Drittdienstleistern[246]

[237] *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 45 Abs 1.
[238] Ebd., Art 45 Abs 3.
[239] Ebd., Art 45 Abs 1 lit a–c.
[240] Ebd., Art 45 Abs 2.
[241] ESMA, *ESAs publish first set of rules under DORA for ICT and third-party risk management and incident classification*.
[242] *Vertrag über die Arbeitsweise der Europäischen Union*, Art 290.
[243] BaFin, *DORA*.
[244] Ebd.
[245] *Delegierte Verordnung (EU) 2024/1772 der Kommission*, Titel.
[246] *Delegierte Verordnung (EU) 2024/1773 der Kommission*, Titel.

- **Delegierte Verordnung (EU) 2024/1774:** Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement[247]

Die delegierte Verordnung (EU) 2024/1773 verlangt im Einklang mit Artikel 28 Absatz 2 DORA das Erstellen und jährliche Überprüfen bzw. Aktualisieren einer Leitlinie für den Umgang mit IKT-Drittdienstleistern[248]. In jener muss festgehalten werden, bei welcher Funktion oder welchem Teil der Geschäftsleitung die Überwachung der vertraglichen Vereinbarungen mit dem IKT-Drittdienstleister liegt[249]. Weiters muss über die Leitlinie sichergestellt werden, dass die vertraglichen Vereinbarungen mit den *IKT-Risikomanagementrahmen*, der *Informationssicherheitsleitlinie*, der *IKT-Geschäftsfortführungsleitlinie* und den *Anforderungen für die Meldung von Vorfällen* aus DORA im Einklang stehen[250]. Ferner muss über die Leitlinie festgelegt werden, dass eine behördliche Aufsicht auch bei Auslagerung möglich ist[251] und Finanzunternehmen, die Revisoren und die entsprechenden Behörden nicht nur Zugang zu den Daten, sondern auch zu den Räumlichkeiten haben müssen (zumindest im Zusammenhang mit kritischen oder wichtigen Funktionen)[252]. Letztere Forderung ergibt sich für Österreich bereits aus dem Bundesgesetz über das Bankwesen (BWG) (siehe Abschnitt 4.9). Wenn ein IKT-Drittdienstleister in einem Drittland Daten verarbeitet bzw. speichert oder dort lokalisiert ist, müssen damit verbundene Risiken betrachtet werden, einschließlich potenzielle Embargos oder Sanktionen[253]. Dabei sei angemerkt, dass alle großen Public Cloud-Dienste aus einem Drittstaat (USA) kommen und für manche Dienste nur die USA als Datenstandort zur Auswahl steht[254].

Interessanterweise muss bewertet werden, ob der IKT-Drittdienstleister in ethischer und sozial verantwortlicher Weise handelt, Menschen- und Kinderrechte und Grundsätze des Umweltschutzes einhält, sowie angemessene Arbeitsbedingungen sicherstellt[255]. Auch wenn diese Forderungen aus sozialer Sicht Sinn ergeben, ist fraglich, warum sie in einer Verordnung zur digitalen operationalen Resilienz festgehalten werden und nicht in einem eigenen entsprechenderen Regulativ.

4.8 Leitlinien der Europäischen Bankenaufsichtsbehörde (EBA) zu Auslagerungen

[247] *Delegierte Verordnung (EU) 2024/1774 der Kommission*, Titel.
[248] *Delegierte Verordnung (EU) 2024/1773 der Kommission*, Art 3 Abs 1.
[249] Ebd., Art 3 Abs 5.
[250] Ebd., Art 3 Abs 6.
[251] Ebd., Art 3 Abs 8 lit b.
[252] Ebd., Art 3 Abs 8 lit d.
[253] Ebd., Art 6 Abs 1 lit d.
[254] Interviewfrage A.2.8
[255] *Delegierte Verordnung (EU) 2024/1773 der Kommission*, Art 6 Abs 1 lit f.

Im Februar 2019 veröffentlichte die Europäische Bankenaufsichtsbehörde (EBA) Leitlinien zu Auslagerungen, denen entsprechend Artikel 16 Absatz 3 der Verordnung (EU) 1093/2010 zur Errichtung einer Europäischen Aufsichtsbehörde (EBA-Verordnung) von zuständigen Behörden und Finanzinstituten nachgekommen werden muss[256]. Viele Anforderungen finden sich in ähnlich gestalteter Form in Regulativen wie in der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA) oder dem österreichischen Bundesgesetz über das Bankwesen (BWG) wieder. So müssen Risiken, die Finanztechnologie und IT betreffen, für Auslagerungsvereinbarungen ermittelt, bewertet, gesteuert und gemindert werden[257]. Bei der Verarbeitung personenbezogener oder vertraulicher Daten sollte das Finanzunternehmen prüfen ob Maßnahmen zum Schutz der Daten in Kraft sind[258]. Konkret angeführt ist auch der Einsatz von Cloud-Diensten: Dabei sollten die betroffenen Unternehmen einen risikobasierten Ansatz betreffend Daten- bzw. Datenverarbeitungsstandort wählen und Anforderungen an die Daten- und Systemsicherheit festlegen sowie dieselbigen überwachen[259]. Besonders bei Drittstaaten müssen auch Unterschiede in nationalen Vorschriften zum Datenschutz berücksichtigt werden[260], dabei könnte auch der Clarifying Lawful Overseas Use of Data Act (CLOUD Act) (siehe Abschnitt 4.11) oder der Foreign Intelligence Surveillance Act (FISA) relevant sein, also der Zugriff durch US-Behörden. Ähnlich zur delegierten Verordnung (EU) 2024/177 fordern die EBA-Leitlinien, dass die Dienstleister bzw. deren Subunternehmer ethisch und sozial verantwortlich handeln[261].

Bei der Auslagerung von kritischen wesentlichen Funktionen müssen die betroffenen Institute und Zahlungsinstitute vereinbaren, dass zuständige Behörden vollständigen Zugang zu allen relevanten Geschäftsräumen haben[262] (analog zur delegierten Verordnung (EU) 2024/1773). Explizit erfasst sind davon alle Geräte, Systeme, Netzwerke, Daten und Informationen, die im Zuge der ausgelagerten Funktion zum Einsatz kommen[263]. Um den Aufwand zu verringern, können Sammelaudits gemeinsam mit anderen Kunden durchgeführt werden[264]. Die zuständige Behörde kann Unternehmen anweisen, Verträge mit Dienstleistern zu kündigen[265]. Folglich kann die Behörde direkt Einfluss nehmen auf Technologie- und Anbieterwahl. Problematisch kann dabei eine Konstellation sein, bei der es nur einen einzigen Lieferanten am Markt gibt. Ferner sind insbesondere Konzentrationsrisiken, die durch Auslagerungen entstehen, zu steuern und überwachen[266].

Ähnlich zu DORA sind Ausstiegsstrategien zu berücksichtigen, zumindest für kritische

[256] EBA, *EBA BS 2019 Guidelines on outsourcing arrangements*, Abs 1.
[257] Ebd., Abs 40 lit c.
[258] Ebd., Abs 72.
[259] Ebd., Abs 82, Abs 83.
[260] Ebd., Abs 84.
[261] Ebd., Abs 73.
[262] Ebd., Abs 87 lit a.
[263] Ebd., Abs 87 lit a.
[264] Ebd., Abs 91 lit a.
[265] Ebd., Abs 98 lit e.
[266] Ebd., Abs 103.

oder wesentliche Funktionen[267]. Die Funktion muss wieder eingliederbar oder an andere Dienstleister vergebbar sein[268]. Alleinig der Ausfall oder eine Qualitätsverschlechterung – obwohl dafür in den Leitlinien keine konkreten Schwellenwerte genannt sind – des Dienstleisters kann ausreichen, um ein Ausstiegsszenario auszulösen[269]. Sollte folglich ein Cloud-Dienstleister von einer Leistungseinschränkung bei bestimmten Services betroffen sein, müsste ein von den EBA-Leitlinien erfasstes Unternehmen einen entsprechenden Aus- oder Umstieg vorbereitet haben.

4.9 Bundesgesetz über das Bankwesen (Bankwesengesetz – BWG)

Im österreichischen Bundesgesetz über das Bankwesen (BWG) gibt es besondere Bestimmungen zu Auslagerungen durch Kreditinstitute und damit folglich auch für den Einsatz von Public Cloud-Computing. Im Sinne des BWG sind jene Einrichtungen Kreditinstitute, die aufgrund gesetzlicher Regelungen berechtigt sind, Bankgeschäfte zu betreiben[270]. Eine Auslagerung darf die Qualität der internen Kontrollen und die Beaufsichtigung durch die Österreichische Finanzmarktaufsicht (FMA) nicht beeinträchtigen[271]. Eine stärkere Sorgfaltspflicht ist bei Auslagerungen an Dienstleister mit Sitz in Drittländern wahrzunehmen[272]. Viele Cloud-Dienstanbieter haben zwar einen Sitz auch innerhalb der EU, jedoch werden manche Services nur in US-Regionen betrieben[273], auch wenn sie in Europa nutzbar sind. Fraglich ist, ob damit noch der EU-Sitz gedeckt ist, oder es sich bereits um ein Drittland handelt, insbesondere wenn Services von Sub-Unternehmen innerhalb eines Konzerns (oder überhaupt von Dritten) betrieben werden.

Im Zuge der Auslagerung dürfen keine Aufgaben der Geschäftsleitung delegiert werden[274]. In diesem Zusammenhang ist Artikel 20 der NISR2 interessant, da dort die Leitungsorgane wesentlicher und wichtiger Einrichtungen (im Sinne der NISR2) verpflichtet werden, die Einhaltung von Risikomanagementmaßnahmen für Cybersicherheit zu billigen und ihre Umsetzung zu überwachen[275]. Bei einer Auslagerung ist also ungeklärt, ob damit schon diese genannten Aufgaben der Geschäftsleitung delegiert werden. Ferner müssen Auslagerungen wesentlicher bankbetrieblicher Aufgaben bei der FMA angezeigt und alle erforderlichen Auskünfte gewährt werden[276].

In der Anlage zu §25 BWG wurden auch konkrete Auslagerungsbedingungen definiert.

[267] Ebd., Abs 106.
[268] Ebd., Abs 40 lit f.
[269] Ebd., Abs 106 lit b, c.
[270] *Bundesgesetz über das Bankwesen (Bankwesengesetz – BWG)*, §1 Abs 1.
[271] Ebd., §25 Abs 1.
[272] Ebd., §25 Abs 1.
[273] Interviewfrage A.2.8
[274] *Bundesgesetz über das Bankwesen (Bankwesengesetz – BWG)*, §25 Abs 3.
[275] *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 20 Abs 1.
[276] *Bundesgesetz über das Bankwesen (Bankwesengesetz – BWG)*, §25 Abs 5.

Hervorhebenswert dabei ist, dass die Möglichkeit der Kündigung der Vereinbarungen vorgesehen werden muss, ohne Einschränkungen der Kontinuität und Qualität für die Kund:innen[277]. So muss es folglich im Falle des Einsatzes von Cloud-Diensten einen entsprechenden Ausweichplan zu einem anderen Dienstleister oder zu On-Premises-Umgebungen geben. Der gewählte Dienstleister muss hinsichtlich der ausgelagerten Tätigkeiten außerdem mit der FMA und Österreichischen Nationalbank zusammenarbeiten[278] und dieselbigen müssen Zugang zu Daten und den Geschäftsräumen des Dienstleisters haben[279]. Wenn also etwa Rechenkapazitäten eines Rechenzentrums in den USA genutzt werden, muss diesen beiden österreichischen Behörden Zugang gewährt werden. Weiters ist ein Notfallplan und dessen laufende Einhaltung gemeinsam mit dem Dienstleister festzulegen[280]. Überdies muss bei Auslagerungen in ein Drittland das Finanzinstitut die politischen, rechtlichen und wirtschaftlichen Entwicklungen im jeweiligen Land durchgehend kontrollieren, um bei negativen Entwicklungen hinsichtlich der Möglichkeiten der Aufsicht von der Auslagerung zurückzutreten[281].

4.10 Bundesgesetz über die Erbringung von Zahlungsdiensten 2018 (Zahlungsdienstegesetz 2018 – ZaDiG 2018)

Mit 1. Juni 2018 trat in Österreich das Bundesgesetz über die Erbringung von Zahlungsdiensten 2018 (ZaDiG 2018) in Kraft, mit dem die Richtlinie (EU) 2015/2366 über Zahlungsdienste im Binnenmarkt (PSD II) in nationales Recht umgesetzt wurde[282]. Damit wurde das auf der Richtlinie 2007/64/EG über Zahlungsdienste im Binnenmarkt (PSD I) basierende Bundesgesetz über die Erbringung von Zahlungsdiensten 2009 (ZaDiG 2009) abgelöst[283]. ZaDiG 2018 ist anwendbar für Zahlungsdienste, die in Österreich ansässige Zahlungsdienstleister erbringen oder an Zahlungsdienstnutzer in Österreich erbracht werden[284] - mit Ausnahmen, die in §3 des ZaDiG 2018 angeführt sind.

Adressaten des ZaDiG 2018 müssen für operationelle und sicherheitsrelevante Risiken einen Rahmen von Risikominderungsmaßnahmen und Kontrollmechanismen festlegen[285] und regelmäßig der FMA übermitteln[286]. Davon erfasst sind auch Verfahren zur Aufdeckung und Klassifizierung schwerer Betriebs- und Sicherheitsvorfälle[287]. Allerdings hat

[277] *Bundesgesetz über das Bankwesen (Bankwesengesetz – BWG)*, Anlage zu §25 Z 7.
[278] Ebd., Anlage zu §25 Z 8.
[279] Ebd., Anlage zu §25 Z 9.
[280] Ebd., Anlage zu §25 Z 11.
[281] Ebd., Anlage zu §25 Z 12.
[282] Wirtschaftkammer Österreich, *Zahlungsdienstegesetz und Zahlungsinstitute*, S. 2.
[283] Ebd., S. 2.
[284] *Bundesgesetz über die Erbringung von Zahlungsdiensten 2018 (Zahlungsdienstegesetz 2018 – ZaDiG 2018)*, §2 Abs 1.
[285] Ebd., §85 Abs 1.
[286] Ebd., §85 Abs 2.
[287] Ebd., §85 Abs 1.

der Gesetzgeber nicht festgelegt, welche Vorfälle schwer sind und was überhaupt unter einem Betriebs- oder Sicherheitsvorfall zu verstehen ist. Beim Auftreten jener schwerwiegenden Betriebs- oder Sicherheitsvorfälle ist die FMA unverzüglich zu informieren[288]. Interessanterweise gilt diese Meldepflicht im Gegensatz zu Bestimmungen der NISR2 offenbar nicht für potentielle Vorfälle, sie müssen wohl tatsächlich eingetreten sein. Beim Einsatz von Public Cloud-Lösungen durch den Finanzdienstleister muss dieser folglich sicherstellen, dass er über Risiken beim Cloud-Anbieter aufgeklärt wird und bei Vorfällen entsprechend unmittelbar unterrichtet wird.

Als sehr konkrete Forderung sieht das ZaDiG 2018 starke Kundenauthentifizierung für Zahler:innen gegenüber dem Finanzdienstleister vor[289] und definiert dabei den aus der PSD II entnommenen Begriff wie folgt:

> *„eine Authentifizierung unter Heranziehung von mindestens zwei Elementen der Kategorien Wissen (etwas, das nur der Nutzer weiß), Besitz (etwas, das nur der Nutzer besitzt) oder Inhärenz (etwas, das nur der Nutzer ist) [...]“*[290]

Hervorhebenswert dabei ist, dass die starke Authentifizierung nur für Zahlungsvorgänge der Kund:innen gilt, nicht aber für andere Aufgaben und offenbar nicht für interne Vorgänge beim Zahlungsdienstleister. So könnte geschlossen werden, dass für den administrativen Zugang auf Kernkomponenten durch Mitarbeiter:innen, die bei Public Cloud-Anbietern betrieben werden, keine entsprechende starke Authentifizierung nötig ist.

4.11 Zugriff durch US-Behörden auf Daten in der Europäischen Union

Im Jahr 2018 trat in den USA der Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in Kraft. Dieser fordert von elektronischen Kommunikationsdienstleistern und Remote-Computing-Diensten (womit wohl auch Cloud-Computing Dienste gemeint sind), dass sie dem Stored Communications Act (SCA) entsprechen müssen, unabhängig davon, ob die Daten ihrer Kund:innen im In- oder Ausland (also außerhalb der USA) gespeichert sind[291]. SCA fordert, dass die zuvor genannten Dienstleister die Inhalte einer elektronischen Kommunikation einer Regierungsbehörde („Governmental Entity“) entsprechend einer richterlichen Anordnung („Warrant“) preisgeben müssen[292]. Betroffene Unternehmen können gegen die Anordnung allerdings Anträge auf Aufhebung oder Änderung („Motions to Quash or Modify“) einbringen, wenn sie glauben, durch die Herausgabe gegen

[288] Ebd., §86 Abs 1.
[289] Ebd., §87 Abs 1.
[290] Ebd., §4 Z 28.
[291] *CLOUD Act*, §2713.
[292] *18 USC Ch. 121: Stored Wire and Electronic Communications and Transactional Records Access*, §2703 lit a.

ausländische Gesetze zu verstoßen[293]. Ein Gericht kann die Aufhebung oder Änderung der Anordnung nur bei Vorliegen der folgenden Voraussetzungen vornehmen:

1. wenn damit die Gesetze einer ausländischen Regierung verletzt werden[294]
2. wenn es die Interessen der Justiz erfordern („interests of justice dictate“)[295]
3. wenn die Person, deren Daten die Preisgabe betrifft, keine US-amerikanische Staatsbürger:in oder Bewohner:in ist[296]

Damit kann gefolgert werden, dass ein Datenzugriff bei US-amerikanischen Cloud-Betreibern auch direkt in Europa durch US-amerikanische Behörden möglich ist. In einem Artikel, der dieses Spannungsfeld behandelt, wurde darauf hingewiesen, dass es unwahrscheinlich sei, dass ein einzelnes Unternehmen von einem Informationszugriff betroffen ist[297]. Der European Data Protection Supervisor (EDPS) und das European Data Protection Board (EDPB) – beides Einrichtungen der EU – führten im Jahr 2019 eine rechtliche Bewertung des CLOUD Acts durch. Dabei kamen sie zu der Ansicht, dass für eine Rechtmäßigkeit internationale Vereinbarungen notwendig wären, wenn nicht besondere Umstände vorlägen, die die Datenverarbeitung zum Schutz wichtiger Interessen eines Datensubjekts notwendig machten[298].

Weitreichende Daten-Zugriffsmöglichkeiten ergaben sich auch durch folgende Entwicklung: Im Jahr 1978 trat in den USA der Foreign Intelligence Surveillance Act (FISA) in Kraft, um elektronische Überwachung rechtlich zu ermöglichen, mit dem Zweck, fremde oder ausländische Geheimdienstinformationen zu sammeln[299]. 2008 erfolgte eine Änderung in Form eines Amendment, in dem gemeinschaftlich dem Direktor der nationalen Nachrichtendienste und dem Generalstaatsanwalt der Vereinigten Staaten das Recht eingeräumt wurde, die Überwachung von Personen außerhalb der USA durchzuführen, um fremde bzw. ausländische Geheimdienstinformationen zu sammeln[300]. Elektronische Kommunikationsdienstleister können angewiesen werden, der US-Regierung sofort sämtliche Informationen, Anlagen oder Unterstützungsleistungen zukommen zu lassen, die im Zuge der Überwachung notwendig sind[301]. Die Informationsweitergabe muss vom Kommunikationsdienstleister geheim gehalten werden[302]. Folglich hat eine betroffene

[293] *18 USC Ch. 121: Stored Wire and Electronic Communications and Transactional Records Access*, §2703 lit h.
[294] Ebd., §2703 lit h Z 2 lit B i.
[295] Ebd., §2703 lit h Z 2 lit B ii.
[296] Ebd., §2703 lit h Z 2 lit B iii.
[297] Hildén, „Mitigating the risk of US surveillance for public sector services in the cloud“, S. 14.
[298] *LIBE Committee letters to the EDPS and to the EDPB regarding legal assessment of the impact of the US Cloud Act on the European legal framework for personal data protection.*
[299] *Foreign Intelligence Surveillance Act of 1978*, S. 1.
[300] *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008*, SEC 702 lit a.
[301] Ebd., SEC 702 lit h.
[302] Ebd., SEC 702 lit h.

Organisation oder Person keine Möglichkeit, überhaupt zu erfahren, dass ihre Daten abgeflossen sind und weitergegeben wurden. Der Unterschied zum CLOUD Act ist, dass unter Sektion 702 kein „Warrant“ (richterliche Genehmigung) nötig ist. Es kommt folglich zu direktem Zugriff auf Inhaltsdaten von Benutzer:innen. Nach weiteren Änderungen und rechtlich notwendigen Verlängerungen trat im Jahr 2024 der Reforming Intelligence and Securing America Act (RISAA) in Kraft[303]. Damit wurde die Definition elektronischer Kommunikationsdienstleister noch einmal breiter gefasst und auf fast alle Unternehmen erweitert, die Zugriff auf elektronische Kommunikationsdaten haben:

> *„any other service provider who has access to equipment that is being or may be used to transmit or store wire or electronic communications“*[304]

Ausgenommen wurden explizit nur Wohn- und Gemeinschaftseinrichtungen sowie Lebensmittelunternehmen[305]. Große Public Cloud-Dienstleister waren allerdings schon vor RISAA von nachrichtendienstlichen Zugriffen betroffen, wie deren Veröffentlichungen zeigen (siehe Unterabschnitt 6.4.2).

Neben den nachrichtendienstlichen Zugriffen aus FISA und RISAA gibt es die Möglichkeit für Bundesbehörden einen National Security Letter (NSL) auszustellen und damit Informationen über Abonnent:innen und Verbindungsdaten (jedoch keine konkreten Inhalte) von gewissen Dienstleistern ohne richterliche Genehmigung anzufordern[306,307]. NSLs können auch Verpflichtungen zur Geheimhaltung über den Datenzugriff beinhalten[308]. Die gängigen Public Cloud-Dienstanbieter sind entsprechend ihren Veröffentlichungen seit Jahren Empfänger von NSLs (siehe Unterabschnitt 6.4.2).

2022 wurde die US-amerikanische Executive Order (EO) 14086 „Enhancing Safeguards for US Signals Intelligence Activities“ verabschiedet, um Artikel 45 der DSGVO bzw. deren Interpretation durch den Europäische Gerichtshof (EuGH) mit dem Schrems II Urteil (in dem der EU-US-Privacy-Shield aufgehoben wurde[309]) gerecht zu werden[310]. Für einen historischen Überblick zu den Abkommen zum Datenaustausch zwischen der EU und den USA bzw. deren Aufhebung siehe Abbildung 4.9. In der EO 14086 sollen vorwiegend Sicherheitsmechanismen beim Zugriff auf Daten durch Sicherheitsbehörden etabliert werden[311]. Auf der Basis dieser EO hat die EK im Juli 2023 eine Entscheidung („COMMISSION IMPLEMENTING DECISION“) zum angemessenen Schutzniveau

[303] *Reforming Intelligence and Securing America Act*.
[304] Ebd., SEC 25 lit a Z 3.
[305] Ebd., SEC 25 lit a Z 3.
[306] Cornell Law School, *National Security Letter*.
[307] *18 USC Ch. 121: Stored Wire and Electronic Communications and Transactional Records Access*, §2709 lit a.
[308] Federal Bureau of Investigation, *NSL-21-538695-request-redacted.pdf*, S. 2.
[309] *Rechtssache C-311/18*.
[310] *COMMISSION IMPLEMENTING DECISION of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, S. 3.
[311] Ebd., S. 31.

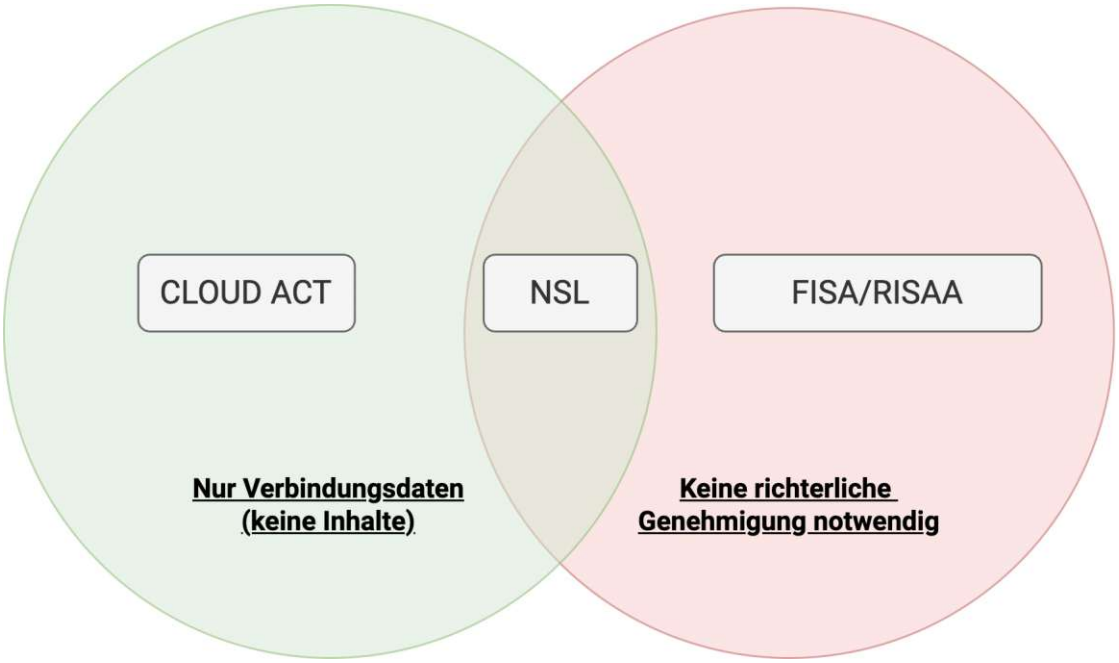

Abbildung 4.8: Bedingungen für Datenzugriff durch US-Behörden, je nach Gesetzesgrundlage (basierend auf *18 USC Ch. 121: Stored Wire and Electronic Communications and Transactional Records Access*, *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008* und *CLOUD Act*)

(im Sinne der DSGVO Artikel 45) persönlicher Daten unter dem EU-US Data Privacy Framework veröffentlicht[312]. Darin wird der Zugriff auf Daten, die von nach dem Framework zertifizierten Unternehmen gespeichert werden, für strafrechtliche Zwecke von US-amerikanischen Behörden (unter bestimmten Rahmenbedingungen) explizit erlaubt[313]. Ebenso dürfen US-Behörden zum Zweck der nationalen Sicherheit auf persönliche Daten außerhalb der USA zugreifen[314]. Die genannte Zertifizierung für Unternehmen ist einsehbar unter www.dataprivacyframework.gov. Bei einer stichprobenartigen Kontrolle vier großer US-amerikanischer Cloud-Anbieter waren alle Unternehmen erfasst und haben eine Selbstbewertung durchgeführt.

Der Verein „NOYB – Europäisches Zentrum für digitale Rechte“, der sich um die Durchsetzung europäischer Datenschutzrechte kümmert, kommt zum Schluss, dass die Rechtmäßigkeit des EU-US Data Privacy Frameworks, genauso wie deren Vorgänger „Safe Harbor“ und „Privacy Shield“ (beide wurden als ungültig erklärt) mit hoher Wahr-

[312] *COMMISSION IMPLEMENTING DECISION of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, S. 1.
[313] Ebd., S. 24.
[314] Ebd., S. 35.

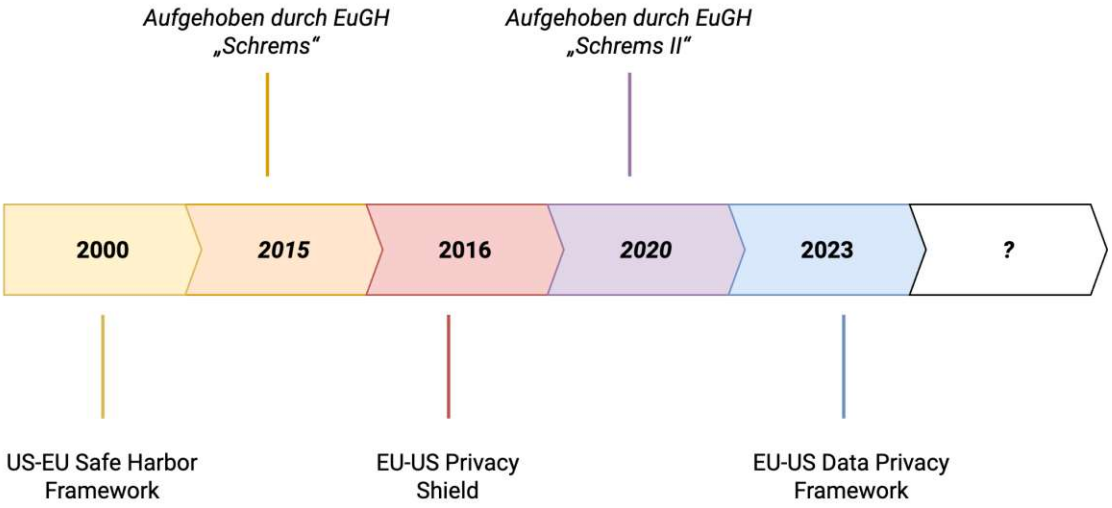

Abbildung 4.9: Zeitlicher Verlauf der Abkommen zum Datenaustausch zwischen der EU und den USA bzw. deren Aufhebung (basierend auf *COMMISSION IMPLEMENTING DECISION of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, S. 1–2 und Adesso, *Schrems II ad acta? Das neue Data Privacy Framework und seine Auswirkungen*)

scheinlichkeit vor dem EuGH entschieden und aufgehoben wird[315]. Als Begründung führt NOYB an, dass in US-amerikanischen Überwachungsgesetzen nach wie vor fundamentale Probleme im Zusammenhang mit europäischen Datenschutzrechten existieren[316].

[315] NOYB, *23 years of illegal data transfers due to inactive DPAs and new EU-US deals.*
[316] Ebd.

KAPITEL 5

Interviewauswertung

5.1 Vorgehensweise

Bereits in der Planungsphase dieser Arbeit zeichnete sich ab, dass es schwierig werden könnte, Personen zu finden, die direkt in Organisationen der kritischen Infrastruktur arbeiten und bereit für ein Interview sind. Da derartige Interviews schützenswerte Informationen beinhalten können, die auch bei einer Anonymisierung auf ein entsprechendes Unternehmen zurückzuführen sein könnten. Entsprechende Hinweise zu dieser Problematik gab es auch schon beim Feedback zum Proposal dieser Arbeit. Damit kam die Idee auf, nicht direkt an die kritische Infrastruktur heranzutreten, sondern bei Unternehmensberater:innen anzufragen, die entsprechende Organisationen beraten. Der Ansatz hat sich als erfolgreich erwiesen, da die Berater:innen einen generellen Überblick zur Lage geben können, ohne auf ein einzelnes Unternehmen eingehen zu müssen. Die Bereitschaft zu Interviews war auch vereinzelt gegeben: Von sechs Angefragten lehnten drei ab und drei sagten zu. Ferner konnte noch ein Security-Experte aus dem Finanzbereich und ein Teamleiter des österreichischen Computer-Notfallteams (CERT) für ein Experteninterview gewonnen werden. Alle Expert:innen haben jahrelange Erfahrung mit der IT bei Unternehmen der kritischen Infrastruktur. Für einen Überblick zu den durchgeführten Interviewanfragen siehe Tabelle 5.1. Die Interviews wurden online durchgeführt und transkribiert. Sie finden sich im Anhang A.

Anhand der im Zuge der Literaturrecherche, rechtlichen Analysen, Auswertung der Sicherheitsvorfälle und Markterhebungen gesammelten Informationen wurden Interviewfragen zusammengestellt. Die Fragestellungen an die Expert:innen sind inhaltlich ähnlich, wurden jedoch an die vorab bekannten Hintergründe der Interviewten angepasst. Im Folgenden werden die wichtigsten Inhalte der Interviews anhand der Transkripte zusammengefasst. Ferner konnten über die Zusammenfassung hinausgehend wertvolle Informationen für diese Arbeit gesammelt und in anderen Kapiteln eingearbeitet werden, wie z.B. Hinweise auf Standards, neue Technologien, Umsetzung in der Praxis etc.

Zeitpunkt der Anfrage	Branche	Funktion	Ergebnis
Jänner 2024	Unternehmensberatung	Consultant	abgelehnt
Jänner 2024	Unternehmensberatung	Consultant	abgelehnt
Februar 2024	Unternehmensberatung	Consultant	abgelehnt
März 2024	IT-Unternehmensberatung	Cloud-Security Leader	durchgeführt
März 2024	IT-Unternehmensberatung	IT-Consultant im Netzwerk und Security	durchgeführt
März 2024	Finanzdienstleister	Security Experte aus dem Finanzbereich in Österreich	durchgeführt
Mai 2024	Computer Emergency Response Team	Teamleiter CERT AT	durchgeführt
Mai 2024	Sicherheitsdruckerei	Mitarbeiter	keine Antwort

Tabelle 5.1: Interviewanfragen und Umsetzung

5.2 Interviewergebnisse

Bei einem interviewten Experten zeigte sich, dass österreichische kritische Infrastruktur-Betreiber im weitesten Sinne bereits begonnen haben, wesentliche und kritische Kernfunktionen auch bei großen Public Cloud-Dienstanbietern zu betreiben[1]. Expertin-A wusste von keinem Unternehmen (der kritischen Infrastruktur), das dies zum jetzigen Zeitpunkt bereits durchführt, jedoch wusste sie von einem, das eine absolute Cloud-First Strategie in Zukunft umsetzen möchte[2]. Interviewpartner Hartleitner hat Zurückhaltung bei kernkritischen Services wahrgenommen und sieht den Public Cloud-Einsatz mehr bei Support Systemen[3]. Der Wahrnehmung von Experte-B (aus dem Finanzbereich) nach, gebe es seit den letzten Jahren keine Hemmschwellen mehr beim Public Cloud-Einsatz[4]. Seiner Erfahrung nach, sei es finanziell sinnvoll, in die Cloud zu gehen und gleichzeitig sollen manche Dienste dort sogar besser umgesetzt werden[5]. Ähnliche Wahrnehmungen

[1] Interviewfrage A.3.9
[2] Interviewfrage A.2.1
[3] Interviewfrage A.1.1
[4] Interviewfrage A.3.9
[5] Interviewfrage A.3.10

hat auch Rosenkranz im Finanzsektor gesammelt, nämlich dass dort an der Cloud kein Weg mehr vorbeiführe[6]. Im Hinblick auf hybride oder Multi Cloud-Lösungen ist die Verbreitung zum heutigen Zeitpunkt für Nicht-Office-IT laut Hartleitner zurückhaltend[7].

Im Hinblick auf Notfallszenarien (Strom-, Telekommunikationsausfall) gibt es laut Expertin-A bei den meisten Unternehmen entsprechende Pläne, die teils auch geübt werden[8]. Jedoch sei die Priorität sehr gering[9]. Experte-B kennt ebenfalls derartige Notfallpläne und Übungen, meint jedoch, dass sich diese noch an neue Technologien, wie die Cloud, anpassen müssten[10].

Die Auskünfte zu den Servicemodellen waren durchmischt. Einer berichtete mehr von Platform-as-a-Service für Supportsysteme[11], während Expertin-A auch Software-as-a-Service wahrgenommen hat, insbesondere bei Identity-Diensten[12]. Für Testsysteme wird auch Infrastructure-as-a-Service genutzt[13].

Das Problem des Vendor Lock-ins findet laut den Expert:innen Beachtung bzw. ist im Bewusstsein. In manchen Systemen ist der Lock-in allerdings bereits passiert; Expertin-A weist hier besonders auf Exchange und Azure AD hin[14]. Laut Hartleitner sei in ISO 27001 Version 2022 im Kapitel Cloud-Security die Exit-Strategie bereits prominent mitgenannt[15]. Rosenkranz weist ebenfalls darauf hin, dass manche Regulative (z.B. DORA) Ausstiegs- bzw. Umstiegsszenarien vorschreiben und möglicherweise durch diese gesteigerten Anforderungen ein Kostenvorteil in der Public Cloud nicht mehr gegeben sei[16].

Experte-B gab an, dass aus seiner Sicht bereits genug auf regulativer Seite passiert ist und die bestehenden Regeln ausreichend sind[17]. Hartleitner meint, dass die Vorgaben Sinn ergeben und sie in eine gute Richtung gehen[18]. Rosenkranz sieht die Entwicklung ähnlich positiv, weist allerdings darauf hin, dass möglicherweise bei manchen Unternehmen das Geschäftsmodell nicht einträglich genug ist, um die Kosten zu stemmen[19]. Er interpretiert die Vorgangsweise von europäischen Gesetzgebern so, dass nur noch Markteilnehmer erlaubt sein sollen, die Digitalisierung auch sicher gestalten können – wem das nicht gelingt, der müsse sein Geschäft einstellen[20]. Aus seiner Sicht hat der Regulator den Spieß umgedreht und betroffene Unternehmen müssen sich künftig fragen, ob sie ihre

[6] Interviewfrage A.4.4
[7] Interviewfrage A.1.2
[8] Interviewfrage A.2.7
[9] Interviewfrage A.2.7
[10] Interviewfrage A.3.12
[11] Interviewfrage A.1.3
[12] Interviewfrage A.2.5
[13] Interviewfrage A.2.5
[14] Interviewfrage A.2.6
[15] Interviewfrage A.1.2
[16] Interviewfrage A.4.3
[17] Interviewfrage A.3.1
[18] Interviewfrage A.1.9
[19] Interviewfrage A.4.2
[20] Interviewfrage A.4.6

Umgebung selbst überhaupt verstehen – es gebe keine Liste, die einfach abzuarbeiten sei, sondern es müsse eine Risikoanalyse mit Blick auf IT-Sicherheit durchgeführt werden[21]. Ferner gebe es das Problem, dass andere Länder NISR2 nicht gleich gut umsetzen und das eigentliche Ziel, ein einheitliches Cybersecurity-Niveau, vielleicht verfehlt wird[22]. Für Expertin-A wirke das juristische Material, als wäre es von Personen verfasst, die in der Praxis bislang nicht direkt mit den Systemen zu tun hatten[23]. Daraus folgend sei manches realitätsfremd verfasst[24].

Kritisch sieht Expertin-A den Datenstandort bei Public Cloud-Anbietern. Sie meint, es gebe oft keine Kontrollmöglichkeiten, wo Daten wirklich liegen und ein Datenabfluss beim Cloud-Anbieter sei ohnehin nicht nachweisbar[25]. Für viele Services gebe es oft nur US-Standorte zur Auswahl; dahin gehend sei es schwer, die Daten in Europa zu halten[26]. Experte-B sieht den Datenzugriff durch fremde Gesetzgebung (z.B. CLOUD-Act) besonders im Banken- und Finanzdienstleister-Umfeld problematisch, da Kundendaten hier besonders schützenswert sind[27]. Hartleitner sieht dabei eine Diskrepanz zwischen der Wahrnehmung der Kritikalität beim Speichern von Daten in Public Clouds im Gegensatz zum (auch automatischen) Beziehen von etwa Software und Updates, die On-Premises installiert werden[28]. Er sieht die Angst vor fremdem Zugriff, vom Verlust des Einflussbereiches kommend, vor allem auch das Problem der Geopolitik bzw. von Abhängigkeitsverhältnissen[29]. Nach Rosenkranz gibt es bis heute keine saubere Lösung, wie mit dem Datenzugriff aus den USA umzugehen sei[30]. Der Versuch eines Microsoft-Rechenzentrums, in Deutschland betrieben durch die Deutsche Telekom, sei wieder eingestellt worden[31].

Bei der Durchführung von Audits bei Public Cloud-Betreibern hat Experte Hartleitner von Dritten erfahren, dass diese mit Kosten verbunden sein würden[32]. Es solle auch ein entsprechendes Rechenzentrum eines Betreibers geben, wo Führungen abgehalten werden[33]. Experte-B wies auf Cloud-Security Posture Lösungen hin, mit denen Security-Konfigurationen von Cloud-Anbietern zentral überwachbar und steuerbar seien[34]. Dadurch seien Schwachstellen leichter auffindbar. Diese Cloud-Security Posture Lösungen würden auch von großen Public Cloud-Anbietern unterstützt werden. Experte-B hat jedoch keinen Einblick, wie sich die Kompatibilität bei kleinen Anbietern darstellt[35].

[21] Interviewfrage A.4.2
[22] Interviewfrage A.4.2
[23] Interviewfrage A.2.13
[24] Interviewfrage A.2.13
[25] Interviewfrage A.2.8
[26] Interviewfrage A.2.8
[27] Interviewfrage A.3.8
[28] Interviewfrage A.1.5
[29] Interviewfrage A.1.5
[30] Interviewfrage A.4.6
[31] Interviewfrage A.4.6
[32] Interviewfrage A.1.7
[33] Interviewfrage A.1.7
[34] Interviewfrage A.3.16
[35] Interviewfrage A.3.18

Expertin-A sieht für sich selbst das Problem des richtigen Interpretierens und Auslegens des Regulatives[36]. Sie meint, es gebe noch kaum Judikatur dazu und daher sei es schwer zu beurteilen, welche Handlungsoption die richtige sei[37]. Ihrer Erfahrung nach werden gesetzliche Regelungen von Betreibern dahin gehend pauschal ausgelegt, dass sämtliche Infrastruktur On-Premises sein müsse[38]. Es sei auch nicht einfach, die Grenze zwischen kritischen und nicht kritischen Funktionen in einer Organisation zu ziehen[39]. Experte Hartleitner meint aus einem nicht juristischen Blickwinkel, dass es kein konkretes Verbot für einzelne Public Cloud-Service-Provider gebe[40]. Gewisse Informationssicherheitsmaßnahmen seien jedoch beim Einsatz dieser Technologien zu adressieren[41]. Kritische Infrastruktur Betreiber müssten genau verstehen, wo die Zuständigkeiten zwischen beiden Parteien liegen[42]. Er sieht das besonders über Zertifizierungen der Cloud-Service-Anbieter realisierbar[43]. Hartleitner weist darauf hin, dass durch neue Regulatorik der Betrieb in der Cloud schwieriger wird, aber auch gleichzeitig der Betrieb On-Premises[44].

Die Bestrebungen, eine europäische Public Cloud-Lösung zu etablieren, fanden alle danach gefragten Interviewten positiv, sie waren jedoch bei den Erfolgsaussichten pessimistisch[45]. Expertin-A meint, dass der Startvorsprung der amerikanischen Anbieter groß sei und Arbeitskräfte in Europa teurer seien, im Vergleich zu den USA oder Asien[46]. Dazu komme der Fachkräftemangel in der IT und bereits mögliche Monopolstellungen anderer Anbieter[47]. Hartleitner schlägt vor, an bestehende Hyperscaler heranzutreten und gemeinsam mit ihnen zu versuchen, ihre Lösungen in Europa zu implementieren[48].

Wichtige Erkenntnisse

Anhand der Interviews konnten folgende Kernpunkte identifiziert werden:

- Auslagerung an Public Cloud-Dienstleister bei kritischer Infrastruktur findet statt
- Vendor Lock-in ist präsent, auch wenn Exit-Strategien vorzusehen sind
- Notfallszenarien sind noch an Public Cloud-Dienste anzupassen
- Möglicherweise sind manche Geschäftsmodelle durch neue Regulative nicht mehr wirtschaftlich

[36] Interviewfrage A.2.11
[37] Interviewfrage A.2.11
[38] Interviewfrage A.2.11
[39] Interviewfrage A.2.11
[40] Interviewfrage A.1.6
[41] Interviewfrage A.1.6
[42] Interviewfrage A.1.6
[43] Interviewfrage A.1.6
[44] Interviewfrage A.1.6
[45] Interviewfrage A.2.14, A.3.15 und A.1.13
[46] Interviewfrage A.2.14
[47] Interviewfrage A.2.14
[48] Interviewfrage A.1.13

- Problematischer potentieller Datenzugriff aus Drittländern
- Kaum Judikatur zu Regulativen
- Unterscheidung kritische/nicht kritische Funktion schwierig
- Zuständigkeit zwischen Kund:innen und Cloud-Betreibern ist zu klären
- Betrieb wird sowohl in der Cloud als auch On-Premises schwieriger
- Pessimistische Aussichten zum Thema europäische Public Cloud
- Regulative werden oft pauschal in der Form so ausgelegt, dass sämtliche IT On-Premises sein müsse

KAPITEL 6

Public Cloud-Dienstanbieter im Vergleich

Im Jahr 2023 nahmen Public Cloud-Anbieter am europäischen Markt über 146 Milliarden US-Dollar ein[1]. 2,4 Milliarden Euro entfielen dabei allein auf Österreich[2]. Aktuell ist davon auszugehen, dass der Markt zeitnah massiv wachsen wird. So prognostiziert das Marktforschungs- und Beratungsunternehmen International Data Corporation (IDC) für Europa Ausgaben im Cloud-Bereich mit 291 Milliarden US-Dollar für 2027 und ein jährliches Wachstum von 20 %[3]. Die Branchen mit den meisten Ausgaben werden Telekommunikation, der Bankensektor und der Handel sein[4]. Für das Jahr 2024 gab es weltweite Ausgaben in Höhe von 723 Billionen US-Dollar für Public Cloud-Dienste[5].

Die folgenden drei größten Cloud-Anbieter machten im ersten Quartal 2024 laut ihren Geschäftsberichten folgende Umsätze:

1. *Amazon Web Services (AWS)* - 25 Milliarden US-Dollar[6]
2. *Microsoft* bzw. *Microsoft Azure (Azure)* - 24 Milliarden US-Dollar[7]
3. *Google Cloud Platform (GCP)* - knapp 10 Milliarden US-Dollar[8]

[1] Statista, *Public Cloud - Europe | Statista Market Forecast*.
[2] Statista, *Österreich: Umsatz im Markt für Public Cloud 2029*.
[3] IDC, *IDC Says European Public Cloud Spending Will Reach $142 Billion This Year, Defying Budget Cuts Amid an Economic Downturn*.
[4] Ebd.
[5] Statista, *Public cloud services end-user spending worldwide from 2017 to 2025*.
[6] Amazon.com, Inc., *Amazon.com Announces First Quarter Results*.
[7] Microsoft, *Microsoft Financial Data - FY24Q1*.
[8] Alphabet, *GOOG Exhibit 99.1 Q1 2024*.

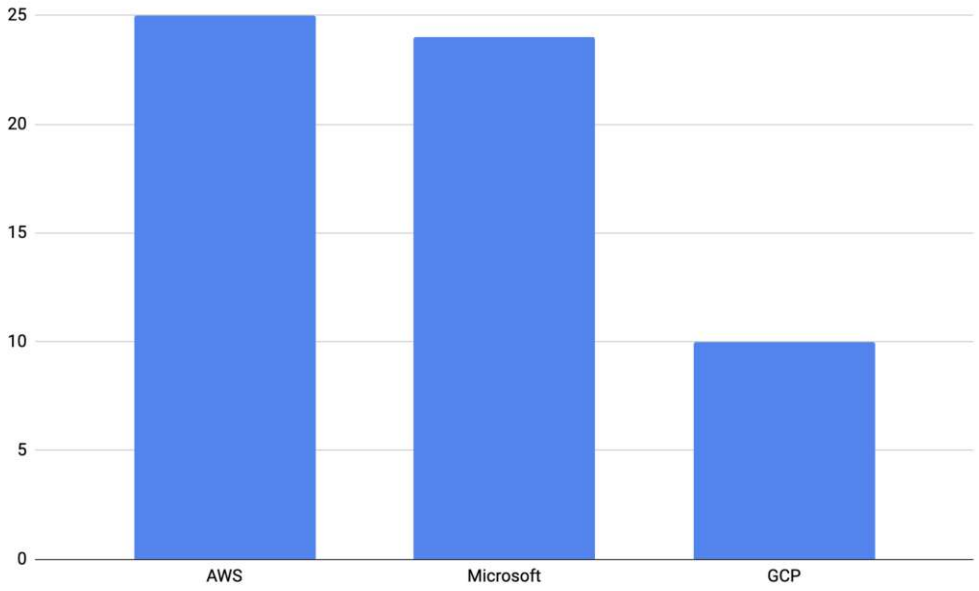

Abbildung 6.1: Umsätze der Cloud-Anbieter Q1 2024 in Milliarden US-Dollar (basierend auf Microsoft, *Microsoft Financial Data - FY24Q1*, Alphabet, *GOOG Exhibit 99.1 Q1 2024* und Amazon.com, Inc., *Amazon.com Announces First Quarter Results*)

Betrachtet man nur das Service-Modell SaaS ist auch Salesforce mit knapp 13 % Marktanteil (für das Jahr 2022) zu nennen, das dabei an zweiter Stelle hinter dem Marktführer Microsoft mit 22 % rangiert[9].

In diesem Kapitel wird zunächst Europas digitale Abhängigkeit beleuchtet, gefolgt von einem Überblick zu Unterstützungsangeboten zur Compliance und einem Vergleich der Leistungsvereinbarungen zwischen den zuvor vorgestellten marktdominierenden Cloud-Anbietern. Ferner wird die Praxis beim Zugriff durch Behörden und staatliche Stellen auf Daten beschrieben und zu guter Letzt der mögliche Lösungsansatz „Sovereign Clouds“ vorgestellt.

6.1 Europas digitale Abhängigkeit

Mit Stand Q1 2024 befindet sich kein einziges europäisches Unternehmen in den fünf umsatzstärksten Cloud-Unternehmen[10].

[9] Statista, *Global cloud software market vendor share 2022*.
[10] Statista, *Global cloud infrastructure market share 2024*.

Nach einem Bericht der Synergy Research Group ist der Anteil der europäischen Public Cloud-Dienstleister am europäischen Markt kontinuierlich von 27 % im Jahr 2017 auf 13 % (2022) gesunken[11]. Die Profiteure waren die zuvor genannten großen US-amerikanischen Unternehmen[12]. Das Center for Advanced Security, Strategic and Integration Studies (CASSIS) misst die digitale Abhängigkeit von 23 Staaten weltweit in verschiedenen Technologiebereichen, wie Hard- und Software, anhand des sogenannten digitalen Dependenz Index (DDI)[13]. Alle angeführten Staaten der EU (Frankreich, Italien, Deutschland) wurden mit einer hohen Vulnerabilität ($0{,}75 < \text{DDI} < 1$) eingeordnet, womit eine sehr niedrige Autonomie, sowie Dominanz ausländischer digitaler Technologien einhergehen[14]. Einzig die USA und die Volksrepublik China werden mit hoher Sensitivität (inländisches Angebot liefert den Großteil der digitalen Technologien) bzw. niedriger Vulnerabilität (globale Märkte liefern den Großteil der digitalen Technologien) ausgewiesen[15]. Folglich kann von einer dramatischen Lage der digitalen Souveränität innerhalb der EU gesprochen werden, mit einer sich verschlechternden Tendenz.

In der Volksrepublik China dominieren mit Q2 2024 ausschließlich chinesische Unternehmen den Cloud-Markt (Alibaba, Tencent, China Telecom und Huawei), womit sie sich deutlich vom Rest der Welt unterscheidet, wo die drei großen US-Vertreter den Markt beherrschen[16]. Als Gründe werden Geopolitik und historische Faktoren genannt, die westliche Cloud-Dienste massiv an der Marktteilnahme in der Volksrepublik China einschränken[17]. Mutmaßlich wird damit versucht, die chinesische digitale Souveränität zu stärken.

Um – unter anderem – dem Problem der digitalen Souveränität zu begegnen, wurde das Projekt Gaia-X von Vertretern der deutschen Bundesregierung, Wirtschaft und Wissenschaft im Jahr 2019 initiiert[18]. Projektziel ist eine europäische leistungs- und wettbewerbsfähige, sichere und vertrauenswürdige Dateninfrastruktur[19]. Dabei sollen zentrale und dezentrale Infrastrukturen (insbesondere Cloud- und Edge-Dienste) zu einem homogenen, nutzerfreundlichen System vernetzt werden[20]. Österreich wollte sich in der Vergangenheit stärker in die Gaia-X-Initiative einbringen und hat dafür einen nationalen Gaia-X Hub geschaffen[21]. Bis dato hat sich trotz solcher Initiativen kein europäischer Public Cloud-Dienstleister mit nennenswertem Marktanteil in Europa hervorgetan und es scheint auch keinen potenziellen Kandidaten dafür zu geben.

[11] Synergy Research Group, *European Cloud Providers Continue to Grow but Still Lose Market Share.*
[12] Ebd.
[13] Center for Advanced Security, Strategic and Integration Studies (CASSIS), *Vermessung der digitalen Dependenz - Digital Dependence Index.*
[14] Ebd.
[15] Ebd.
[16] Synergy Research Group, *Cloud is a Global Market - Apart from China.*
[17] Ebd.
[18] Bundesministerium für Wirtschaft und Energie (BMWi), *Das Projekt GAIA-X – Eine vernetzte Dateninfrastruktur als Wiege eines vitalen, europäischen Ökosystems*, S. 1.
[19] Ebd., S. 2.
[20] Ebd., S. 12.
[21] Bundesministerium für Arbeit und Wirtschaft, *OE-Cloud Initiative.*

6.2 Unterstützungsangebote zur Compliance

Anhand öffentlicher Informationen bei den größten Public Cloud-Dienstanbietern (AWS, Azure, Salesforce und GCP) werden nachfolgend unterschiedliche Unterstützungsangebote zur Compliance (Cloud-Anbieter bezeichnen diese als „Compliance-Angebote“) entsprechend ihrer Relevanz für kritische Infrastruktur allgemein in der EU, aber besonders für Österreich erfasst und zwischen den Anbietern verglichen. Die Ergebnisse werden in Tabelle 6.1 dargestellt. Gewisse Angebote oder Zertifizierungen gelten teilweise nur für bestimmte Dienste oder Regionen und manche sollen erst in Zukunft verfügbar sein. Verglichen wurden die folgenden Unterstützungsangebote zur Compliance:

- **Unionsrechtsvorschriften**
  - **Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA)** hat das Ziel, die Cybersicherheit im Finanzsektor zu stärken (siehe Abschnitt 4.7).
- **Nationale Rechtsvorschriften**
  - **Bundesgesetz über das Bankwesen (BWG)** ist ein österreichisches nationales Gesetz, das unter anderem Vorgaben für Kreditinstitute bei der Auslagerung an Dritte beinhaltet[22] (siehe Abschnitt 4.9).
- **Leitlinien**
  - **Europäische Bankenaufsichtsbehörde (EBA)** ist eine unabhängige Behörde für den gesamten EU-Bankensektor, die unter anderem auch Empfehlungen zum Outsourcing an Cloud-Dienstanbieter veröffentlicht[23] (siehe Abschnitt 4.8).
  - **European Cloud User Coalition (ECUC)** ist ein Zusammenschluss von Finanzdienstleistern in Europa, die sich dem Thema Public Cloud widmen und eine Checkliste herausgeben, die Cloud-Dienstanbieter beantworten können[24].
  - **Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA)** trägt als europäische Behörde zur Stabilität des Finanzsystems bei und legt Richtlinien zum Outsourcing an Clouddienstanbieter fest[25].
- **Technische Standards**

[22] Google, *BWG (Österreich) – Compliance.*
[23] Microsoft, *Europäische Bankenaufsichtsbehörde (EBA) - Microsoft Compliance.*
[24] ECUC Group, *ECUC Group – European Cloud User Coalition.*
[25] Google, *ESMA (EU).*

- **Security, Trust, Assurance and Risk (STAR)** ist ein Programm der Cloud Security Alliance (CSA) um den Stand der Sicherheit in der Cloud nachzuweisen[26]. Dabei kommt die ebenfalls von CSA entwickelte Cloud Controls Matrix (CCM) zum Einsatz[27]. Dabei gibt es mehrere Assurance-Levels: Level 1 besteht aus einer Selbst-Bewertung, während bei Level 2 bereits ein Audit von Dritten durchzuführen ist[28].
- **ISO/IEC 27001** ist ein Standard für ein Informationssicherheitsmanagementsystem (ISMS)[29]. Das System soll dabei CIA gewährleisten und umfasst die Aufbauorganisation (Rollen und Gremien), die Ablauforganisation (Sicherheitsprozesse) und Richtlinien[30].
- **ISO/IEC 27017** stellt Richtlinien für Informationssicherheitskontrollen beim Cloud-Einsatz zur Verfügung[31].
- **ISO/IEC 27018** zielt auf Richtlinien für den Umgang mit und Schutz von personenbezogenen Daten in Public Cloud-Umgebungen ab[32].
- **System and Organization Controls (SOC)** ist ein Standard, herausgegeben durch das American Institute of Certified Public Accountants (AICPA) und unterscheidet zwischen SOC-1 (für Finanzreporting), SOC-2 (Maßnahmen für Sicherheit, Verfügbarkeit, Verarbeitungsintegrität, Vertraulichkeit oder Datenschutz), SOC-3 sowie Cybersecurity und Lieferkettensicherheit[33].
- **EU Cloud Code of Conduct (CoC)** ist ein vom Europäischen Datenschutzausschuss (EDSA) bestätigter Verhaltenskodex für Cloud-Dienstanbieter, der Richtlinien zur Einhaltung von Artikel 28 DSGVO zur Verfügung stellt[34]. Eine positive CoC-Prüfung dient als Nachweis gegenüber Behörden und Endkunden in Hinblick auf selbigen Artikel[35].
- **Payment Card Industry 3 Domain Secure (PCI 3DS) Core Security Standard** soll Onlinekäufe durch Reduktion von Online-Betrug sicherer gestalten[36]
- **Payment Card Industry Data Security Standard (PCI DSS)** ist ein Standard, der vorgibt, wie mit Kreditkartendaten umzugehen ist und

[26] Cloud Security Alliance, *STAR | CSA*.
[27] Ebd.
[28] Ebd.
[29] ISO, *ISO/IEC 27001:2022 - Information security management systems*.
[30] IKT-Sicherheitsportal, *Informationssicherheits-Managementsystem (ISMS)*.
[31] ISO, *ISO/IEC 27017:2015 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.
[32] ISO, *ISO/IEC 27018:2019 - Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*.
[33] AICPA & CIMA, *System and Organization Controls: SOC Suite of Services*.
[34] EU Cloud CoC, *EU Cloud CoC*.
[35] Ebd.
[36] Google, *PCI 3DS – Compliance*.

Unterstützungsangebot	AWS	Azure	GCP	Salesforce
CSA Star Level 1	✓	✓	✓	✓
CSA Star Level 2	✓	✓	✓	
ISO/IEC 27001	✓	✓	✓	✓
ISO/IEC 27017	✓	✓	✓	✓
ISO/IEC 27018	✓	✓	✓	✓
SOC 1	✓	✓	✓	✓
SOC 2	✓	✓	✓	✓
SOC 3	✓	✓	✓	✓
EBA		✓	✓	
BWG			✓	
DORA			✓	
ECUC			✓	
ESMA			✓	
CoC		✓	✓	✓
PCI 3DS		✓	✓	
PCI DSS	✓	✓	✓	✓
CIS Benchmarks	✓	✓	✓	

Tabelle 6.1: Public Cloud Unterstützungsangebote zur Compliance (basierend auf den Informationen aus Microsoft, *Dokumentation zur Azure-Compliance*; Amazon Web Services (AWS), *Compliance-Programme*; Salesforce, *Salesforce Compliance*; Google, *Cloud Compliance – Vorschriften und Zertifizierungen*)

beinhaltet Sicherheitsprävention sowie das Erkennen und Reagieren auf Sicherheitsvorfälle[37].

– **Center for Internet Security (CIS) Benchmark** veröffentlicht Konfigurationsempfehlungen in Hinblick auf Cybersicherheit für etliche Produktkategorien, wie z.B. Cloud-Produkte, Betriebssysteme und Netzwerkkomponenten[38].

GCP deckte von den verglichenen Anbietern die meisten relevanten Unterstützungsangebote zur Compliance ab. Es finden sich auch Angebote zu konkreten gesetzliche Vorgaben angeführt, wie DORA oder BWG, mit denen Compliance hergestellt werden kann. Für Ersteres will Google ab Februar 2024 aktualisierte Vertragsbedingungen zu Artikel 30 DORA (dieser betrifft besonders IKT-Drittdienstleister) bereitstellen[39]. In Hinblick auf direkte behördliche Kontrollen erklärt Google, dass das Unternehmen bereit sei, Regulierungsbehörden Zugriffsrechte zu gewähren[40]. AWS kündigte an, ihre

[37] IKT-Sicherheitsportal, *Payment Card Industry Data Security Standard*.
[38] CIS, *CIS Benchmarks*.
[39] Google, *EU DORA – Compliance*.
[40] Ebd.

Kund:innen beim Herstellen der Compliance mit DORA zu unterstützen[41]. Selbiges gilt für Salesforce[42]. Besonders im österreichischen Umfeld ist interessant, dass GCP Unterstützungsangebote zur Compliance für das BWG bereitstellt und ein entsprechendes Mapping zu den Outsourcing-Bedingungen und ihrer Umgebung erstellt hat[43]. Hinsichtlich Outsourcing-Vorgaben der ESMA ist auch hier GCP der alleinige Anbieter. Die Vorgaben der EBA deckt sowohl Azure als auch GCP ab. Die gängigsten Zertifizierungen im Bereich Cybersicherheit und Cloud-Betrieb, wie CSA, SOC, CIS und verschiedene Varianten von ISO/IEC decken alle drei untersuchten Unternehmen ab.

Für NISR2 hat Google in einem Beitrag angekündigt, analog zu DORA, Kund:innen bei der Umsetzung unterstützen zu wollen[44]. Ähnliches hat Amazon in einem veröffentlichten Whitepaper angekündigt, dabei aber auch auf das Shared Responsibility Model, also der geteilten Verantwortung zwischen Kund:innen und Cloud-Anbietern, verwiesen[45]. Ferner wurde dezidiert auf den Unterschied zwischen Sicherheit der Cloud und Sicherheit in der Cloud verwiesen:

> *„Generally, AWS manages security of the cloud, by verifying that AWS Cloud Infrastructure complies with global and regional regulatory requirements and good practices for cloud providers.[...]Security in the cloud is typically the responsibility of the customer.“*[46]

Ein einfaches Abgeben der gesamten Verantwortung und Pflichten an den Cloud-Anbieter scheint hier AWS bereits nicht möglich zu machen und möchte scheinbar bei Kund:innen Bewusstsein schaffen, dass für Sicherheit auf beiden Seiten etwas zu tun ist.

Ein wichtiger Punkt in diesem Kontext ist die Differenzierung zwischen Compliance und rechtlichen Notwendigkeiten. So definiert das Austrian Standards International (vormals Austrian Standards Institute, davor Österreichisches Normungsinstitut) den Begriff Compliance:

> *„[...]dass sich Organisationen und deren Mitarbeiterinnen und Mitarbeiter an geltende Gesetze – zum Beispiel an das Kartellrecht –, aber auch an interne Regelungen zu ethischen Standards [...] halten müssen.“*[47]

Compliance ist damit deutlich breiter als das bloße Befolgen von Gesetzen. Entsprechende Regeln müssen den Mitarbeiter:innen klar und verständlich vermittelt werden und

[41] Amazon, *AWS responds to European Supervisory Authorities' second consultation on technical standards under the Digital Operational Resilience Act (DORA) | AWS for Industries.*
[42] Salesforce, *UPDATED: DORA FAQ (March 2023).*
[43] Google, *BWG (Österreich) – Compliance.*
[44] Google, *How Google Cloud is preparing for NIS2 and supporting a stronger European cyber ecosystem.*
[45] Amazon, *NIS2 Considerations for Customers*, S. 5–7.
[46] Ebd., S. 7–8.
[47] Austrian Standards, *Compliance: Definitionen, Begriffe, Standards und Richtlinien — austrian-standards.at.*

beinhalten üblicherweise auch den Verhaltenskodex (Code-of-Conduct)[48]. Compliance wird häufig mit einem Compliance-Management-System (CMS) abgebildet[49]. Bestehende CMS können jedoch keine bisher nicht existierenden Gesetze (z.B. die nationale Umsetzung der NISR2) oder noch in Arbeit befindliche Zertifizierungen abbilden. Auch für bereits etablierte Gesetze gibt es laufend neues Unterstützungsmaterial (beispielsweise NIS Fact Sheets), das den Weg in ein derartiges Managementsystem erst finden muss. Diese zeitliche Verzögerung könnte verkürzt werden, indem schon frühzeitig veröffentlichte Entwürfe von Regulativen eingearbeitet werden, selbst wenn die finalen Vorgaben noch nicht bis ins Detail feststehen. Daneben werden Vorgaben oft von Branchenverbänden oder Kammern entsprechend aufbereitet, um eine Übersetzung in konkrete Vorgaben für den Endadressat zu vereinfachen.

6.3 Service Level Agreements

Im Folgenden wurden die drei größten Public Cloud-Anbieter Azure, GCP und AWS anhand ihrer Service Level Agreements (SLA) verglichen. Alle betrachteten Unternehmen berechnen die Verfügbarkeit monatsweise. Um Vergleichbarkeit herzustellen, wurde das Service „virtuelle Maschine“ (VM) hergenommen. Einen Überblick zu den Unterschreitungen bzw. Folgen liefert Tabelle 6.2. Sämtliche Modelle sehen ausschließlich Gutschriften für Unterschreitungen der Vereinbarungen vor. Betreiber kritischer Infrastruktur müssen sich fragen, ob die im Folgenden dargestellten Kompensationen den potenziellen Schaden eines Ausfalls ausgleichen. Die angebotenen Gutschriften sind bei allen Anbietern sehr ähnlich ausgestaltet und unterscheiden sich nur marginal. Nennenswerte Unterschiede wurden bei der Berechnungsmethode zur Verfügbarkeit identifiziert. Für Details zum generellen Thema Verfügbarkeit siehe Abschnitt 2.3.

Microsoft Azure

Microsoft bietet für viele Onlinedienste eine Verfügbarkeit von 99,9 % an; üblicherweise werden für eine Verletzung zwischen 10 und 25 % der Servicegebühren gutgeschrieben

[48] Austrian Standards, *Compliance: Definitionen, Begriffe, Standards und Richtlinien — austrian-standards.at*.
[49] Ebd.

Verfügbarkeit	AWS	Azure	GCP
Unter 99,99 %	10 %	10 %	10 %
Unter 99 %	30 %	25 %	25 %
Unter 95 %	100 %	100 %	100 %

Tabelle 6.2: Vergleich zwischen den Gutschriften bei SLA-Verletzungen (basierend auf den Informationen aus Amazon, *Amazon Compute Service Level Agreement*; Microsoft, *Service Level Agreement for Microsoft Online Services*; Google, *Compute Engine Service Level Agreement (SLA)*)

und bei größeren Verletzungen im Extremfall bis zu 100 % für bestimmte Services (wobei für ein Service nie mehr gutgeschrieben wird, als bezahlt wurde)[50]. Für das konkrete Service VM gibt es beispielsweise 99,99 % Verfügbarkeit mit einer Gutschrift von 10 % für Unterschreitungen bzw. 25 % für weniger als 99 % und den Gesamtersatz bei unter 95 %. Zur Berechnung verwendet Microsoft folgende Formel:

$$U = ((M - D)/M) * 100 \tag{6.1[51]}$$

Dabei bezeichnet U die monatliche Betriebszeit (Uptime) in Prozent, M die maximale Verfügbarkeit in Minuten und D die summierte Ausfalldauer (Downtime) in Minuten.

Monatliche Wartungsfenster, die eine Ausfallzeit zur Folge haben, sind von der Berechnung ausgenommen[52]. Ferner kann ein Verlangsamen der Services aufgrund des Verdachts missbräuchlichen Verhaltens erfolgen, ohne dass dadurch Gutschriften aus dem SLA schlagend werden[53]. In Microsofts Dokument zu SLAs wurde nicht explizit erläutert, welche Konsequenzen ein falscher Verdacht hat. Bei einer Abhängigkeit der Netzwerkverbindung zu einem einzigen Rechenzentrum ist der Ausfall desselbigen nicht vom SLA erfasst[54]. Gleichermaßen muss bei einer Verständigung der Kund:innen durch Microsoft, dass diese ihre Servicebenutzung ändern müssen, dieser nachgekommen werden[55]. Daraus könnte gefolgert werden, dass Microsoft den Kund:innen vorgeben kann, wie diese ein Service zu nutzen haben, wenn diese eine entsprechende Verfügbarkeit haben möchten.

Azure hat für das Jahr 2024 insgesamt acht sogenannte Post Incident Reviews (PIR) zu Servicezwischenfällen veröffentlicht[56].

Google Cloud Platform (GCP)

GCP unterscheidet zwischen Premium-Tier mit besseren Verfügbarkeiten und dem Standard-Tier[57]. Es gibt für das Service VM im Premium-Tier 99,99 % Verfügbarkeit mit einer Gutschrift von 10 % für Unterschreitungen bzw. 25 % für weniger als 99 % und dem Gesamtersatz bei unter 95 %[58]. Die Berechnung erfolgt folgendermaßen:

$$U = ((T - D)/T) * 100 \tag{6.2[59]}$$

[50] Microsoft, *Service Level Agreement for Microsoft Online Services*, S. 6.
[51] Ebd., S. 89.
[52] Ebd., S. 6.
[53] Ebd., S. 6.
[54] Ebd., S. 6.
[55] Ebd., S. 6.
[56] Microsoft, *Azure status history*.
[57] Google, *Compute Engine Service Level Agreement (SLA)*.
[58] Google, *Cloud Compliance – Vorschriften und Zertifizierungen*.
[59] Ebd.

Dabei bezeichnet U den monatlichen Verfügbarkeitsprozentwert (Uptime), T die Gesamtsumme an Minuten in einem Monat und D die Summe aller Ausfallzeiten (Downtime) in einem Monat in Minuten.

Für das Jahr 2024 hat GCP insgesamt 261 Zwischenfälle für alle Produkte berichtet[60]. Die Vergleichbarkeit zwischen Public Cloud-Anbietern in Hinblick auf Zwischenfälle ist allerdings nur sehr beschränkt gegeben, da in Abhängigkeit davon, wie ein Unternehmen einzelne Funktionen zu Produkten zusammenfasst und Zwischenfälle betrachtet, die Ergebnisse variieren.

Amazon Web Services (AWS)

AWS kann entsprechend der Kund:innenvereinbarung SLAs ändern oder kündigen, verpflichtet sich aber, das mindestens 90 Tage zuvor anzukündigen[61]. Kund:innen müssen folglich in der Lage sein, in der genannten Frist Service oder Dienstleister zu wechseln, wenn sich ein SLA derart verändert, dass es für den von den Kund:innen vorgesehenen Verwendungszweck nicht mehr einsetzbar ist. Für Preisänderungen sieht AWS überhaupt nur 30 Tage vor[62]. Im Service VM bietet AWS 99,99 % Verfügbarkeit, mit einer Gutschrift von 10 % bei Unterschreitung bzw. 30 % bei weniger als 99,0 % und 100 % bei weniger als 95,0 %[63]. AWS zahlt damit bei einer Verletzung von 99,0 % um 5 Prozentpunkte mehr Gutschrift als die anderen beiden Cloud-Anbieter. Die Berechnung erfolgt anhand folgender Formel:

$$U = 100 - D \tag{6.3[64]}$$

Dabei bezeichnet U die monatliche Betriebszeit (Uptime) in Prozent und D die prozentuellen Minuten eines Monats, in dem das Service ausgefallen war.

Für AWS konnten keine vom Anbieter offiziell veröffentlichten Informationen zu historischen Zwischenfällen und Ausfallzeiten gefunden werden.

6.4 Datenzugriffe durch Behörden und staatliche Stellen

6.4.1 Anfragen im Kontext der internationalen Rechtsdurchsetzung

Microsoft, Amazon und Google veröffentlichen regelmäßig Berichte zu Zugriffsanfragen durch Organe der Rechtsdurchsetzung bzw. Behörden. Die Anzahl der eingegangenen Anfragen für das Jahr 2022 ist in Abbildung 6.2 zwischen den Anbietern gegenübergestellt

[60] Google, *Google Cloud Service Health*.
[61] Amazon, *AWS Customer Agreement*, Section 1.6.
[62] Ebd., Section 3.1.
[63] Amazon, *Amazon Compute Service Level Agreement*.
[64] Ebd.

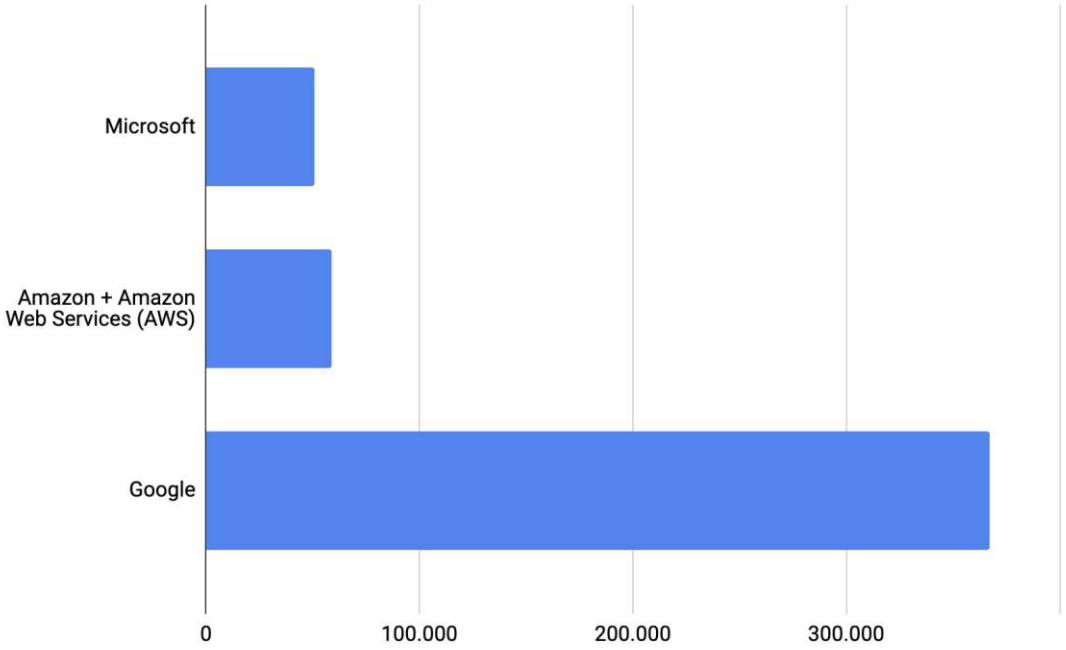

Abbildung 6.2: Weltweite Anfragen nach Kundendaten durch Behörden 2022 (basierend auf Amazon, *Amazon Information Request Report H1*, Amazon, *Amazon Information Request Report H2*, Google, *Auskunftsersuchen zu Nutzerdaten – Google Transparenzbericht* und Microsoft, *Law Enforcement Request Report* – Ersuchen um Offenlegung von Nutzerdaten)

(ausgenommen davon sind Anfragen im Zusammenhang mit nationaler Sicherheit der USA). Google bekam dabei mit Abstand die meisten Anfragen. Möglicherweise resultiert die größere Anzahl aus den anderen Geschäftsbereichen, etwa dem Suchmaschinendienst. Von allen im betrachteten Zeitraum eingegangenen Anfragen legte Google in 76 % - 79 % der Fälle Informationen offen[65]. Sowohl Microsoft als auch Google veröffentlichen die Prozentwerte der Offenlegungen ebenfalls für einzelne Länder: Dabei zeigen sich teils große Unterschiede. So hat beispielsweise Microsoft im Q2 2022 zu Anfragen aus Russland keine Daten offengelegt, mit der Begründung, dass rechtliche Anforderungen nicht erfüllt seien[66]. Für Österreich wurden mit der gleichen Begründung in nur 27,9 % der Fälle keine Informationen preisgegeben[67].

[65] Google, *Auskunftsersuchen zu Nutzerdaten – Google Transparenzbericht*.
[66] Amazon, *Amazon Information Request Report H2*.
[67] Ebd.

6.4.2 Anfragen im Kontext der US-amerikanischen nationalen Sicherheit

Neben Anfragen zur Offenlegung bestimmter Kund:innendaten zum Zweck der Rechtsdurchsetzung aus unterschiedlichen Nationen gibt es Anfragen mit Bezug auf die nationale Sicherheit der USA.

Dabei kommen je nach Anwendungsfall der National Security Letter (NSL) und der Foreign Intelligence Surveillance Act (FISA) (siehe Abschnitt 4.11) zum Einsatz. Bei beiden werden nur Spektren – beginnend bei null bis zu einem bestimmten Wert –, in denen sich die tatsächliche Anzahl der Anfragen bewegt, durch die Cloud-Anbieter veröffentlicht. Wie viele Anfragen es tatsächlich gegeben hat, kann dabei nicht abgeleitet werden, nur dass eine bestimmte Anzahl nicht überschritten wurde, nämlich das obere Ende des Spektrums. Für einen vergleichenden Überblick zwischen den Anbietern für das Jahr 2022 im Zusammenhang mit NSL-Anfragen siehe Abbildung 6.3. Im selben Zeitraum wurden von Behörden insgesamt 10.941 NSLs ausgestellt[68]. Anfragen basierend auf FISA sind in Abbildung 6.4 dargestellt. Laut einem jährlichen Bericht des Office of the Director of National Intelligence (ODNI) gab es im Vergleichszeitraum 2022 insgesamt 246.073 sogenannte Ziele nach FISA (erfasst sind nur Nicht-US-Bürger:innen)[69], wobei in einer Anfrage zur Offenlegung von Daten mehrere Ziele enthalten sein können.

[68] Office of the Director of National Intelligence, *Annual Statistical Transparency Report*, S. 40.
[69] Ebd., S. 18.

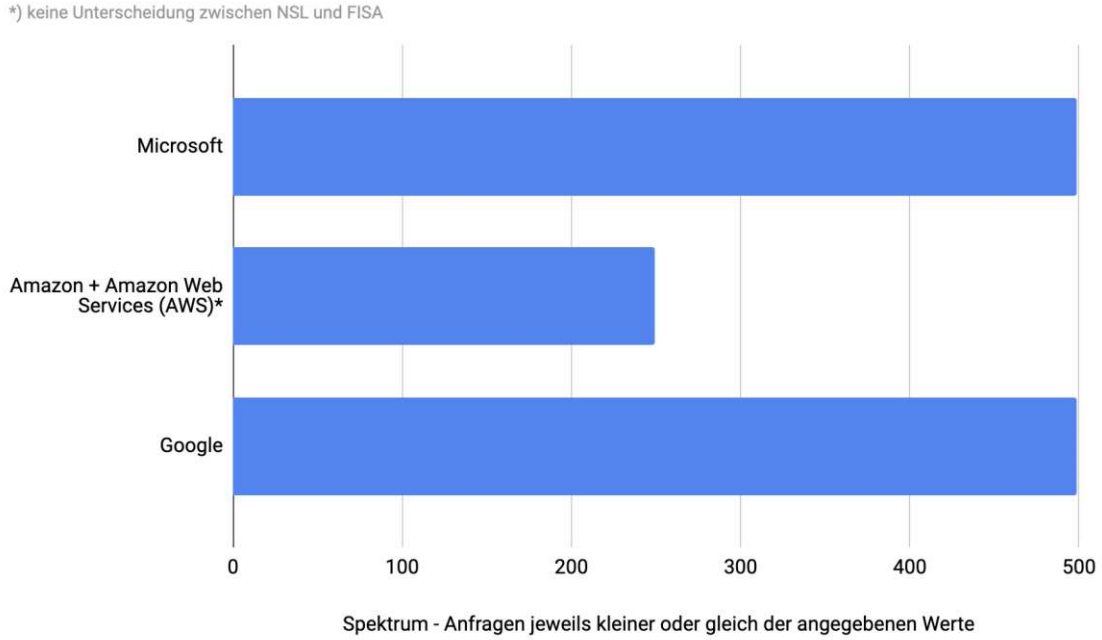

Abbildung 6.3: Maximale Anzahl der Anfragen basierend auf NSL Q1–Q2 2022 (basierend auf Amazon, *Amazon Information Request Report H1*, Amazon, *Amazon Information Request Report H2*, Microsoft, *US National Security Orders Reports | Microsoft CSR* und Google, *Auskunftsersuchen zu Nutzerdaten – Google Transparenzbericht*)

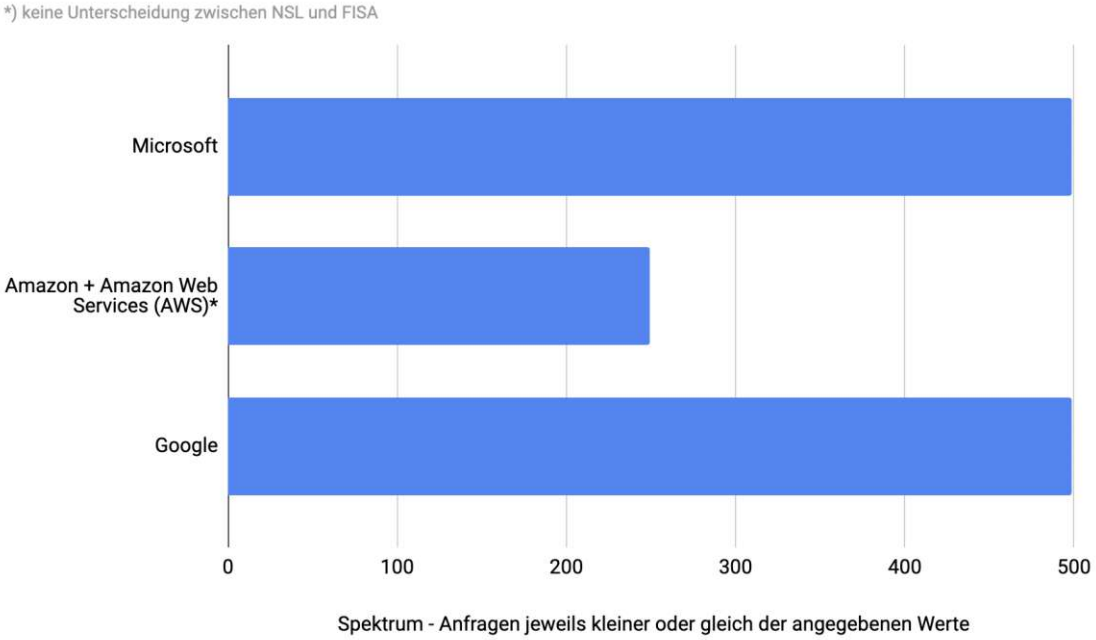

Abbildung 6.4: Maximale Anzahl der Anfragen basierend auf FISA Q1–Q2 2022 (basierend auf Amazon, *Amazon Information Request Report H1*, Amazon, *Amazon Information Request Report H2*, Microsoft, *US National Security Orders Reports | Microsoft CSR* und Google, *Auskunftsersuchen zu Nutzerdaten – Google Transparenzbericht*)

6.5 Sovereign Clouds

Alle großen Public Cloud-Unternehmen bieten Europa als Datenresidenz an. Das bedeutet im Cloud-Kontext, dass Kund:innen die Wahl haben ihre Daten in bestimmten geographischen Lokationen, Ländern oder Regionen zu speichern, üblicherweise um damit lokalen Datenschutz- und Sicherheitsvorgaben gerecht zu werden[70]. Manche Cloud-Anbieter sind dazu übergegangen, Sovereign Clouds in ihr Portfolio aufzunehmen. Es gibt keine einheitliche Definition des Begriffs Sovereign Cloud: Manche verstehen darunter die Unabhängigkeit von einer spezifischen Technologie, andere den Einsatz von Open-Source-Lösungen[71]. Oracle nutzt etwa für ihre EU Sovereign Cloud separate europäische juristische Personen[72]. Damit soll ein besserer Schutz vor Nicht-EU-Anfragen zur Datenoffenlegung bestehen[73]. Oracle vertritt in einem Artikel die Ansicht, dass sie im Fall von Anfragen im Zusammenhang mit dem CLOUD Act keinen Zugriff auf EU Sovereign Cloud Daten haben[74].

Auch Amazon plant eine europäische Sovereign Cloud bzw. deren Ausbau und will über 7 Milliarden Euro in dieselbige investieren[75]. Dazu stehen sogenannte Dedicated Local Zones bereit, die von Kund:innen exklusiv genutzt und in einer gewünschten Gerichtsbarkeit verortet sind[76]. Sie werden von Amazon verwaltet bzw. betrieben und Amazon trägt dabei auch die Verantwortung für Konnektivität und Kapazitätsplanung[77]. Überdies gibt es Outposts, die On-Premises installiert sind und AWS-Technologie nutzen[78]. Wobei die Konnektivität, die Kapazitätsplanung, die Sicherheit der Einrichtung und der Betrieb allerdings im Verantwortungsbereich der Kund:innen liegen[79].

Es konnten jedoch keine Hinweise gefunden werden, ob durch all diese Maßnahmen im Zusammenhang mit Sovereign Clouds ein Schutz vor Offenlegungen durch den CLOUD Act, FISA oder NSL besteht. Unter Umständen liefern Outposts noch am ehesten Hinweise, ob ungewollt Daten abfließen, da hier Kund:innen Kontrolle über das Netzwerk haben und anhand des übermittelten Datenvolumens entsprechende Schlüsse ziehen könnten.

[70] Jackley, *Data Sovereignty vs. Data Residency: 3 Key Differences.*
[71] Rath, Keller und Spies, „Sovereign Clouds — An overview of the current privacy challenges associated with the use of US cloud services, and how sovereign clouds can address these challenges“.
[72] Oracle, *Oracle sovereign cloud solutions: Providing transparent review of data access requests.*
[73] Ebd.
[74] Ebd.
[75] Amazon, *AWS plans to invest €7.8B into the AWS European Sovereign Cloud.*
[76] Amazon, *Dedicated Local Zones FAQs Page.*
[77] Ebd.
[78] Ebd.
[79] Ebd.

KAPITEL 7

Auswertung von Sicherheitsvorfällen

7.1 Sicherheitsvorfälle bei Betreibern kritischer Infrastruktur in Österreich

7.1.1 Vorgehensweise

Es wurden bei den Internet-Suchmaschinen *google.com* und *bing.com* nach IT-Sicherheitsvorfällen bei österreichischen wesentlichen oder wichtigen Organisationen gesucht. Sowohl die Textsuche als auch die Nachrichtensuche wurden dabei genutzt. Zeitlich wurde dabei vom Verfassen dieses Kapitels – März 2024 – bis ins Jahr 2016 zurückgegangen. Folgende Suchbegriffe wurden dazu verwendet:

- *Hackerangriff Österreich*
- *Cyberangriff Österreich*
- *IT-Angriff Österreich*
- *Hackerangriff Unternehmen Österreich*
- *Cyberangriff Unternehmen Österreich*
- *IT-Angriff Unternehmen Österreich*

Die gefundenen Vorfälle wurden nach möglichen Sektoren und dazugehöriger Kritikalität (wesentlich/wichtig) der NISR2 kategorisiert. Diese Einstufung und Klassifizierung wurde durch den Autor dieser Arbeit anhand öffentlicher Informationen zu den Organisationen

selbst eingeschätzt und dient nur der Vergleichbarkeit. Die streng juristische Beurteilung am Maßstab von NISR2 kann natürlich eine andere sein. Zusätzlich wurde nach Umfang der verfügbaren Daten, die Art der Bedrohung (z.B. Ransomware , Data Leak bzw. Breach) und der Einstiegspunkt (z.B. Phishing) erhoben. Die Rohdaten der Auswertung finden sich tabellarisch dargestellt im Anhang Abschnitt B.1. Allerdings ist davon auszugehen, dass das Dunkelfeld größer und nicht beurteilbar ist.

7.1.2 Auswertung

Beim größten Teil der erhobenen Vorfälle (40,5 %) war die Art der Bedrohung unbekannt bzw. wurde in den dazugehörigen Berichten nicht erwähnt (siehe Abbildung 7.1). Die nächstgrößte Art war ein Datenleck (Data Leak bzw. Breach) mit 24,3 %, bei dem es zu unerlaubten Zugriff auf Daten kam. Dicht folgend war Ransomware (Verschlüsselungs-/Erpressungssoftware) mit 21,6 %. Im einstelligen Bereich waren Denial-of-Service-Angriffe und CEO-Fraud – also wenn Mitarbeiter:innen durch Betrug dazu gebracht werden, unerlaubte Transaktionen durchzuführen[1] – zu finden. Von bloßen Versuchen wurde in 2,7 % der Fälle berichtet, wobei über derartige Ereignisse aufgrund des fehlenden Neuigkeitswerts vermutlich in den seltensten Fällen in den Medien berichtet wird. Je nach Branche kann sich ein Sicherheitsvorfall unterschiedlich stark auswirken; so ist ein Datenleck bei einem Kraftwerk möglicherweise weniger drastisch wie bei einer Bank oder in der öffentlichen Verwaltung, wo teils sensible Informationen verarbeitet werden. Gleichzeitig ist ein Denial-of-Service-Angriff bei weniger zeitkritischen Sektoren, wie z.B. der Forschung unproblematischer als beim Kraftwerksbetrieb.

Bei den betroffenen Sektoren (siehe Abbildung 7.2) stach primär das verarbeitende Gewerbe bzw. das Gewerbe für Herstellung von Waren heraus, bei dem fast doppelt so viel über Sicherheitsvorfälle berichtet wurde wie beim zweithäufigsten Sektor, nämlich der öffentlichen Verwaltung. Erstere ist allerdings auch die umsatzstärkste Branche unter den genannten[2]. Der drittgrößte Bereich betrifft die Forschung, obwohl sie im Vergleich zu den anderen Sektoren wohl deutlich kleiner ist. Möglicherweise wird dort besonders offen über Vorfälle kommuniziert, weil ein Imageschaden unwahrscheinlicher ist.

Bei der vom Autor durchgeführten Kategorisierung anhand NISR2 in wesentliche und wichtige Betreiber kritischer Infrastruktur war die Anzahl der berichteten Vorfälle fast identisch (siehe Abbildung 7.3). Einen leichten Überhang gab es bei den wesentlichen Betreibern mit 51,4 % im Gegensatz zu den wichtigen Einrichtungen mit 48,6 %. Der Überhang bei wesentlichen Betreibern ist insofern interessant, als viele Betreiber durch NISG schon stärker reguliert sein können als wichtige Betreiber. Unter den Annahmen, dass beide Gruppen gleichermaßen von Vorfällen berichten, sie gleich häufig im Visier von Cyberangriffen stehen und die Umsetzung von NISG 2024 ihre positiven Effekte entfaltet, müsste sich zukünftig der Überhang der wesentlichen Betreiber bei Sicherheitsvorfällen zurückentwickeln.

[1] Bundeskriminalamt, *CEO Fraud*.
[2] Statista, *Umsatz Branchen Österreich 2022*.

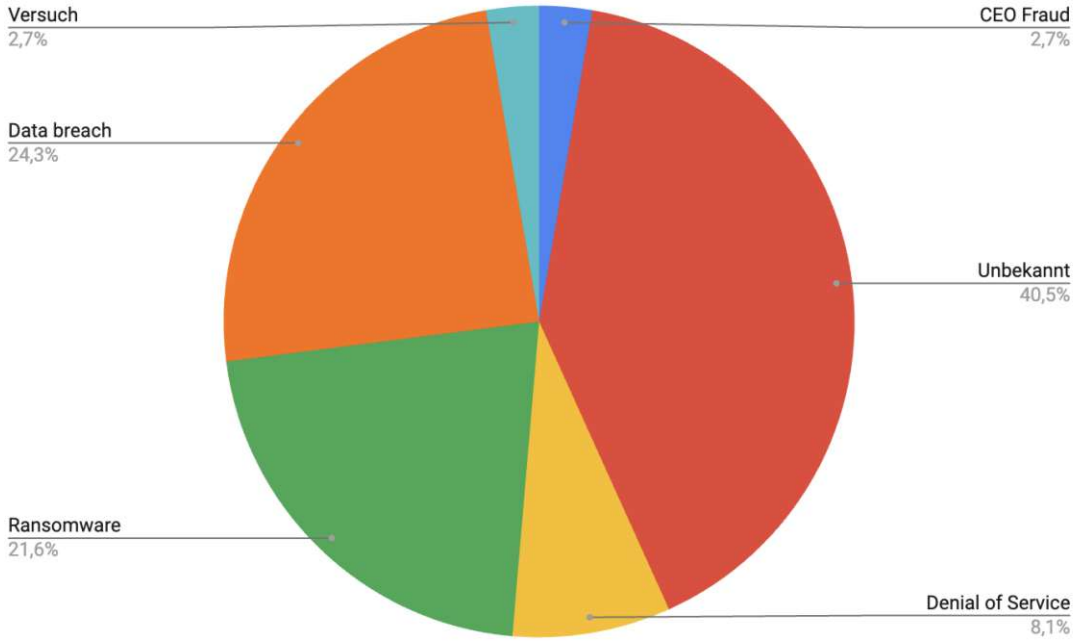

Abbildung 7.1: Arten von Sicherheitsvorfällen bei Betreibern kritischer Infrastruktur in Österreich (basierend auf Daten aus Abschnitt B.1)

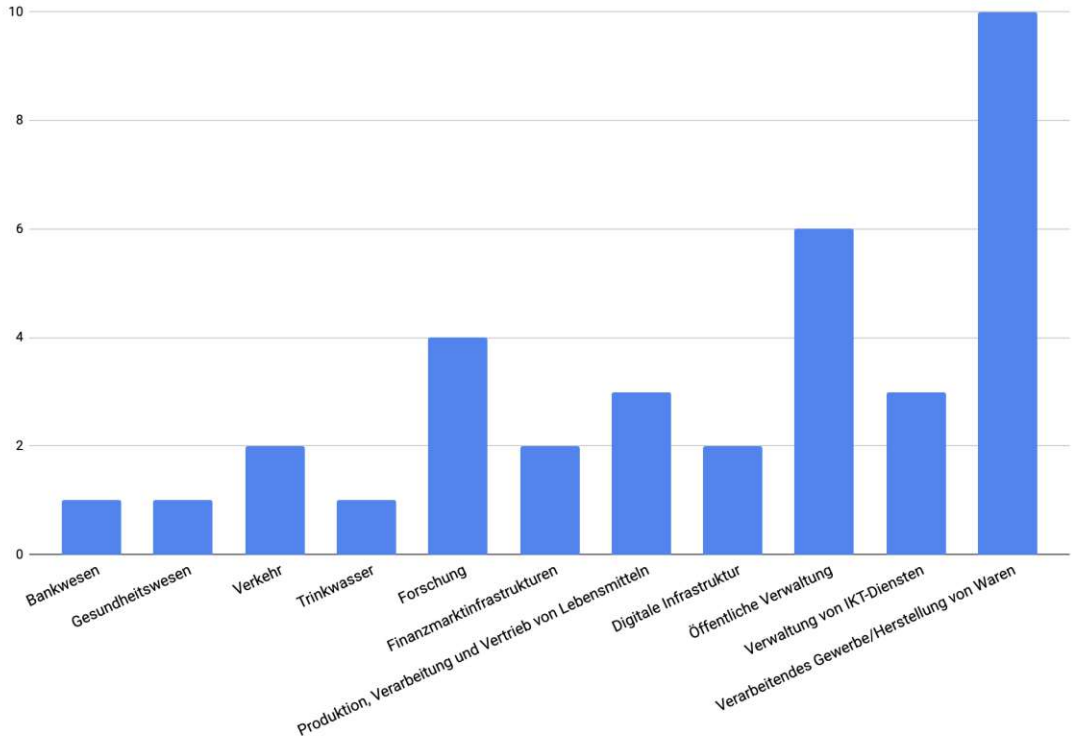

Abbildung 7.2: Von Sicherheitsvorfällen betroffene Sektoren bei Betreibern kritischer Infrastruktur in Österreich (basierend auf Daten aus Abschnitt B.1)

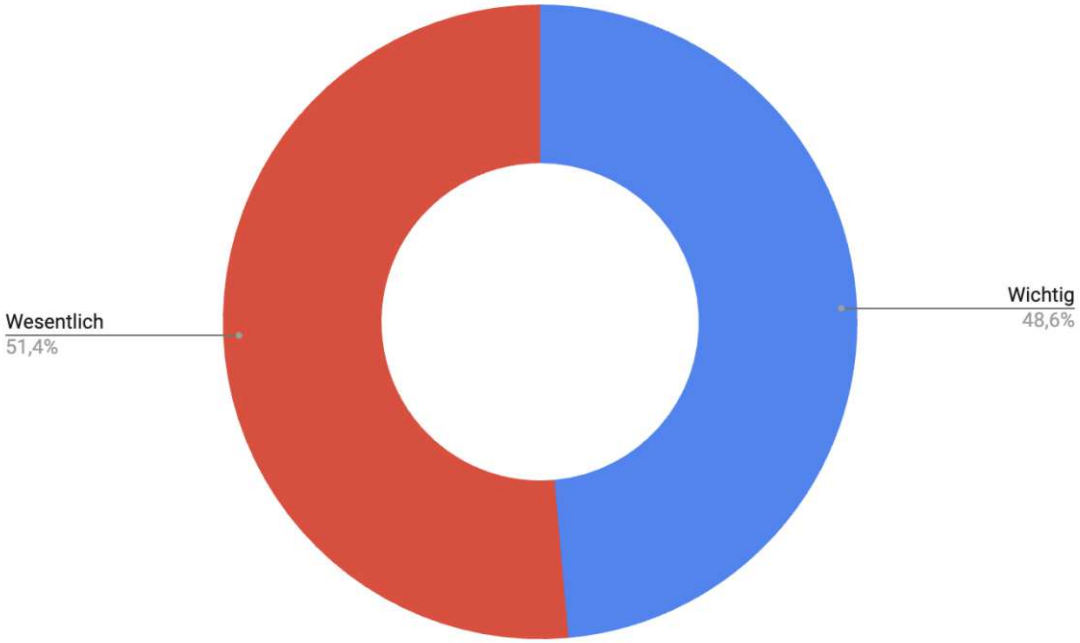

Abbildung 7.3: Kategorien von Betreibern kritischer Infrastruktur in Österreich, bei denen Sicherheitsvorfälle gemeldet wurden (basierend auf Daten aus Anhang Abschnitt B.1)

7.2 Sicherheitsvorfälle mit Bezug zu Public Cloud

7.2.1 Vorgehensweise

Ähnlich zur Vorgehensweise in Abschnitt 7.1 wurde bei den Internet-Suchmaschinen *google.com* und *bing.com* nach IT-Sicherheitsvorfällen mit Bezug Public Cloud gesucht. Der Fokus wurde auf die größten Anbieter – nach Marktanteil 2024 laut Statista[3] – gelegt. Es kamen Textsuche und Nachrichtensuche zum Einsatz. Zeitlich wurde dabei vom Verfassen dieses Kapitels – Mai 2024 - bis ins Jahr 2016 zurückgegangen. Folgende Suchbegriffe wurden dazu verwendet, in Kombination mit den Namen der unterschiedlichen Anbieter:

- *Cloud-Security Incident*
- *Cloud-Security Breach*
- *Cloud-Breach*
- *Cloud-Leak*
- *Cloud-Data Leak*

Die Ergebnisse werden in Unterabschnitt 7.2.2 präsentiert und grafisch aufbereitet. Ausgewertet wurden dabei die möglichen Ursachen und potenziellen Folgen der Vorfälle. Sowohl Ursachen als auch Folgen wurden vom Autor dieser Arbeit anhand der öffentlich zugänglichen Informationen angenommen – die tatsächlichen Ursachen und Folgen könnten natürlich auch andere gewesen sein, insbesondere da viele Details bei Vorfällen nicht öffentlich sind. Die Rohdaten der Auswertung finden sich tabellarisch dargestellt im Anhang Abschnitt B.1.

7.2.2 Auswertung

In 61,3 % der ermittelten Vorfälle (siehe Abbildung 7.4) war eine Fehlkonfiguration ursächlich für Sicherheitsvorfälle. Allerdings haben in vielen der berichteten Fällen die Nutzer:innen selbst eine fehlerhafte Konfiguration vorgenommen. In diesem Kontext ist besonders das Shared Responsibility Model zu erwähnen (siehe Unterabschnitt 2.6.2), das die Verantwortlichkeit zwischen Kund:innen und Cloud-Anbietern regeln soll. Bei vielen Ereignissen (19,4 %) ließ sich anhand der öffentlichen Informationen eine potenzielle Ursache nicht eruieren, da die entsprechenden Berichte zu wenig detailreich oder uneindeutig waren. Mit 9,7 % war der drittgrößte Bereich verursacht durch Schwachstellen (Vulnerability) in diversen Systemen, gefolgt von Lieferkettenangriffen (Supply Chain Attack) mit 6,5 % und Phishing (3,2 %).

Die mit Abstand am häufigste Folge von Sicherheitsvorfällen mit Bezug zu Public Cloud war die Datenpanne (Data Leak bzw. Breach) mit 74,2 % (siehe Abbildung 7.5). Die

[3] Statista, *Global cloud infrastructure market share 2024*.

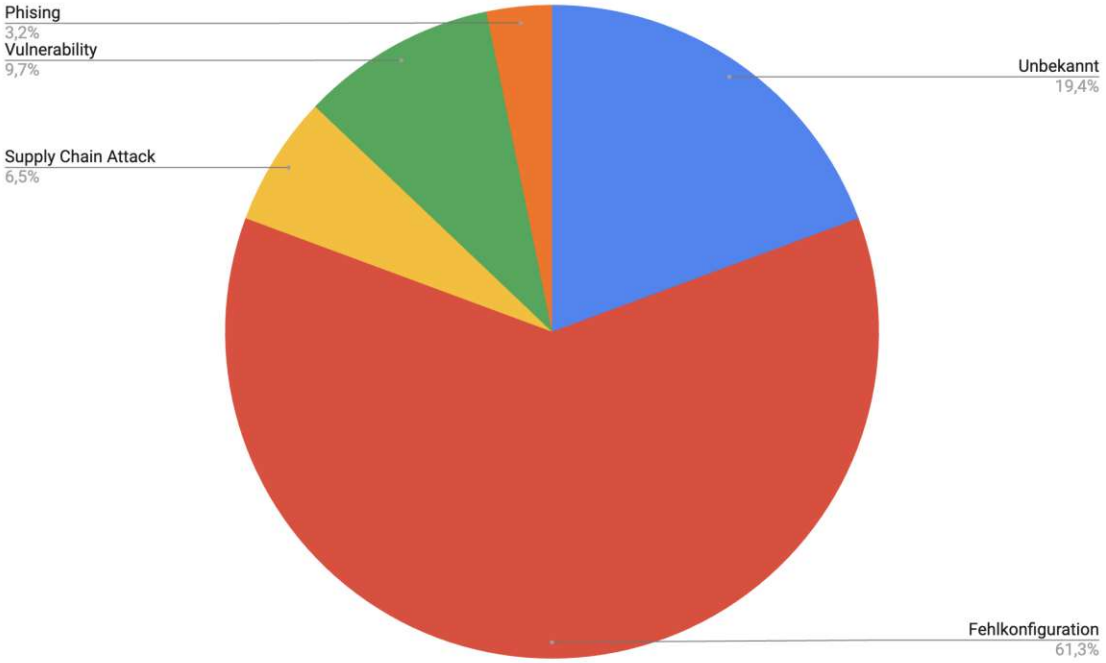

Abbildung 7.4: Mögliche Ursachen von Sicherheitsvorfällen mit Bezug zu Public Cloud (basierend auf Daten aus Anhang Abschnitt B.2)

anderen Folgen kamen selten vor bzw. waren untereinander schwer zu differenzieren. Fast immer gab es eine Art von Datenabfluss in eine unerlaubte Richtung. In einem Fall kam es zu Cryptojacking.

7.2.3 Nennenswerte Vorfälle im Detail

Im Folgenden werden zwei Sicherheitsvorfälle bei großen Public Cloud-Anbietern genauer beschrieben, die medial viel Verbreitung fanden und wohl zu den bemerkenswertesten Ereignissen der jüngeren Vergangenheit gehören. Sie sind auch deswegen erwähnenswert, weil sie zu den wenigen Fällen gehören, die möglicherweise nicht eindeutig auf einen Fehler durch die jeweiligen Kund:innen zurückzuführen sind.

Storm-0558 Exchange Online 2023

Zwischen Mai und Juni 2023 kam es bei einem großen Public Cloud-Anbieter zu einem Sicherheitsvorfall – mutmaßlich durch die Gruppe Storm-0558 – bei dem durch gefälschte Authentifizierungstoken unerlaubter Zugriff auf E-Mails von ca. 25 Einrichtungen, darunter auch Regierungsbehörden, stattgefunden haben soll[4]. Die Authentifizierungstoken seien mit einem Microsoft Account (MSA) Signaturschlüssel aus dem Consumer-Bereich des Jahres 2016 erstellt worden, dieser soll allerdings auch für Enterprise Umgebungen

[4]Microsoft, *Analysis of Storm-0558 techniques for unauthorized email access.*

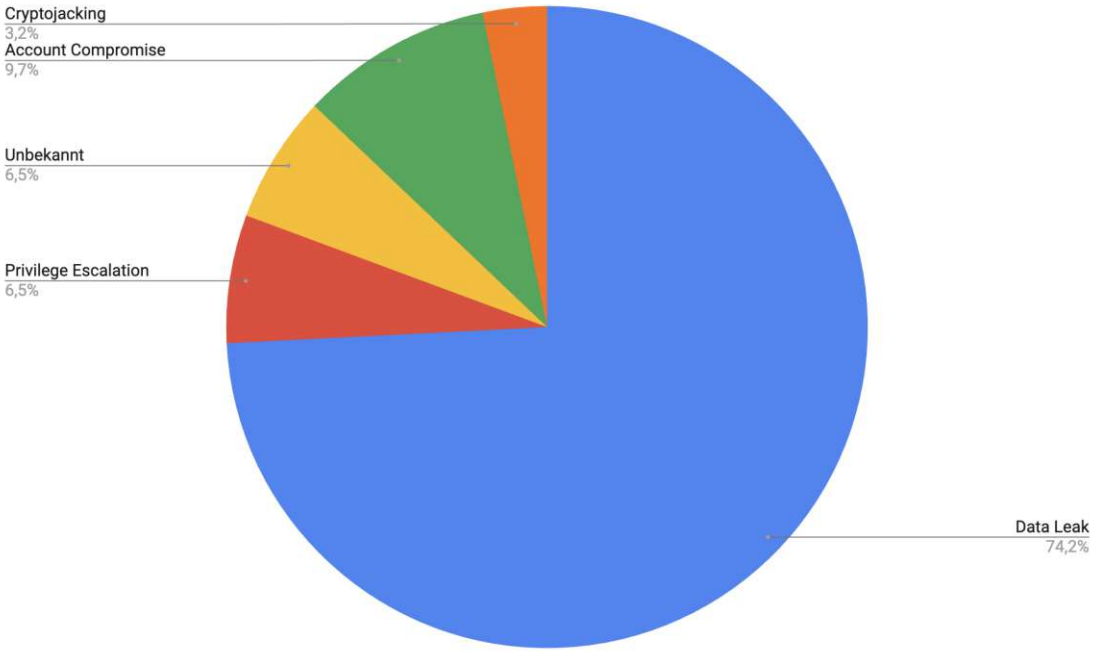

Abbildung 7.5: Mögliche Folgen von Sicherheitsvorfällen mit Bezug zu Public Cloud (basierend auf Daten aus Anhang Abschnitt B.2)

gültig gewesen sein[5]. Ursprünglich wurde berichtet, dass der Bedrohungsakteur den Zugang zu jenem Schlüssel über einen Crash Dump nach einem Absturz des Consumer-Signatursystems im April 2021 erlangt hat[6]. Allerdings konnte nachträglich kein entsprechender Crash Dump gefunden werden, in dem sich der Schlüssel befunden hätte[7]. Nach einem Bericht der Cybersecurity and Infrastructure Security Agency (CISA) konnte der betroffene Public Cloud-Anbieter bisher nicht zeigen, wie der Signaturschlüssel durch den Bedrohungsakteur erlangt wurde[8]. Erstmals entdeckt wurden die unerlaubten Zugriffe durch das Außenministerium der Vereinigten Staaten im Juni 2023 wegen Anomalien beim Zugriff auf E-Mailboxen[9]. Dazu war das Außenministerium allerdings nur in der Lage, weil es erweitertes Logging durch entsprechende Lizenzen erworben hatte[10]. Nach einer anonymisierten Quelle im CISA-Report veröffentlichen Cloud-Dienste im Allgemeinen nicht immer ihnen bekannte Schwachstellen und Anfälligkeiten – Common Vulnerabilities and Exposures (CVE) – ihrer Infrastruktur, wenn keine Aktionen der Kund:innen notwendig sind[11]. Für Kund:innen von Cloud-Diensten können sich damit unter Umständen

[5] Microsoft, *Analysis of Storm-0558 techniques for unauthorized email access.*
[6] Microsoft, *Results of Major Technical Investigations for Storm-0558 Key Acquisition.*
[7] Ebd.
[8] Cybersecurity and Infrastructure Security Agency (CISA), *Review of the Summer 2023 Microsoft Exchange Online Intrusion*, S. 2.
[9] Ebd., S. 6.
[10] Ebd., S. 9.
[11] Ebd., S. 6.

Gefahren ergeben, wenn der entsprechende Cloud-Anbieter die Schwachstelle falsch einschätzt oder die Kund:innen eine Konfiguration verwenden, die bei der Behebung keine Beachtung findet. Damit könnten Kund:innen Risiken ausgesetzt sein, die durch offenere Kommunikation reduzierbar wären. Eine bessere Informationspolitik der Cloud-Anbieter wurde im CISA-Bericht als Empfehlung für die Zukunft aufgenommen[12]. Die Gruppe Storm-0558 soll nach Berichten mit einem asiatischen Staat – einschließlich Militär und Geheimdienste – verbunden sein, dessen Regierung auch andere Bedrohungsakteure sponsert[13].

Capital One Data Breach 2019

Am 19. Juli 2019 erfuhr der US-Finanzdienstleister Capital One, dass ein unerlaubter Zugriff auf Informationen seiner Kund:innen stattgefunden hatte, mit ca. 100 Millionen Betroffenen in den USA und ca. 6 Millionen in Kanada[14]. Das Unternehmen hat nach entsprechenden Berichten eine State-of-the-Art Cloud-Infrastruktur genutzt[15]. Der Angriff soll zuerst durch das Ausnutzen eines falsch konfigurierten Reverse Proxys erfolgt sein[16]. Durch diesen Reverse Proxy sei ein Metadaten-Service erreicht worden, das dem Angreifer wiederum temporäre Zugangsdaten verfügbar machte, die zu viele Rechte hatten und unerlaubten Zugang zu den schützenswerten Informationen ermöglichten[17]. Die darunterliegende Infrastruktur des Public Cloud-Anbieters wurde zwar nicht kompromittiert, jedoch sollen Schwächen im Design der Cloud-Infrastruktur durch den Bedrohungsakteur ausgenutzt worden sein[18]. Als eine jener Schwächen wird das Metadaten-Service angeführt, dass die Legitimität bestimmter interner API-Anfragen nicht prüft[19]. Jener Vorfall zeigt, dass ein Einstiegspunkt für einen Angriff durch einen Konfigurationsfehler der Kund:innen passieren kann, aber sich auch nachgelagerte Designschwächen in der Cloud-Infrastruktur verstärkend negativ auswirken können.

7.2.4 Ergebnisse Dritter

Im Zuge des Cloud-Security-Reports 2023, herausgegeben von Check Point Software Technologies Ltd., wurden 1052 Cybersicherheitsexpert:innen im April 2023 zum Thema Cloud und Sicherheit befragt[20]. 24 % der Befragten gaben an, in den vergangenen 12 Monaten einen Sicherheitsvorfall mit Public Cloud-Bezug in ihrer eigenen Organisation erlebt zu haben[21]. Insgesamt waren 19 % auf Fehlkonfigurationen, 16 % auf kompromittierte Accounts, 16 % auf ausgenutzte Schwachstellen und 13 % auf fälschlicherweise durch

[12] Ebd., S. 23.
[13] New Jersey Office of Homeland Security and Preparedness, *2024 Threat Assessment*, S. 38.
[14] One, *2019 Capital One Cyber Incident*.
[15] Khan u. a., „A systematic analysis of the capital one data breach: Critical lessons learned“, S. 2.
[16] Ebd., S. 7.
[17] Ebd., S. 7.
[18] Ebd., S. 15.
[19] Ebd., S. 15.
[20] Check Point Software Technologies Ltd., *Cloud Security Report*, S. 2.
[21] Ebd., S. 4.

Benutzer:innen geteilte Daten zurückzuführen[22]. Aus dem Bericht geht allerdings nicht hervor, ob und welche Vorfälle durch Probleme beim Public Cloud-Anbieter entstanden sind, oder ob es sich um Fehler der Kund:innen handelte.

Einen ähnlichen Bericht hat das Unternehmen Netwrix im Jahr 2022 erstellt. Dabei wurden im März 2022 insgesamt 720 IT-Expert:innen weltweit über ein Onlineformular befragt[23]. 53 % waren von einem Sicherheitsvorfall bei Cloud-Diensten in den vergangenen 12 Monaten betroffen[24]. Am häufigsten mit 73 % kam es zu Phishing-Angriffen, gefolgt von kompromittierten Accounts mit 31 % und Ransomware oder Malware-Zwischenfällen mit 29 % und irrtümlichen Datenlecks mit 25 %[25]. Gezielte Angriffe auf die Cloud-Infrastruktur hat es in 29 % der Fälle gegeben[26]. Vermutlich ist mit diesen gezielten Angriffen gemeint, dass es sich dabei tatsächlich um Probleme beim Cloud-Anbieter handelt. 23 % gaben an, dass die Cloud-Anbieter das größte Risiko für Datensicherheit darstellen, während 39 % die eigenen Mitarbeiter:innen angaben[27].

[22] Check Point Software Technologies Ltd., *Cloud Security Report*, S. 4.
[23] Netwrix, *Cloud Data Security Report*, S. 3.
[24] Ebd., S. 10.
[25] Ebd., S. 10.
[26] Ebd., S. 10.
[27] Ebd., S. 20.

KAPITEL 8

Conclusio und Ausblick

Diese Arbeit widmete sich der Frage, ob und wie Betreiber der kritischen Infrastruktur – mit besonderem Fokus auf Österreich – Cloud-Dienste für Kernkomponenten ihrer Tätigkeit nutzen können. Die umfassende und vergleichende Analyse der rechtlichen Lage ergab, dass es praktisch keine explizit formulierten Verbote für Auslagerungen von Diensten an Cloud-Anbieter für Betreiber der kritischen Infrastruktur gibt. Der Grundtenor ist allerdings, dass eine wirksame Rechtsdurchsetzung und Aufsicht durch die Behörde auch bei Auslagerungen möglich sein muss und Verantwortung nicht einfach an Dienstleister abgegeben werden kann. Der Finanzsektor war diesbezüglich schon bisher in Österreich durch das BWG und die EU-Vorgaben wie die Leitlinien der EBA (zukünftig auch DORA) stärker reguliert als andere Sektoren. Die rechtliche Materie ist aktuell besonders vielen Veränderungen unterworfen und hat sich auch im Laufe dieser Arbeit ständig weiterentwickelt. Es zeigte sich, dass eine Harmonisierung der Vorgaben wünschenswert ist, da viele Anforderungen formuliert wurden, die teils inhaltlich identisch mit anderen Vorgaben sind oder sich selbst sogar widersprechen (zum Beispiel beschreibt DORA den Umgang mit Altsystemen, die es gar nicht geben dürfte, da die Verordnung verlangt, dass alle Systeme aktuell gehalten werden müssen[1]). Zukünftig kommt hinzu, dass wesentliche und wichtige Einrichtungen zur Verwendung von zertifizierten Dienstleistern (europäische Schemata für Cybersicherheitszertifizierung) verpflichtet werden können[2]. Betreiber der kritischen Infrastruktur müssen mit Public Cloud-Anbietern wohl eigene Verträge verhandeln, da Standardprodukte Anforderungen, wie engmaschige Meldepflicht (bereits bei der reinen Möglichkeit von Schäden), höhere Verfügbarkeit oder den unterbrechungslosen Wechsel des Dienstanbieters oft nicht in der geforderten Form abdecken. Ferner müssen Vor-Ort-Kontrollen beim Cloud-Dienstleister durchsetzbar vereinbart werden und Personal, mit Zugang zu kritischen Komponenten, muss einer Zuverlässigkeitsüberprüfung

[1] *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 7 bzw. Art 8 Abs 7.

[2] *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 24 Abs 1.

unterzogen werden[3]. Letzteres ist in der Praxis bei Mitarbeiter:innen in Drittstaaten wohl nur begrenzt aussagekräftig. Europäische Mitgliedstaaten haben vermutlich nur wenig Einblick in Hintergrundinformationen von ausländischen Personen, sofern eine Zuverlässigkeitsüberprüfung überhaupt möglich ist.

Aus geopolitischer Sicht ist die Konzentration aller großen Public Cloud-Anbieter in den USA problematisch. Hier macht sich die österreichische Infrastruktur von unternehmerischen und politischen Entscheidungen weit außerhalb der Einflusssphäre Österreichs und auch der EU abhängig. Anhand der Daten von Public Cloud-Anbietern muss davon ausgegangen werden, dass US-Behörden zur Rechtsdurchsetzung (CLOUD Act), aber auch für Zwecke ihrer Sicherheitsinteressen (FISA) auf Daten der Kund:innen dieser Dienstleister zugreifen – teilweise ohne richterliche Genehmigung. Dieses Vorgehen scheint nur schwer vereinbar mit Vertraulichkeitsanforderungen aus NISR, NISR2, DORA oder europäischen Datenschutzgesetzen. Als möglicher Lösungsansatz wurden Sovereign Clouds identifiziert, in der Form, dass vom Mutterkonzern unabhängige juristische Personen innerhalb der EU gegründet werden, die nicht von US-amerikanischem Recht erfasst werden können. Eine rein europäische Public Cloud mit nennenswertem Marktanteil hat sich bisher nicht etabliert. Ein Lösungsvorschlag wäre eine von öffentlicher Stelle geförderte innereuropäische Cloud-Lösung, um Unabhängigkeit von der starken US-Marktdominanz zu schaffen. In eine ähnliche Stoßrichtung ist das europäische Projekt Gaia-X ausgelegt.

Eine umfassende Auswertung der Mitteilungen zu Sicherheitsvorfällen bei Public Cloud-Diensten ergab, dass relativ zur Größe wenig über Sicherheitsvorfälle berichtet wird. Gleichzeitig betreffen diese Sicherheitsvorfälle dafür eine große Anzahl an Kund:innen. So haben nach Umfragen teilweise über die Hälfte der befragten Public Cloud-Kund:innen angegeben, von Sicherheitsvorfällen betroffen gewesen zu sein[4]. Außerdem sind Public Cloud-Dienste für staatliche oder staatlich unterstützte Bedrohungsakteure besonders interessant, wie der Storm-0558 Exchange Online 2023 Vorfall zeigte. Jene Akteure können sich auf wenige große Cloud-Unternehmen konzentrieren und damit auf einen Schlag eine Vielzahl an Einrichtungen ausspionieren bzw. schädigen. Auch bei der kritischen Infrastruktur in Österreich wurde in den vergangenen Jahren von etlichen Sicherheitsvorfällen – allerdings ohne Informationen zu einem möglichen Cloud-Bezug – berichtet. Die häufigste bekannte Bedrohung waren Datenlecks bzw. unerlaubte Datenzugriffe. Am meisten wurde im verarbeitenden Gewerbe von Sicherheitsvorfällen berichtet. Insgesamt war die Anzahl der Mitteilungen über Sicherheitsvorfälle bei wesentlichen und wichtigen Einrichtungen nach NISR2 fast identisch. Nachdem in letzter Zeit mehr berichtet wurde, könnte gefolgert werden, dass es tatsächlich auch in Österreich zu mehr Sicherheitsvorfällen kommt. Durch neue rechtliche Melde- und Auskunftspflichten wird wohl zusätzlich der Anteil der Veröffentlichungen steigen.

Alle großen Public Cloud-Dienstleister bieten eine Vielzahl von Compliance-Services an, jedoch (noch) keine explizit formulierte Lösung, um die neuen Anforderungen aus

[3] *Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 13 Abs 1.

[4] Netwrix, *Cloud Data Security Report*, S. 10.

NISR2, DORA oder CER zu erfüllen. Bis jetzt fanden sich nur Ankündigungen mit der grundsätzlichen Bereitschaft, zukünftig Kund:innen unterstützen zu wollen. Im Zuge der durchgeführten Expert:inneninterviews wurde die Gefahr identifiziert, dass manche Unternehmen die neuen gesetzlichen Anforderungen aus finanzieller Sicht nicht erfüllen können, weil deren Geschäftsmodell nur sehr knapp wirtschaftlich positiv ist[5]. Jene Unternehmen könnten dann vom Markt verschwinden. Eventuell sind für Unternehmen Cloud-Dienste ein Lösungsansatz, um mit den neuen Bedingungen umzugehen, indem sich der Dienstleister um Teile der Compliance kümmert. Zukünftig wird es interessant, wie in Österreich die Aufsicht von NISR2 bzw. deren nationalstaatliche Umsetzung vonstattengehen kann. Nach Schätzungen sind bis zu 6.000 Einrichtungen betroffen[6] und eine effektive Aufsicht bräuchte entsprechend personelle Ressourcen. Eventuell ist dabei der Einsatz von Cloud-Dienstleistern auch für die Aufsicht hilfreich, indem mit der Prüfung eines einzigen Cloud-Unternehmens automatisch viele Gebiete für ebenfalls regulierte Unternehmen abgedeckt sind, die diese Dienste dort beziehen. Bei den Expert:inneninterviews zeigte sich, dass österreichische kritische Infrastruktur bereits begonnen hat, Kernfunktionen bei Public Cloud-Diensten zu betreiben, auch wenn teils noch Zurückhaltung vorherrscht. Die weiteste Verbreitung war im Finanzsektor wahrnehmbar.

Zukünftig sollte auf europäischer Ebene eine stärkere Vereinheitlichung der Cybersicherheit angestrebt werden. Möglicherweise ist die Art des Rechtsakts für NISR2 – nämlich eine Richtlinie – nicht optimal gewählt und es wäre eine Verordnung passender gewesen, denn durch die Richtlinie kommt es zu unterschiedlichen Umsetzungen in den einzelnen Mitgliedstaaten und wieder zu Differenzen im Niveau der Cybersicherheit. Die digitale Abhängigkeit in der EU ist in den letzten Jahren weiter gestiegen, während gleichzeitig die digitale Souveränität sank. Selbst wenn dies mit Ausnahme der Volksrepublik China ein weltweites Phänomen ist, sollte jene Abhängigkeit bei Entscheidungsträger:innen der zweitgrößten Weltwirtschaftsmacht EU eine dem Problem angemessene Aufmerksamkeit bekommen. Besonders besteht durch die vermehrte Nutzung von Public Cloud-Diensten, auch durch kritische Infrastruktur, die Gefahr, dass nicht nur die digitale Souveränität immer schmäler wird, sondern die Souveränität der Mitgliedstaaten insgesamt gefährdet wird.

[5] Interviewfrage A.4.2
[6] Interviewfrage A.4.2

ANHANG A

Transkripte der Expert:inneninterviews

A.1 Markus Hartleitner

Interviewpartner	Markus Hartleitner
Hintergrund	Cloud Security Leader bei PwC Österreich
Datum	5. März 2024
Uhrzeit	17:15-18:15
Ort	Online-Meeting via MS Teams

A.1.1 Werden Cloud Dienste in der österreichischen kritischen Infrastruktur schon verbreitet eingesetzt und auch bei wesentlichen Funktionen oder aktuell nur bei Support Systemen?

Dazu möchte ich kurz ausholen. Es ist vielleicht inhaltlich jetzt nicht 100% notwendig, aber ich glaube, es dient vielleicht zum Verständnis. Ich habe auch meine Masterarbeit dazumal über den rechtssicheren Einsatz von Public Cloud-Systemen bei kritischen Infrastrukturen unter Berücksichtigung der NIS-Anforderungen geschrieben. Generell konnten keine Vorschriften identifiziert werden, welchen den Einsatz von Public Cloud Systemen bei kritischen Infrastrukturen per se verbieten. Dazu hat es damals in Deutschland auch recht gute Informationen und eine Umfrage gegeben, wo der Status quo der kritischen Infrastruktur und der Cloud-Services ist. Da war das Ergebnis: Es ist sehr zurückhaltend, eher konservativ. Es gibt jetzt weniger kritische Infrastrukturen, die mit den kritischsten Systemen direkt in die Cloud gehen. Den Eindruck habe ich auch auf Basis meiner Erfahrung so mitbekommen. Der Großteil der Erfahrungen, die ich gemacht habe, geht

in die Richtung, dass die kernkritischen Services und On-Premises betrieben werden und dass die auch hinsichtlich Internetkonnektivität etc. sehr stark eingeschränkt sind. Das heißt also, bei supportive Services sieht man es, glaube ich schon recht gut. Alles, was in Predictive Maintenance geht, wenn es ein wenig in den Bereich Analyse von großen Datenmengen und Logs geht etc.: Ja, aber meistens so, dass man sagt, wenn die Cloud irgendwie falsch funktioniert oder gebreacht wird oder ein Sicherheitsvorfall passiert, darf es keine Auswirkungen auf unsere kernkritische Infrastruktur haben. Also das sehe ich schon konservativ.

A.1.2 Gibt es hybride Ansätze? Man hat ein Backup On-Premises und betreibt es aber hauptsächlich in der Cloud und wenn es zu einem Ausfall kommt, dann springt man On-Premises zurück oder, dass mehrere Clouds einsetzt werden, z.B. Multi-Clouds, dass man Cloud Betreiber wechselt, wenn eine ausfällt?

Also ich denke, gerade wenn wir in die Richtung NIS schauen, wenn wir in Richtung ISO 27001 schauen, dann ist ja auch die Exit-Strategie gerade in der Version 2022 sehr prominent mitgenannt, mit dem neuen Kapitel zur Cloud Security. Da ist es schon so, dass ich es generell als Good-Practice empfinde, eben auch Exit-Strategien mitzudenken und eben auch auf Basis der verschiedenen Servicemodelle wie beispielsweise Infrastructure-as-a-Service die Exit-Strategie zu definieren. Das heißt, wenn ich jetzt meine Plattform neu baue und sagen wir sehr stark in der Cloud Transformation als solches, wenn ich meine Plattform auf Kubernetes beispielsweise baue, ist es meistens Erachtens einfacher auf AWS zu hosten, On-Premises zu hosten oder in Azure, wie wenn ich jetzt irgendein Software-Service Tool verwende, wie Salesforce, wie beispielsweise SAP oder Ähnliches.

Ich sehe es aber bei den kritischen Industrien bisher nicht, für die kritischen Themenbereiche. Also da hätte ich noch keinen Kunden kennengelernt, die von der Maturity auch so ausgeprägt sind, wirklich das kernkritische Geschäft so umzubauen, technologisch, dass es auch wirklich move-bar ist zwischen Cloud Service Provider. Das dauert natürlich ja, und das kann gerade bei kritischen Infrastrukturen Jahre dauern. Wo ich es schon sehe und wenn ich vielleicht noch einen Unterschied aufzeige: Wenn wir von kritischen Infrastrukturen sprechen, gibt es für mich diesen klassischen kritischen Bereich wie beispielsweise: Das Öl muss fließen, der Strom muss fließen oder das Wasser muss fließen und da gibt es natürlich den gesamten Office-Bereich, den IT-Bereich. Da sehe ich die Cloud natürlich schon. Ja, die meisten der Kundinnen und Kunden setzen natürlich zum Teil schon auf Cloud-Services, wenn auch sehr eingeschränkt bei der kritischen Infrastruktur selbst.

A.1.3 Und was ist deine Erfahrung bei den Servicemodellen? Was da genutzt wird? Also Software-as-a-Service oder so Platform-as-a-Service oder ganz durchmischt?

Im kernkritischen Bereich, wie gesagt, ist es sehr sehr eingeschränkt. Also da sieht man Cloud-Services fast nicht, insbesondere Public Cloud Services, eben große Hyperscaler

wie beispielsweise AWS, Google etc. Bei den Supportive Services sehe ich eher diesen Plattform-as-a-Service Bereich. Ja. In die Richtung IOT denkend, Predictive Maintenance, Logs, Auslastungsmodellierungen, Business Intelligence et cetera. Dann ist es meistens nicht ganz das Thema, dass man selbst hostet, weil die meisten großen Cloud Service Provider genau für solche Anwendungsszenarien natürlich schon recht gute Produkte gebaut haben. Ich denke nicht, dass ich Software-as-a-Service Angebote der großen Cloud Service Provider bereits in kernkritischen Bereichen gesehen habe. Vielleicht ein Thema noch dazu: Ich glaube, das hat doch ganz viel damit zu tun, dass der kernkritische Bereich, meistens auf einer Technologie, die auf keine Commodities und auf keiner Technologie basiert, wie beispielsweise SAP oder Power BI für irgendwelche Analytics oder Ähnliches, sondern das sind ja meistens tatsächlich ganz stark integrierte prozessintegrierte Systeme und Technologien und ich denke, dass in diesem Software-Servicemodell, diese sehr starke Anpassbarkeit auch oftmals gar nicht gegeben, ist. Es ist vielleicht auch ein Grund, warum ich das so bisher nicht gesehen habe.

A.1.4 Ein anderer Punkt: Wie ist deine Erfahrung mit Zugriff von US-Behörden auf Daten bei amerikanischen Firmen, die zwar in Europa lagern, aber es den bekannten amerikanischen Cloud-Act gibt, der den US-Behörden trotzdem Zugriff erlaubt, auch wenn das möglicherweise im Widerspruch zu europäischen Gesetzen steht und man möglicherweise nicht ausschließen kann, dass es da Zugriffe gibt, auch wenn die Daten in Europa lagern.

Ich möchte die Frage gar nicht abwimmeln, aber was ich ganz klar sagen möchte, ich denke, wir müssen hier zwischen einem technologischen und zwischen einem rechtlichen Problem unterscheiden. Es gibt ein massives rechtliches Problem. Und so konnten wir auch beispielsweise Max Schrems beobachten, der diese rechtliche Problematiken immer auf höchster Ebene (erfolgreich) aufgezeigt hat. Das ist immer so einen Hin und Her und ich glaube auch in den letzten 1-2 Monaten hat sich da ja wieder was getan, mit einer von Biden verabschiedeten Executive Order.

A.1.5 Es hatte noch ein Abkommen gegeben zwischen den USA und Europa. Aber das ist so, wie ich das verstanden habe, nur wieder ein neuer Versuch und NOYB hat da schon geschrieben, dass das möglicherweise „more of the same“ ist und wahrscheinlich wieder aufgehoben wird. Also im Kern ist erhalten geblieben, dass amerikanische Behörden gerne auf Daten zugreifen wollen, die in Europa lagern.

Die Executive Order von Joe Biden war ja dementsprechend auch ein Thema und am Ende des Tages wird es das Problem wohl auch immer geben. Da gibt es einfach gewisse andere Herangehensweisen. Wenn man jetzt eine Stufe nach oben geht: auch in dem Bereich Security versus Privacy. Was möchte ich haben: möchte ich Zugriff auf meine

Daten und wirklich den Behörden Sichtbarkeit geben, dass Sie mich beschützen? Ich glaube, dass wir Europäer da auch sicher anders denken wie die Gesellschaft in den USA. Schwieriges Thema. Wir sprechen von einer Microsoft und wir haben jetzt identifiziert, dass die Microsoft beziehungsweise die US-Behörden teilweise auf unsere Daten zugreifen können. Welche Abhängigkeit habe ich denn per se zu Microsoft? Weil auf der anderen Seite Windows Betriebssysteme zu verwenden und vielleicht über Updates Server, die im Internet stehen, automatisch Updates zu installieren etc. pp., das alles durchzuführen und zu sagen, das ist überhaupt kein Problem und vollkommen in Ordnung. Eine Datei in der Cloud zu speichern, ist aber auf keinen Fall ein Thema. Es geht sich für mich aus technologischer Perspektive manchmal nicht ganz aus. Wenn natürlich auch für gewisse Datenkategorien so etwas wie Hold Your Own Key oder Ähnliches auch eine gut charmante Möglichkeit ist, um Daten nur verschlüsselt dem Cloud-Service Provider zu geben. Habe ich aber tatsächlich weniger in den Gesprächen identifiziert, dass kritische Infrastrukturen sagen: Wir gehen nicht in die Cloud, weil wir Angst vor dem Zugriff von US-Behörden haben. Ich glaube, die Angst, zurecht oder nicht, sei jetzt mal dahingestellt. Die Angst kommt eher daraus, dass man einen gewissen Einflussbereich verliert, dass man auch, gerade wenn es in Richtung Geopolitik, wenn es in Richtung Abhängigkeitsverhältnisse etc. geht, man noch etwas geschützter ist, wenn man es in seinen eigenen vier Bereichen hat, in seinen eigenen vier Wänden hat.

A.1.6 Und sind aus deiner Sicht eigentlich die Möglichkeiten für den Cloud-Betrieb eingeschränkt worden für kritische Infrastruktur durch neue Regulative wie NIS und NIS2 und dem Cyber-Resiliance-Act, von DORA und so weiter? Hat man dieselben Möglichkeiten wie vorher als kritische Infrastruktur?

Also meines Erachtens, und hier bitte auch noch mal Disclaimer, ich bin überhaupt kein Jurist und möchte das auch gar nicht aus juristischer Brille bewerten, aber was ich nicht sehe, ist, dass in irgendwelchen diesen Themenbereichen steht, Public Cloud-Service Provider wie beispielsweise XYZ dürfen nicht verwendet werden, das steht nicht drinnen. Wenn man jetzt beispielsweise NIS hernimmt: Ursprungsversion 1. Auch da steht nicht drinnen, dass ich keinen Cloud-Service Provider verwenden darf. Selbstverständlich gibt es gewisse Zuständigkeiten oder gewisse - ja ich nenne es mal Informationssicherheitsmaßnahmen, welche ich adressieren muss, die Verantwortung zur Adressierung liegt auch immer bei der kritischen Infrastruktur, wenn ich hier von Verantwortung spreche, meine ich damit, die kritische Infrastruktur muss sicherstellen, dass alle Anforderungen aus der Regulatorik auch tatsächlich umgesetzt sind. Jetzt ist natürlich die Frage, wie das sichergestellt werden kann: Da kommt natürlich stark das Shared-Responsibility oder Shared-Security Responsibility Model hinein. Da kommt sehr stark hinein, dass die kritischen Infrastrukturen ganz genau verstehen müssen, wo liegt denn die Zuständigkeit und tatsächliche Adressierung der Informationssicherheitsmaßnahmen und welchen Weg kann ich gehen, um mir selbst zu gewährleisten, dass mein Cloud-Service Provider das auch wirklich auf dem Niveau macht, wie ich es gern hätte oder die Regulatorik vorschreibt.

Und das funktioniert am Ende des Tages eben über Zertifizierungen des Cloud-Service Providers, gerade wenn man in Richtung AWS, Google oder Azure geht, die spielen alle Stücke, die sind zertifiziert von bis. Da ist natürlich ein BSI C5 dabei, der auch im Zuge einer NIS Prüfung als Nachweis vorgebracht werden kann, so wie es das BSI und dazumal identifiziert hat. Wir haben ISO 27001 für das Managementsystem, wir haben die Cloud Security Alliance mit der Cloud Control Matrix und dem CSA Star Level 2 Zertifikat, SOC 2. Die haben eigentlich alles. Also für die kritischen Infrastrukturbereiche sehe ich eigentlich keine Show-Blocker. Wenn es in das Thema DORA geht oder Banken und diese Themenbereiche, da ist es auch oftmals so, dass explizit eine Exit-Strategie gefordert wird, und ich denke, das resultiert aus einer EBA-Guideline. Aber wie zuvor erwähnt, ich bin kein Jurist, das müssten wir noch kurz genauer spezifizieren. Banken benötigen auch ein gewisses Auditrecht gegenüber den Dienstleisterinnen und Dienstleistern. Das wiederum stellen die großen Cloud-Service-Provider nicht zur Verfügung. Die Microsoft geht hier den Weg mit dem Financial Services Amendment in Österreich, das ist ein Zusatzvertrag, den man abschließen kann, wenn man sich unter diesen Guidelines regulativ befindet. Also auch dafür gibt es Herangehensweisen und potenzielle Lösungen. Wird es schwieriger in Richtung Cloud-Services zu gehen durch die gesamte Regulatorik? Ja, selbstverständlich. Aber wird es schwieriger, Services On-Prem zu betreiben aufgrund der Regulatorik? Ja auch, also nur wegen der Aussage, es wird schwieriger in die Cloud zu gehen, heißt das nicht, dass per se die Regulatorik gegen Cloud Services geht, sondern dass die Regulatorik einfach ordentliche Informationssicherheit vorsieht. Egal, ob Cloud oder On-Prem. Das geht vielleicht sogar in die Richtung, dass man sagt, anhand von Cloud Services kann man gewisse Anforderungen schneller adressieren, weil eben die Zuständigkeit wegfällt.

A.1.7 Die Auditpflicht ist aus deiner Sicht bei den meisten Public Cloud Provider schwieriger zu erfüllen?

Also ich muss ehrlich gestehen, ich habe noch nie einen Kunden dahin gehend begleitet, dass er beispielsweise eine Microsoft auditiert. Hörensagen ist, dass es mit gewissen Kosten verbunden ist. Es gibt, glaube ich, auch in Dublin oder irgendwo in die Richtung, ein Rechenzentrum von Microsoft, wo tatsächlich auch Führungen abgehalten werden. Inwiefern das für den Auditprozess relevant ist, kann ich nicht beurteilen. Ein Thema, das vielleicht generell noch spannend wäre und wo ich vielleicht auch deinen Input gern dazu hören möchte: Weil ich da selbst nicht am aktuellsten Stand bin. Wir haben ja mit den EBA-Guidelines dieses Einräumen des Auditrechts bei Auslagerungsverträgen. Es hat doch mal den Gedanken gegeben, dass eine zentrale Stelle, die wesentlichsten Zulieferinnen und Zulieferer von den kritischen Infrastrukturen im Bereich der Banken auditieren können. Ist das noch relevant?

A.1.8 Könnte man eigentlich auf Gesetzgeberseite aus deiner Sicht noch mehr Sinnvolles machen, um die Sicherheit zu steigern? Oder gängelt man die kritische Infrastruktur jetzt schon genug mit Regulativen?

Ehrlicherweise, ich denke, dass gerade das mein Gefühl ist, dass viele kritische Infrastrukturen gerade sehr viel tun in dem Bereich. Wenn wir skizzieren: Es muss ein risikoorientiertes Vorgehen geben oder Ähnliches. Das ist eine Spirale, die sich immer weiterdrehen wird. Ich müsste mich jetzt tatsächlich eine halbe Stunde hinsetzen und mir genau Gedanken machen. Wo könnte denn ein Gesetzgeber weitere Lücken schließen? Oder auch die Unternehmen unterstützen. Sei es mit irgendwelcher Threat Intelligence, die zur Verfügung gestellt wird, oder Threat Intelligence innerhalb von gewissen Branchen, der kritische Infrastrukturen, die geteilt wird usw.

A.1.9 Und zum Gesamtbild: Hast du den Eindruck, dass diese Regulative etwas bringen oder ist das jetzt plakativ gesagt, nur mehr Papier erzeugen und am Ende des Tages wird eigentlich gar nicht viel besser?

Also ich denke 100%, dass es etwas bringt und ich beobachte das bei Kundinnen und Kunden. Wir unterstützen viele Kundinnen und Kunden bei der Adressierung von genau diesen Sicherheitsmaßnahmen etc. Also ja, ich denke, dass hier mit diesen regulatorischen Vorgaben die letzten Jahre schon einiges in die richtige Richtung geht. Dass es viel Papier ist: Naja, das bleibt nicht aus, es ist halt so. Aber auch technologisch und der tatsächliche Mehrwert im Bereich der Informationssicherheit ist sicher erkennbar.

A.1.10 Würdest du es gut finden, wenn die noch strengeren Regulative für Drittparteien aus DORA auch Richtung NIS wandern, also jetzt nicht nur auf Finanzunternehmen angewandt werden sollen, sondern auch auf kritische Infrastruktur?

Kannst du vielleicht ganz kurz zusammenfassen, was in diesen Drittparteien Anforderungen mit inkludiert ist?

A.1.11 Im Wesentlichen, dass Finanzunternehmen sie [die Drittparteien] kontrollieren oder auditieren dürfen und dass die Behörde die Rechtsvorschriften wirksam durchsetzen kann. Ich denke, das ist der Knackpunkt.

Ich sehe das so: Es ist wieder ein rechtliches Thema bzw. ein rechtliches Problem. Es wäre zielführend, teilweise natürlich, wenn man sich darauf konzentriert, dass man die tatsächliche Informationssicherheit bei diesen Unternehmen verbessert. Wenn das der beste Weg ist, dann soll es so sein. Ich kann mir aber auch vorstellen, dass es teilweise zu viel ist, also, wenn ich jetzt beispielsweise als kritische Infrastruktur für jede Drittpartei ab

einer gewissen Größe Auditierungsrechte benötige. Also mir wäre es lieber, wenn man sagt, kritische Infrastruktur muss das im Bereich des Vendormanagements berücksichtigen, welche Dienstleisterinnen und Dienstleister in welcher Größenordnung mit welchem Impact auf das Unternehmen eingesetzt werden. Und die Finanzunternehmen sollen das dementsprechend im Griff haben. Das geht ja auch in die Richtung, dass man sagt, Achtung: Du bist mein Dienstleister, für eine gewisse Zeit etc. pp. gibt es Klauseln in Verträgen: Das Unternehmen muss vielleicht, ISO 27001 oder SOC 2, usw. zertifiziert sein, weil ansonsten auch auf vertraglicher Seite gewisse Klauseln wirksam werden. Also das ist alles, was man sich gut vorstellen kann. Ich denke das Auditieren sollten vielleicht eher zentralere Organisationen machen und weniger jede kritische Infrastruktur für sich selbst. Wenn ich mir vorstelle, ich bin Zulieferer von sechs kritischen Infrastrukturen, dann werde ich sechsmal im Jahr auditiert – wenn es passt oder wenn ich Pech habe, ist auch nicht angenehm.

A.1.12 Was hältst du so von den Bestrebungen, dass man eine europäische Public Cloud etabliert? Es gibt zwar schon viele Anbieter, aber dass man versucht sie öffentlich zu fördern und sie eine ernst zu nehmende Konkurrenz zu großen Hyperscaler in Europa werden.

Wann gibt es diese Idee schon?

[Vermutlich Jahrzehnte.]

Wo ist die Cloud oder wie heißt sie?

A.1.13 Aber denkst du, wäre das eine gute Idee, auch wenn es man bis jetzt nicht geschafft hat, das umzusetzen?

Generell empfinde ich es als gute Idee, dass man versucht, etwas Unabhängiges, eben im mitteleuropäischen/europäischen Raum aufsetzen. Ja, das macht Sinn. Ich bin mir tatsächlich nur nicht sicher, ob wir eine Chance haben, gegen die großen Hyperscaler oder ob es nicht vielleicht geschickter wäre, dass man sich eher in die Richtung bewegt, dass man sagt: Liebe bestehenden Hyperscaler, lasst uns vielleicht überlegen, wie wir eure Lösungen auch als europäische Lösungen implementieren können. Aber woran ich weniger glaube ist, dass wir innerhalb von 1-2 Jahren in Europa ein Basis-Microsoft Azure Pendant aufgesetzt haben, mit der gesamten Integrationsfähigkeit usw., wie es Microsoft mit Azure zur Verfügung stellt.

Das ist so etwas wie Amazon: Manchmal verstehen wir auch das Business-Modell dahinter nicht. Das ist sicher nicht nur Webseiten durchsuchen, sondern das gesamte Netzwerk zur Auslieferung, der Kundensupport etc. Und das ist bei den Cloud-Service-Providern ähnlich, die funktionieren schon richtig gut. Vielleicht noch ein Thema, das ich auch sehr spannend finde: Teilweise beobachtet man, dass Auslagerungen durchgeführt werden, so etwas wie Housing oder virtuelle Maschinen werden von einem Partner gemanagt. Das

ist teilweise schon auch vorzufinden in den kritischen Infrastrukturen. Wenn man in dem Bereich Cloud Services denkt, ist es aber wieder so ein Red-Flag. Ich denke, dass es eine gewisse Zeit braucht, um auch dieses Vertrauen in Cloud-Services zu stärken. Auch zu Recht, es hat einige Vorfälle gegeben, teilweise schwierigere oder stärkere Vorfälle, teilweise Vorfälle, so wie man sie überall hat. Es hat, glaube ich, viel mit Vertrauen zu tun. Und das nächste ist, wenn ich beispielsweise meine VMs in meiner kritischen Infrastruktur von dem Unternehmen A verwalten lasse, oder das Housing und das Management und auch das ist eben vorzufinden. Dann habe ich erstens nicht solche robusten Rechenzentren wie beispielsweise eine Microsoft Azure Region, im Normalfall ja auch Zertifizierung etc. liegen oft nicht vor. Und zweitens, wenn dann diese Umgebung, die administrativ auf meine kritische Infrastruktur zugreifen kann, vollständig von der Microsoft verwaltet wird, dann habe ich vielleicht weniger das Problem, dass die Microsoft so auf meine Daten zugreift oder eben auch US-Behörden oder Ähnliches. Einen gewissen Weg gibt es dann natürlich schon. Das heißt, wir müssten sich gar nicht die Frage stellen - ich als kritische Infrastruktur - welche Abhängigkeit habe ich denn zu Microsoft? Um etwas zu skizzieren: sollte die Microsoft gehackt werden und eine Supply Chain Bedrohung von Microsoft ausgehen, welchen Impact hätte das denn für meine kritische Infrastruktur? Das ist weniger der Bereich: Wir haben Daten in der Cloud, sondern was passiert mit Updates? Wie werden Schwachstellen geschlossen, wie funktioniert mein Provider, der meine VMs verwaltet, wie funktioniert die gesamte Supply Chain von mir und welche Abhängigkeit haben die zu Microsoft, wenn das auch beispielsweise gar keine kritische Infrastruktur ist? Noch auf einem Stück weiter oben, vielleicht auf einem Land, Mitteleuropa oder Europa zu identifizieren: Gegenüber welchen Technologieherstellern hat man denn welche Abhängigkeit? Das ist, glaube ich, ein Thema, das unheimlich spannend wäre. So eine Arbeit würde ich unheimlich gerne lesen.

A.1.14 Ich finde es interessant, dass DORA in diese Richtung geht, mit IKT-Drittdienstleister, dass sie gar nicht unterscheiden: Was macht der Dienstleister genau, sondern einfach nur ist der wichtig für mich und wenn ja, dann ist er streng zu regulieren.

Die DORA schaut sich insbesondere die Prozesse an. Ist der Prozess wesentlich, dann ist auch die Auslagerung wesentlich, ergo ziehen andere Maßnahmen. Es ist generell spannend, dass viele Leute einen Unterschied machen zwischen normale Auslagerung und zwischen Cloud-Service Providern, weil am Ende des Tages ist eine extrem hochqualitative automatisierte Auslagerung, welche ich über Schnittstellen steuern kann, eigentlich ein Cloud-Service Provider und ich denke, weil das oftmals ein bisschen missverstanden wird, hat es eben auch einen prominenteren Platz in der ISO 27001 in der Version 2022 bekommen, weil eine Due-Diligence, bevor ich etwas auslagere, das habe ich immer schon benötigt. Ob jetzt Cloud-Service Provider oder normale Auslagerung - um die Informationssicherheit bei der Partei, an die ich ausgelagert habe, das habe ich auch schon immer machen müssen. Jetzt muss ich es auch bei Cloud-Services machen. Das ist für mich eigentlich kein Unterschied. Den einzigen Unterschied, den ich sehe, ist im Risiko

oder in den Maßnahmen, welche man selbst adressieren muss, also Kostenmanagement zum Beispiel: Crypto Miner in der eigenen Infrastruktur, dann wird es einmal heiß und das war es. Crypto Miner in Cloud Services kann mit unheimlich vielen Kosten zu tun haben. Es gibt ein paar Bedrohungsszenarien, die bei Cloud Services einfach anders sind, auf die muss man Rücksicht nehmen, aber ansonsten mache ich da keinen Unterschied. Etwas, das auch neu ist, ist das Shared Security Responsibility Model, also diese geteilte Zuständigkeit zur Adressierung von Informationssicherheitsmaßnahmen. Also man muss wirklich die Frage stellen, wer ist für was verantwortlich. Um das mit einer Story zu hinterlegen: Netflix beispielsweise hat bei dem AWS Ausfall, was dazumal ich glaube, in US-EAST war, ich müsste nachschauen, hat nahezu keinen Impact gehabt, und andere Unternehmen sind da stundenlang gestanden. Die Frage ist, ist jetzt der Cloud-Service Provider schuld oder nicht. Der war innerhalb seines SLA und die anderen haben die Cloud-Services nicht Cloud nativ aufgebaut. Da funktionieren ein paar Sachen anders.

A.1.15 Was mir zum Gedanken einfällt, das macht nicht so viel Unterschied, ob jetzt ein Externer meine Infrastruktur betreut oder ob ich die Infrastruktur bei anderen miete, im Sinne von Public Cloud. Macht es vielleicht dahin gehend ein Unterschied, dass wenn jetzt wirklich mein Netzwerk komplett weg ist und ich trotzdem betriebsbereit sein und den Betrieb aufrechterhalten muss, auch ohne Netzwerk, dann kann ich das vielleicht um On-Premises noch, wenn die Systeme laufen, wenn sie kein Netzwerk brauchen, um grundsätzlich zu funktionieren.

Also das auf jeden Fall und ich glaube, das ist auch eben genau das, wo viele Leute sagen, es muss irgendwo On-Prem laufen. Also es muss auch offline lauffähig sein, so im Sinne von, wenn ich mich zu Hause einsperre, möchte ich zwei Wochen überleben können. Das macht auch Sinn. Und was schon ist: bei Cloud Services ohne Internet und ohne anständiges Internet wird es schwierig. Dann ist das auf jeden Fall ein ernst zu nehmendes Bedrohungsszenario. Noch eine Anmerkung: Ob ich jetzt beispielsweise einen Cloud-Service Provider bei mir habe oder per Internet auf meine virtuelle Maschine, die beispielsweise bei Hetzner in Deutschland gehostet ist, zugreife, macht für mich keinen Unterschied, wenn auch das erste ganz klassisch Cloud-Service ist und oftmals als Böse identifiziert wurde, ist zweiteres gut, weil das ist physische Hardware. Cloud Services sind per se nicht böse, das möchte ich damit sagen, wenn auch natürlich sicher nicht für jeden Use Case einsetzbar.

A.2 Anonyme Expertin A

Interviewpartnerin	Anonym (in dieser Arbeit *Expertin-A* genannt)
Hintergrund	IT-Consultant im Netzwerk und Security Bereich
Datum	8. März 2024
Uhrzeit	11:00-11:30
Ort	Online-Meeting via MS Teams

A.2.1 In welchen Unternehmensbereichen werden deiner Erfahrung nach bei der österreichischen kritischen Infrastruktur Cloud Dienste eingesetzt? Wird es auch für wesentliche Funktionen verwendet oder nur für Support, IT und weniger im OT Bereich?

Ganz unterschiedlich, also wo Kunden extrem motiviert sind, in die Cloud zu gehen, ist zum Beispiel Mobile Device Management. Nicht weil es nicht um heikle Daten geht, sondern weil es ohne Cloud Dienste ohnehin nicht funktioniert. Wenn halb Google steht, brauche ich mir keine Sorgen darüber machen, ob ich meine Android-Smartphones noch verwalten kann. Ich kenne sehr wohl einige Umgebungen, wo solche Dinge wie HR Daten und dergleichen auch mitunter mitgehen. Wirklich im operativen Bereich, was das tiefste Kerngeschäft betrifft, fällt mir jetzt ad-hoc überhaupt kein Beispiel ein. Also wo es um mehr als um Supportdaten geht. Nein, da fällt mir jetzt gar niemand ein. Wobei ich ein großes Unternehmen kenne, das jetzt eine absolute Cloud First Strategie für all ihre Dinge macht. Transition ist aber bislang nicht fertig. Cloud für einfach alles. Sie betreiben kein Data Center mehr. Also ich sage mal, die ziehen das durch, auch wenn sie es bisher nicht gemacht haben.

A.2.2 Und bei einem großen Public Cloud-Anbieter?

Bei einem großen Public Cloud-Anbieter. Ich gehe fix davon aus, dass sie das durchziehen. Wüsste nichts, was Sie davon abhalten soll. Also, ich wüsste technisch einiges, was sie davon abhalten soll, aber ich glaube, sie machen es dennoch. Das ist aber jetzt die große Ausnahme. Ansonsten sehr konservativ, einzelne Services draußen ja meistens irgendwas im Supportkontext.

A.2.3 Und werden Hybridlösungen eingesetzt, dass ein Unternehmen sagt, man hat ein Backup vielleicht On-Premises oder ein System On-Premises laufen und eines in der Cloud und man teilt auf?

Es ist gefühlt entweder das eine oder das andere. Ich kenne schon Unternehmen, die so darüber nachgedacht haben, eine Backup-Umgebung in der Cloud zu haben bis hinzu zu

Proof of Concept Geschichten. Jemand, der das wirklich hat und testet? Nein.

A.2.4 Gibt es deiner Erfahrung nach, welche, die vielleicht sogar mehr in Richtung Community Clouds gehen? Also sie schließen sich mit anderen Unternehmen zusammen und bauen eine gemeinschaftliche Cloud?

Ganz, ganz wenig. Also mir würde da jetzt, auch wenn ich es selbst kaum kenne, das Unternehmen [Name entfernt] einfallen, die bisschen in diese Richtung gehen. Wobei ich kaum Services gesehen oder erlebt habe, die darin gehostet sind. Da wäre, glaube ich, die Idee dafür da.

A.2.5 Und wie schaut es mit den Cloud Service-Modellen aus, die genutzt werden?

Also teils teils. Software-as-a-Service definitiv ja. Da sind wir beim Mobile Device Management Beispiel wieder. Das ist eine fertige Software, die zur Verfügung gestellt wird, meistens mit sehr wenig Handlungsspielraum. Infrastructure[-as-a-Service] meistens nur im Testbereich. Also es gibt durchaus Unternehmen, die haben 2-3 Maschinen in einer Cloud stehen und wenn es nur ist, um externe Tests auch durchführen zu können oder Monitoring über extern haben zu können.

Was natürlich schon viel genutzt wird, ist Azure Entra ID als Identity Provider. Citrix pusht finanziell meines Erachtens die Migration des Verwaltungsteils in die Citrix Cloud. Die Citrix Cloud, wo du wirklich die Backpane draußen hast, das heißt, du machst deine Maschinenkataloge und dergleichen alles draußen, auch wenn deine Ressourcen in Wahrheit immer noch inhouse sind. Die meisten stellen die Ressourcen selbst bereit, die kaufen sich die Maschinen nicht in Azure, AWS oder sonstigen unterstützten Plattformen, sondern sie lassen sie On-Prem, weil dort auch all ihre anderen Ressourcen sind. Sie sind nur mit Geld dazu gelockt worden, keine Delivery-Controller und keine Datenbank On-Prem zu betreiben. Obwohl ich nicht weiß, ob das nicht meistens eine finanzielle Entscheidung ist.

A.2.6 Wird der Vendor Lock-in als Risiko beim Cloud-Betrieb wahrgenommen?

Also ich glaube schon, dass es ein Risiko ist. Ich glaube aber, dass der Lock-in durch Mailsystem und Exchange mit Azure bereits passiert ist. Und ich glaube, die Angst ist da. Die meisten IT-Admins empfinden, das als Hilflosigkeit in Wahrheit. Weil ich sage, jetzt einmal frech meine virtuellen Maschinen - also bleiben wir bei dem Beispiel Citrix: Ich habe mich für einen Vendor entschieden. Ich habe meine Maschinenkataloge und meine Infrastruktur danach aufgebaut. Der Vendor Lock-in ist völlig egal, also der Aufwand von Citrix wegzukommen und auf ein vergleichbares oder auf ein anderes Produkt zu wechseln, ist der gleiche On-Prem wie in der Cloud. Wenn ich jetzt sage, mir reicht es

mit der Citrix, ich gehe zum zweiten namhaften Hersteller, der sich gerade kaufen lässt. Im Endeffekt, ich brauche neue Desktop Delivery-Controller und ich werde an meine Master Image etwas herumschrauben müssen, das hat aber nichts mit der Cloud zu tun. Der Aufwand ist der Gleiche. Ja, ich habe eine SQL Datenbank weniger On-Prem wegzuwerfen. Das sind aber solche Kleinigkeiten. Ich sehe den größten Vendor Lock-in im Hinblick auf Identity-Verwaltung und Exchange, also Mail Service. Welches Unternehmen hat seine User nicht in irgendeiner Weise in Microsoft? Wer bindet mich dann als eine Applikation an, dass sie sich gegen Azure AD anmelden kann?

A.2.7 Gibt es deiner Meinung nach bei den Unternehmen Katastrophenszenarien, wie sie sich auf irgendwelchen Blackouts oder Zusammenbruch der Telekommunikationsleitungen vorbereiten? Also was ist, wenn Sie die Cloud einfach nicht mehr erreichen?

Ja, also es gibt in den meisten Unternehmern Szenarien, was ist, wenn ich keine Internetverbindung mehr habe. Was passiert, wenn Standorte getrennt sind. Das kenne ich in sehr schön und in ausgeprägter Form, manche testen das noch ein zweimal im Jahr und natürlich glaube ich, dass es auch manchmal nur ein Papier gibt und es nicht zu Ende gebracht wird. Es ist etwas, was unglaublich Low-Prior ist. Ich kenne zum Beispiel ein Unternehmen, das hat in ihrem Ausfallszenario: Was ist, wenn das Internet weg ist? Die haben das jetzt glaube ich vier Jahre und einmal im Jahr testen sie es und haben aber seit vier Jahren ein und dasselbe Problem damit. Das Problem war blöd zu finden, da will ich jetzt überhaupt nichts dagegen sagen, aber dass sie deshalb öfter testen? Nein. Weil es nicht dringend ist. Darüber nachdenken und darüber reden müssen doch alle tun. Es ist in der Priorität aber sehr weit unten.

A.2.8 Wie sehen deiner Meinung nach Unternehmen das Risiko, dass bei US-amerikanischen Anbietern, Datenzugriff durch US-Behörden erfolgen kann, auch wenn die Daten in Europa liegen. Der Cloud-Act ermächtigt unter Umständen US-Behörden auf Daten in Europa zuzugreifen, auch wenn betroffene Unternehmen damit möglicherweise europäische Gesetze verletzen.

Mir kommt das überhaupt vor wie ein Freispruch: Die Daten sind in Europa und deshalb brauche ich mir keine Sorgen zu machen, weil du es nicht kontrollieren kannst. Du kannst in Wahrheit nicht einmal bei allen Anbietern kontrollieren, wo die Daten wirklich liegen. Bei einem Daten-Abfluss hat man keine Chance. Wie soll man das überprüfen? Es fängt schon damit an, wenn du dir diverse Cloud-Anbieter anschaust: Die sagen, wir haben in Europa Rechenzentren, dann willst du dieses oder jenes Service haben und kannst dich frei entscheiden zwischen US-East und US-West Coast, weil es auf der anderen Seite nicht verfügbar ist. Sind einzelne kleine Services, blöd, wenn ich genau das brauche.

A.2.9 Wird man in die Richtung gedrängt, Daten nach Amerika zu übertragen?

Teilweise sind es einzelne Services, die dich dazu zwingen. Das ist die Frage, was genau an Daten wo liegt. Aber die zweite Frage ist auch, was für Daten fließen über diesen Service. Ich persönlich fühle meine Daten in der europäischen Cloud, der von einem US-Anbieter betrieben wird, nicht wahnsinnig besser oder sicherer geschützt, als wenn sie in den USA sind. Es ist ein gefühlter Freibrief: Ich habe mich an die Vorgaben gehalten und ich bin in Europa mit meinen Daten.

A.2.10 Wird es deiner Meinung nach auch interpretiert von den Unternehmen, dass sie sagen: Die Daten liegen in Europa. Alles gut?

Ich glaube, dass da die Diskrepanz zwischen, wie es der IT-Admin empfindet und dem, was übergeordnete Einheiten empfinden, sehr groß ist. Also ich glaube durchaus, dass der einzelne Admin, der für diese Lösung verantwortlich ist, sich dessen bewusst ist, es auch mitunter artikuliert, man es aber nicht hören will. Die Vorgabe ist erfüllt. Lasst mich in Ruhe.

A.2.11 Sind deiner Meinung nach mit den Gesetzen oder Verordnungen und Richtlinien, die es in den letzten Jahren gegeben hat, von der EU - Stichwort NIS, Cyber Resilience Act und DORA für die Finanzdienstleister - die Möglichkeiten für einen Cloud-Betrieb bei der kritischen Infrastruktur eingeschränkt worden?

Also für mich fehlt gefühlt bei den meisten von den EU-Verordnungen[/Richtlinien] zu dem Thema: Ich kann die als Techniker, wenn ich sie für mich lese sehr unterschiedlich auslegen. Es gibt sehr wenig Judikatur dazu. Das heißt, das macht es für mich schwer, es deterministisch einzuschätzen. Ist das ok, was ich hier tue oder nicht? Mir kommt vor, es wird einerseits nicht ungern dazu verwendet, für: Passt, wir betreiben alles On-Premises, weil wir dürfen nicht. Oder man verwendet es als Ausrede: Die Daten liegen in Europa, ich darf ohnehin. Es gibt ja wirklich Services, wofür dann auch der Ausfallplan fehlt. Es gibt schon Unternehmen, wo ich jetzt behaupten würde, gefühlt, das ist kritische Infrastruktur, auch im engeren Sinne, die haben Anforderungen im Notfall Szenario, also wenn wir von Ausfall reden und wir haben gewisse Zugriffe nicht, dann muss z.B. der Mailserver funktionieren, weil sie dann alle im gleichen Haus sitzen, damit sie sich Mails schreiben können. Mir geht es ein bisschen darum, auszudefinieren, was ist kritisch? Ich bekomme bei vielen mit: Mails und Kommunikation sind kritisch, ich denke mir, aber das ist jetzt ein Service, das kann ich ohnehin nicht redundant für mich allein betreiben.

Vor allem kenne ich eigentlich nur beide Extreme. Ich kenne Unternehmen, die sagen, keine Cloud für eigentlich 90% unserer Services, weil wir kritisch sind, wir brauchen

das alles On-Prem, wir können die Daten nicht hinauslegen, egal wohin. Die sich damit selbst auch teilweise im Weg stehen, weil vieles nicht möglich ist, weil sie möglicherweise lizenzrechtliche Probleme bekommen. Microsoft Office ist dann auch immer ein Schlagwort, dann ist auf einmal Word und Excel kritisch, weil sonst bekomme ich meine Notfalldokumentationen nicht auf. Ich glaube, dass der kritischere Bereich enger definiert werden muss, vom Rest des Unternehmens. Es kann nicht ein ganzes Unternehmen systemkritisch sein, in allem, was es tut. Damit stehe ich mir selbst im Weg.

A.2.12 Aber es ist möglicherweise nicht leicht aufzudröseln.

Ja, sie dröseln es nicht auf. Sie sagen einfach alles. Nur wird es gefühlt zunehmend immer schwieriger Services ohne Cloud Berührung zu verwenden, wo bekomme ich meinen Multifaktor her? Kein Multifaktor geht es auch wiederum gar nicht. Wo bekomme ich meinen zweiten Faktor her, wenn ich überhaupt keinen Bezug nach draußen haben darf? Also irgendwo in den ersten Hops brauche ich einen. Ich brauche ihn dann vielleicht nicht mehr für alles, was ich weiter mache, aber der einzige Multifaktor, den ich zu 100% an On-Premises betreiben kann, sind Zertifikate. Oder blanker time based OTP zum Eintippen, den könnte ich On-Prem berechnen, abschreiben und so lange das Device, auf dem ich sie installiert habe, die Zeit noch richtig hält und das wird es schon eine Zeit lang, werde ich den nehmen können. Aber ganz ehrlich? Fast keiner der Multifaktor Implementierungen ist darauf ausgerichtet. Die meisten haben zumindest eine Push-Notifikation und erlauben den Passcode ohne Push mitunter nicht.

A.2.13 Könnte der Gesetzgeber, also die EU oder auch nationale Gesetzgeber, mehr zum Schutz der Informationssicherheit machen oder sind die bestehenden Regulative ausreichend? Wäre da noch Verbesserungsbedarf?

Ich glaube, dass der Ansatz falsch ist. Das, was jetzt passiert ist, teilweise wirklich Papierproduziererei, wo ich mir denke ich, ich weiß nicht, wie es uns weiterbringen soll. Es gibt haufenweise Texte, wo ich fast davon ausgehe, dass die jemand geschrieben hat, der das selbst noch nie in der Hand hatte. Was falsch ist bei solchen Gesetzesentwürfen beziehungsweise bei solchen Gesetzen. Manches ist dann so realitätsfremd geschrieben, dass ich sage, OK, dann können wir gleich sagen, wir verbieten es. Dann wäre es wenigstens eindeutig. Dann hätte ich keinen Graubereich dort. Weil, wenn ich nur versuche, didaktisch etwas auszuschließen und den Ersten finde, der dann sagt, in seiner Auslegung, ok ich probiere es andersherum, weil ich es so argumentieren kann. Dann ist das keine Absicherung von irgendetwas, sondern dann ist es die Absicherung von dem, der am längsten einen Gerichtsstreit durchhält.

A.2.14 Was hältst du von Bestrebungen eine europäische Cloud Lösung zu etablieren, um sich unabhängiger zu machen, von großen amerikanischen Anbietern?

Fände ich von der Grundidee her gut. Ich bin mir nur, ob der Umsetzbarkeit nicht sicher. Einerseits, da gibt es jetzt schon so viele, so große, die einen echten Startvorsprung haben. Die profitieren davon, dass sie billigere Arbeitskräfte außerhalb von Europa haben, um das überhaupt zu erzeugen. Ich bin mir jetzt nicht ganz sicher, ob Europa das auf den Boden bekommen kann.

A.2.15 Also auch mit staatlicher/europäischer Subventionen?

Wir finden schon in den einzelnen Bereichen keine Fachkräfte für die Unternehmer in der IT. Jetzt soll ich da wen finden, der das aufbaut? Und der Mitarbeiter kostet hier mehr, als in den USA und erst recht mehr, als er Richtung Asien kostet. Und wenn ich mir jetzt anschaue, was für Preise für virtuelle Maschinen, blödes Beispiel, ich bei Amazon bezahle, ich kann mir nicht vorstellen, dass wir das Hinkriegen. Ja, ich empfände es als cool, es wäre alleine angenehm, gegen die größeren namhaften Anbieter irgendwie eine Konkurrenz zu haben und das konkurrenzfähig zu halten. Ich glaube, dass Microsoft möglicherweise ein unglaubliches Monopol hat, das uns unglaublich wehtun könnte. Ich bin mir nur nicht sicher, wie realisierbar es ist. Oder ich habe ein Misstrauen darin.

A.3 Anonymer Experte B

Interviewpartner	Anonym (in dieser Arbeit *Experte-B* genannt)
Hintergrund	Security Experte aus dem Finanzbereich in Österreich
Datum	19. März 2024
Uhrzeit	17:30-18:00
Ort	Online-Meeting via MS Teams

A.3.1 Soll man auf Gesetzgeberseite mehr machen, um die IT-Sicherheit bei kritischer Infrastruktur besser zu gestalten, oder macht man bereits genug?

Ich glaube, dass man mittlerweile genug tut. Seit NIS 1 hat es einen guten Beginn genommen. Im Banken oder Finanzdienstleister Umfeld war die Regulierung ohnehin immer schon eine Spur stärker oder früher dran. Ich glaube, von Gesetzgeberseite wird derzeit ausreichend viel gemacht.

A.3.2 Du hast also nicht das Gefühl, dass noch ein NIS 3 in Kürze notwendig ist?

Nein, glaube ich nicht. Ich spreche jetzt hauptsächlich für DORA, aber ich glaube auch mit NIS 2 werden die IT-Provider viel mehr an die kurze Leine genommen.

A.3.3 Macht es deiner Erfahrung nach Sinn, dass man Vorschriften aus DORA, z.B. das Drittparteienrisiko – dass man sich Dienstleister genau anschauen und Ausstiegsszenarien vorhalten und sicherstellen muss, dass man kein Vendor Lock-in erfährt – würde es Sinn ergeben, dieses Regulativ auch auf andere kritische Infrastruktur auszuweiten?

Vermutlich ja. Ich glaube schon, die Idee diesen Vendor Lock-in zu verhindern, ergibt Sinn, aber die Frage ist eben, wo ist die Trennung zwischen unternehmerischen Risiko und kritischer Infrastruktur. Also da weiß ich nicht genau, was der richtige Weg wäre, aber ich glaube, wenn es da Vorgaben gibt, die zukünftigen Blödsinn verhindern, schadet das aus meiner Sicht nicht.

A.3.4 Hast du Erfahrungen gemacht, dass es schwieriger wird, wenn man unter solche Regulative fällt, als Unternehmen überhaupt gewisse Anbieter zu finden, die sich dem unterwerfen?

Ich persönlich bisher nicht, ich hätte es auch noch nicht gehört in meinem Umfeld.

A.3.5 Wird das bei einer Ausschreibung deiner Erfahrung nach abgenickt und akzeptiert, dass man sagt: ja, wir nehmen dich als Kunde, auch wenn du unter DORA fällst oder unter NIS.

Ich weiß gar nicht, ob das so deutlich immer bei den Ausschreibungen zum Tragen kommt. Wir zum Beispiel gehen mit eigenen Fragenkatalogen oder mit Anforderungen hinaus an die Provider, wo nicht nur steht: o. k., erfüllst du die Anforderungen von NIS oder GDPR oder von DORA oder was auch immer. Also nein, wäre mir bislang nicht aufgefallen, dass das ein Hinderungsgrund ist. Man streitet oder diskutiert immer wieder über manche Punkte dieser Anforderungen. Also so hundertprozentig – ja ja, wir machen alles, kein Problem – ist es auch nicht.

A.3.6 Sind die Möglichkeiten zu einem gewissen Grad eingeschränkt worden, als Unternehmen bei der Auswahl, insbesondere Richtung Cloud denkend, dass man sagt: Ich kann jetzt diesen und jenen Anbieter nicht mehr nehmen, weil er schlecht in den Medien dargestellt wurde oder der kann etwas möglicherweise nicht erfüllen?

Da habe ich keine genauen Einblicke, aber bei GDPR, wenn der Provider nicht in der EU ist und es keine entsprechenden Abkommen gibt, ist das jedes Mal eine Herausforderung.

A.3.7 Wie siehst du das Risiko für europäische Daten bei US-amerikanischen Anbietern durch den CLOUD-Act und der damit einhergehenden Problematik, dass Unternehmen möglicherweise zwei widersprüchliche Gesetze befolgen müssen (Datenweitergabe an USA vs. europäische Gesetze)?

Definitiv schwierig. Da habe ich jetzt keine persönlichen Berührungspunkte im Alltag, aber was ich von Kollegen mitbekomme, ist das natürlich ein Hindernis.

A.3.8 Gibt es auch ein Bewusstsein für die Problematik des CLOUD-Acts?

Wenn eine fremde Gesetzgebung auf unsere Daten vielleicht Zugriff hat, ja, das hindert dann sicher. Also gerade im Finanzdienstleister-Umfeld oder im Bankenumfeld. Es sind natürlich die Daten unserer Kundinnen der wichtigste Schatz sozusagen. Und wenn man dort die Vertraulichkeit aus der Hand gibt, tut man sich schwer. Das ist eine definitive Challenge.

A.3.9 Werden deiner Erfahrung nach in der österreichischen kritischen Infrastruktur Public Cloud Dienste eingesetzt für wirklich wesentliche Funktionen oder begrenzte das wirklich mehr auf Office IT?

Das kenne ich durchaus, auch unser Unternehmen setzt in kritischen Services Public Cloud ein. Ich glaube, diese Schwelle bzw. Hemmschwelle ist gefühlt vor ein paar Jahren gefallen. Wir setzen vermehrt auf Public Cloud. Und dort nicht nur auf eine, sondern auf hybride Cloudansätze. Den Vendor Lock-in z.B. probiert man zu vermeiden oder zumindest zu verteilen.

A.3.10 Gibt es Bereiche, wo Public Cloud Betrieb eine Red Flag wäre? Dass man ein bestimmtes Service nicht in die Cloud geben will, sondern es unbedingt und On-Premises hält?

Ich lehne mich jetzt aus dem Fenster, aber ich glaube, die Red Flags gibt es nicht mehr wirklich. Immer wieder wird der Preis genannt, also preislich zahlt es sich glaube ich aus. Man hat erkannt, dass Dinge wie eben Security oder Logging oder all diese Dinge von großen Providern teilweise wahrscheinlich sogar besser gemacht werden können, als wir die inhouse machen könnten. Man sieht auch Vorteile, warum man in die Cloud geht. Man steckt Ressourcen dazu oder nimmt sie auch wieder weg, wohin hingegen im Keller in einem Rechenzentrum, bis ich neue Rechenressourcen zugekauft habe, das heißt, bis die physisch bei uns sind, dauert es einfach. In der Cloud geht es hoffentlich mit einem Fingerschnippen. Ich glaube, es gibt Vorteile, die dann ebendiese Red Flags fallen lassen haben.

A.3.11 Welche Servicemodelle kommen deiner Erfahrung nach zum Einsatz?

Quer durch die Bank wird es bei uns eingesetzt. Je nachdem wo gerade Bedarf ist.

A.3.12 Gibt es bei den Unternehmen, die du kennst auch Katastrophenszenarien für Blackouts oder Internetausfall beim Zugriff auf Cloud-Dienste?

Kenne ich nicht im Detail, aber ja, ja klar gibt es da Notfallpläne, ja.

A.3.13 Und werden die geübt?

Mit Cloudanbietern offen gesagt weiß ich nicht, ob die schon geübt werden. Also ich hätte bis jetzt nicht gehört, dass man sagt, o. k., Internetleitung zum Cloudanbieter ist abgedreht. Ich glaube, man muss sich dort hinbewegen. Ich glaube für On-Premises Lösungen hat man zumindest im Bankenumfeld sicher jahrelang schon Stresstest oder Notfallübungen gemacht, aber ich denke, mit neuen Technologien sozusagen, dass man

Ausfälle von Cloud Anbietern übt, das ist neu, so wie Cloud an sich im Prinzip neu ist. Nun müssen auch die Dinge darum herum wieder neu eingespielt werden, unter anderem Notfallübungen.

A.3.14 Wo siehst du die größten Risiken bei Public Cloud Anbietern für kritische Infrastruktur?

Vielleicht nicht direkt für den individuellen Kunden, aber wenn großflächig bei einem Provider etwas passiert, sind gleich auf einen Schlag viele kritische Infrastrukturen betroffen. Microsoft war da vor Kurzem erst in den Medien, mit einem Security-Thema in der Cloud. Also wenn zentral etwas passiert, eben vielleicht ein zentrales Authentifizierungssystem oder eine zentrale Verschlüsselungskomponente, glaube ich schon, dass das kritisch wäre, wenn es dann auf einen Schlag viele erwischt. Das würde ich jetzt als größtes Risiko sehen. Für das individuelle Unternehmen glaube ich, ist das Risiko überschaubar. Wenn man etwa entsprechende Notfallpläne hat oder Services verteilt auf mehrere Rechenzentren auf unterschiedlichen Kontinenten oder auf unterschiedliche Provider hat, glaube ich, ist es handlebar.

A.3.15 Was hältst du eigentlich von den Bestrebungen, dass man eine europäische Cloud Lösung etablieren will?

Als schwarz-Denker glaube ich nicht, dass es viel Erfolgschancen hat. Ich sehe niemanden am Horizont. Ich könnte jetzt keinen großen europäischen Cloud-Anbieter nennen.

Es kommt allerdings auf die unterschiedlichen Cloud Service Modelle an. Dahin gehend glaube ich schon, dass es eine Chance gibt, wenn große Provider wie die Deutsche Telekom oder französische große Anbieter, wie OVH, für gewisse Servicemodelle in der Cloud [etwas anbieten], hat es vielleicht Erfolgschancen. Aber eben je weniger man auch selbst macht, desto weniger hat man Chancen, weil einfach Microsoft, Google und Co. schon so gute Produkte haben: die Vernetzung mit den Tools, die man noch dazu benötigt, wie administriert man das Ganze, wie bekomme ich Logs hinein oder hinaus? Wie bekomme ich Daten hinein oder hinaus? Wie bekomme ich Zugriffe hin, dann nutzen sie teilweise eigene Technologien. Oder z.B. Mail Systeme. Ich glaube nicht, dass Microsoft 365 leicht ablösbar durch etwas anders ist.

A.3.16 Hast du vielleicht noch etwas zu ergänzen zu dem Thema oder was noch wertvoll, wichtig sein könnte?

Wir sind z.B. dabei, Cloud Security Posture Lösungen einzusetzen. Dort kann man Security Konfigurationen von Cloud Anbietern zentral monitoren und zentral steuern, auch über mehrere Clouds hinweg. Das ist sicher ein Thema für die Zukunft. Du findest gleich Schwachstelle in den Konfigurationen oder Schwachstellen, die draußen herumkreuchen und fleuchen. Also ganz normale CVEs sind auch über diese Tools auffindbar in deinen Cloudlösungen, weil dort sind Webserver, Datenbanken und Co. im Einsatz, die auf

Schwachstellen geprüft gehören. Und das können manche dieser Tools, das ist sicher ein Zukunftsthema bzw. schon da.

A.3.17 Das könnte eine Idee sein, wie man mit diesem Risiko ein bisschen besser umgeht.

Wie man damit umgeht oder wie man es darstellen kann, vielleicht so, dass da super schöne Reports generiert werden, die dann wirklich etwas bringen eben in der zentralen Verwaltung und Remediation von Risiken.

A.3.18 Und Cloud-Anbieter unterstützen das?

Die großen definitiv ja. Auch da wieder vielleicht zur Frage vorhin: unterstützen die Kleinen das? Sind diese Tools mit den Kleineren kompatibel? Vielleicht sind es aber auch Standardschnittstellen, da fehlt mir der Einblick. Also zentrale Steuerung, zentrales Orchestrieren, zentrales Auswerten von Dingen über mehrere Clouds, das ist sicher ein Thema.

A.4 Wolfgang Rosenkranz

Interviewpartner	Wolfgang Rosenkranz
Hintergrund	Teamleiter CERT AT
Datum	3. Mai 2024
Uhrzeit	09:00-09:45
Ort	Online-Meeting via MS Teams

A.4.1 Wie schätzen Sie die aktuelle IT-Security Lage bei der österreichischen kritischen Infrastruktur ein?

Die kritische Infrastruktur hat zusammengefasst weniger Probleme als die anderen Bereiche, wobei kritisch Infrastruktur muss man immer unterscheiden: Die offizielle Definition ist einfach eine Liste, die das BVT irgendwann einmal erstellt hat. Das sind nicht zwangsweise und definitiv nicht die Unternehmen, die im Cyber Security Bereich relevant sind, weil es da mehr um die physische Sicherheit ging. Da ging es darum, wenn die ausfallen, dann sind größere Teile der Bevölkerung davon betroffen. Da geht es um Sabotage, Spionage und so weiter und sofort. Deswegen ist für die kritische Infrastruktur auch der Verfassungsschutz zuständig, weil der sich mit Terrorismus usw. beschäftigt. Der NIS unterworfene Unternehmen, für die war immer schon relevant, haben sie im Cyber Security und digitalen Bereich eine größere Bedeutung. Und mit NIS 2 wird das Ganze jetzt dann noch erweitert. Einfach auf alle Unternehmer, die mehr als 50 Mitarbeiter haben und bestimmte finanzielle Grenzwerte überschreiten. Es gibt viele Unternehmen, die bis jetzt einfach nur unter Anführungszeichen Betreiber kritische Infrastrukturen waren und mit NIS 1 nichts zu tun hatten. Wenn die zwei zusammengeführt werden, was unter NIS 2 ganz sicher bei vielen passiert wird, weil normalerweise Betreiber kritischer Infrastruktur eher größer sind, wird die Überschneidung interessant. Was passiert mit den Unternehmen, die bis jetzt NIS 2 nicht umsetzen mussten. Melden die dann mehr, sehen wir dann mehr Cyber Vorfälle, als wir es vorher gesehen haben, weil die alles, was sie bis jetzt hatten, unter den Teppich kehren konnten – was keine Unterstellung ist – aber nur die die Möglichkeit war da, das einfach für sich zu behalten. Grundsätzlich, ich glaube nicht, dass es eine riesige Überraschung wird, weil wir unter NIS 1 schon sehen, dass die Meldungen, die bei uns über das nationale CERT und auch über das Energy CERT geliefert werden müssen, dass diese Meldungen so gut wie immer Meldungen von technischen Defekten sind und keine Cyberangriffe. Was bedeutet, dass die Unternehmen, die unter NIS 1 fallen, ihren Laden gut im Griff haben. Und dann habe ich noch dieses Beispiel im Energiebereich, weil wir auch der Betreiber des Energy CERT sind. Der Energiebereich hat nahezu keine erfolgreichen Cyberangriffe und dem unterstellt man permanent, dass er de facto den Untergang des Abendlandes verursachen wird. Was aber einfach ein schlechtes Gerücht ist und eine Angst, wenn man sagt, Strom benötigt man in jedem Fall, aber die haben sich dementsprechend auch wirklich schon seit vielen, vielen Jahren mit dem Thema beschäftigt und die stehen einfach besser da als viele

andere, obwohl sie das Image haben, dass sie immer noch mit Ferraris-Zähler arbeiten und Digitalisierung nicht im Griff haben, das stimmt einfach nicht.

A.4.2 Ist die aktuelle regulatorische Entwicklung mit NIS, NIS 2, DORA, Cyber Resilience Act usw. auf dem richtigen Weg? Was könnte man besser machen?

Das ist definitiv der richtige Weg, obwohl ich auch das Risiko sehe, dass es der Wirtschaft massiv wehtun kann. Man muss aber zum Teil die Kirche im Dorf lassen, weil es sind 6.000 Unternehmer maximal, also zumindest ist das die gängige Schätzung, so genau weiß das keiner. Aber das sind weniger als 2% der österreichischen Unternehmen, die das jetzt tatsächlich betrifft. Allerdings muss man wieder deren Lieferanten und usw. dazu rechnen. Es müssen diese circa 6.000 Unternehmen auf den Stand der Technik kommen, was Cybersicherheit betrifft und das ist nicht ein „Ich kaufe mir jetzt irgendeine Software oder ich kaufe mir irgendein Gerät“ oder so in die Richtung, sondern wir sehen das jetzt schon auch in Diskussionen, was dann im Detail vorgeschrieben wird. Das sind ganz viele Prozessthemen dabei, es sind ganz viele Policy Themen dabei, dass einfach alles dokumentiert wird, dass jeder Patch vorbereitet wird, in eine Patch Policy hineinpassen muss, das dokumentiert wird, wer was wann eingespielt hat und so weiter und sofort, dass Schwachstellen gemonitored werden, dass es hier für alles, was ein Unternehmen im digitalen Bereich macht, muss es einfach eine bewusste Entscheidung geben, die auch nachvollziehbar ist, und auch dokumentiert wird. Das ist der Kernpunkt der ganzen Geschichte, und das Ganze baut auf dem Fundament Risikoanalyse auf, und zwar nicht einfach irgendwie, sondern das ist etwas, was man tatsächlich jedem, der neu in das Thema hineinkommt, mindestens dreimal erklären muss. Die sagen „Risikoanalyse kenne ich ja, da macht man eine Matrix und fertig und der Geschäftsführer sagt am Schluss, was ihm wichtig ist.“ Das ist es nicht, sondern sowohl NIS als auch DORA zwingt die Unternehmen ihr komplettes Unternehmen anzuschauen, in einer Risikoanalyse und dann selbst zu bewerten, was jetzt im Unternehmen aus einer Cybersecurity Sicht heraus relevant ist und was gefährdet ist und was geschützt werden muss. Aber nicht so, dass der Geschäftsführer selbst entscheidet, sondern es schaut jemand extern auch noch darauf. Aber die erste Arbeit ist die Risikoanalyse, sich das komplette Unternehmen anzuschauen aus einer Cyber Security Brille heraus. Das muss das Unternehmen vorher machen. Alle Diskussionen, die derzeit mit den Autoren des Gesetzes geführt werden, sind immer so: „Muss ich das machen und fällt das auch darunter?“ und die Antwort ist meistens: „Das weiß ich nicht, das kommt auf das Ergebnis der Risikoanalyse an“. Und das ist schon ein massiver Fortschritt, dass man einfach sagt: Nein, es gibt nicht einfach nur eine Vorschrift und eine Liste, über die ich mich dann beschweren kann, dass da nur Ahnungslose sitzen, die mein Unternehmen nicht verstehen. Sie haben den Spieß umgedreht, sie haben gesagt, verstehst du dein Unternehmen eigentlich? Weißt du, was du hast? Kennst du alle Assets, die du hast? Weißt du, was die tun? Weißt du, wohin die kommunizieren? Weißt du, wo die ihre Updates herbekommen und so weiter und so fort und wenn nicht, dann brauchst du nicht zu mir kommen und mir einfach sagen, das ist unfair, was da passiert. Ja, weil

das, was wir von dir erwarten, ist, dass du, wenn du digitale Geräte verwendest, auch das verstehst, dass du das alles im Griff hast. Und das kann nur dazu führen, dass die Cybersicherheit verbessert wird. Das ist etwas, wenn ich mit Leuten spreche, die solche Sachen schon seit längerer Zeit implementiert haben, sagen sie: „State of the Art, ist nichts Neues dabei!“ Wenn man mit Unternehmen redet, die bisher nicht unter NIS dabei waren oder mit dem Thema wenig zu tun haben, sagen sie, wie soll das gehen? Ich brauche massenhaft Leute dafür, das ist alles neu. Das haben wir noch nie gemacht, wir haben noch nie aufgeschrieben, wann wir Updates einspielen, wir spielen die einfach ein und hoffen, dass dann alles gut wird. Ja und das wird ein Angleichen dieser Nachzügler der Unternehmen, die bis jetzt nicht viel gemacht haben, weil sie gesagt haben, auch teilweise zu Recht, sie können es sich nicht leisten, weil ihr Geschäftsmodell es vielleicht nicht hergibt. Anders die Unternehmen, die sagen, wir mussten das schon immer machen, weil wir mussten immer schon nachweisen, dass wir sicher sind, weil sonst können wir nicht arbeiten. Siehe kritische Infrastruktur. Also, es kann nur besser werden.

Zum zweiten Teil der Frage: was kann man besser machen? Ich glaube das, was sich jetzt wieder abzeichnet, ist, dass anscheinend erneut ein paar Länder es geschafft haben oder argumentieren werden, dass sie, die Vorgaben aus Brüssel nicht so ernst nehmen wie Österreich. Österreich ist lustigerweise tatsächlich ein Musterschüler, was diese Sachen betrifft. Oder manche Leute behaupten, wir betreiben Goldplating. Ja, das ist dann eine negative Interpretation. Aber andere Länder werden das wahrscheinlich wieder lockerer sehen und damit habe ich wieder nicht das eigentliche Ziel von NIS: ein einheitliches Cybersecurity-Niveau in ganz Europa. Das ist das eigentliche Problem und das wird wahrscheinlich mit NIS 3, wenn es dann einmal kommt wahrscheinlich ausgeglichen werden, weil dann wird irgendwann Brüssel sagen, es reicht, wir machen eine Verordnung, die gilt jetzt für alles, es gibt keinen Interpretationsspielraum mehr bei den einzelnen Ländern. Aber momentan sehe ich bei der österreichischen Umsetzung von NIS 2 noch nichts, wo ich sagen kann, da ist etwas falsch oder fehlt, sondern jetzt würde ich ganz gerne mal sehen, wie die Umsetzung funktioniert und das Problem, dass dabei entstehen könnte, ist das, was ich vorher schon kurz angerissen habe, dass viele Geschäftsmodelle das einfach nicht verkraften. Weil sie so arbeiten, dass sie knapp positiv sind. Und dann kommt jemand und sagt, ich gebe euch einen sehr umfangreichen, aufwendigen Verwaltungsapparat. Ich schreibe euch den vor und prüfe den auch noch und wenn das nicht funktioniert, werdet ihr bestraft. Das bedeutet viel, viel Geld und das können sich möglicherweise nicht alle leisten.

A.4.3 Sehen Sie Risiken oder Hindernissen, wenn kritische Infrastruktur Kernfunktionen an Dritte bzw. Cloud Dienste auslagert?

Na ja, das ist die übliche Sache: Ich gebe etwas jemand anderem. Die Frage ist, wie sehr kann ich mich darauf verlassen, dass der andere dann seinen Job richtig macht oder auch mich nicht hintergeht. Das ist wahrscheinlich dann die Extremform, dass ich mich auf jemand verlasse, der in Wirklichkeit nicht vertrauenswürdig ist und meine Daten stiehlt

oder so in die Richtung. Aber das ist eher das seltenere Problem. Das größere Problem ist, dass man sagt, man hat dann einen zentralen Anbieter, der für mehrere Kunden tätig ist, was normalerweise der Fall ist, sonst funktioniert solch ein Geschäftsmodell nicht gescheit und ist dementsprechend auch ein lohnendes Ziel für Angreifer. Und wenn dann da jemand hineinkommt, dann ist gleich mal viel Schaden angerichtet. Siehe Microsoft, die Problematik, die sie momentan gerade haben, wo man sagen kann, größer geht wohl nicht mehr. Also das ist nicht irgendein kleines Unternehmen, dass das Thema nicht ernst genommen hat, sondern die nehmen das Thema Security sehr wohl ernst, auch wenn es Kritik gibt, dass sie mehr machen könnten, aber das ist trotzdem bei denen einfach immer da und auch dort passiert es. Das ist eben ein Vorteil bei NIS 2, dass NIS 2 auch die Unternehmen zwingt, wenn sie das machen, dass sie sich auch damit beschäftigen, an wen sie da auslagern und wie dieses Unternehmen die Sicherheit gewährleisten will. Das Problem, das diese Cloud-Anbieter jetzt dann haben werden: (ich bin mir nicht sicher, ob das bei NIS 2 dabei ist) aber bei DORA ist es in jedem Fall so, dass es derzeit diskutiert wird, ob man diese Prüfungen dann nicht zusammenlegen kann, damit nicht die Cloudanbieter ein Audit, eine Prüfung nach der anderen haben und damit haben die auch wieder das Problem, dass sie zumindest mehr Aufwand betreiben müssen. Damit wird das Ganze wahrscheinlich zumindest teurer, weil sie mehr Spezialisten brauchen und so weiter. Also ich verschiebe zum Teil das Problem, dass ein Unternehmer keine Fachkräfte hat, findet oder einstellen will, auf den Cloud-Anbieter, der sich ein wenig leichter tut, weil er es für mehrere Unternehmen macht, aber der trotzdem sein Geschäftsmodell wahrscheinlich noch mal anschauen muss. Und dann habe ich wieder das Problem, dass mir der Cloud Lieferant dann irgendwann abhandenkommt, weil er sagt, ich schaffe das nicht. Was interessant ist, dass insbesondere unter DORA die Vorgabe auch besteht, dass wenn man einen Cloud-Anbieter hat, dass man einen alternativen Plan braucht, der aber auch getestet sein muss. Also ich muss tatsächlich ausprobieren, ob ich von Azure auf die AWS ausweichen kann, wenn ich das in meinem Konzept drinnen habe. Man sieht bei DORA im Finanzbereich sind die Sachen ein wenig weiter vorn, die sind ein wenig strenger. Ich glaube, dass das wahrscheinlich dann bei NIS auch irgendwann mal der Fall sein wird, dass man sagt, ich kann nicht einfach nur auslagern in die Cloud, ich brauche eine Alternative, das muss auch funktionieren, wenn der eine Cloud-Anbieter betroffen ist oder zu sperrt oder was auch immer und dementsprechend ist der Aufwand, den ich dann damit habe, möglicherweise irgendwann nicht mehr geringer als wenn ich die Sache selbst betreibe. Also das wird ganz sicher jetzt noch schwieriger sein zu bewerten, wann zahlt es sich aus, das auszulagern, oder ist es nicht vielleicht doch wieder geschickter Sachen selbst zu machen, weil einfach die Vorgaben so intensiv werden?

A.4.4 Haben Sie eine grobe Idee, wie viele Betreiber der österreichischen kritischen Infrastruktur bereits Kernfunktionen an Public Cloud-Anbieter ausgelagert haben?

Ich weiß es konkret nur aus dem Finanzbereich, weil dort die Unternehmen, mit denen wir reden, uns gesagt haben, man kommt als Finanzunternehmen an einer Auslagerung

in eine Cloud überhaupt nicht mehr vorbei. Also bei denen ist jedes Rechenzentrum de-facto eine Cloud. Von den Banken her, ist das das gängige Bild, dass dort alle, auch die Großen auslagern, weil sie es nicht anders schaffen, oder wollen.

A.4.5 Die setzen auch auf Public Cloud-Anbieter?

Großteils ja, also wenn Sie darunter Azure, AWS und so weiter verstehen, dann ja.

Ein Thema in diesem Zusammenhang sind Shared Services, dass momentan auch unter NIS 2 aufkommt. Wie sehr die Sicherheit nachgewiesen werden kann bei Shared Services. Wie weit hier zum Beispiel auch der Kunde Einfluss nehmen kann auf Patch-Zyklen und so weiter, wer da die Dokumentation macht. Also das wird tatsächlich recht kompliziert und dadurch alleine, dass diese Diskussion – und auch teilweise sehr emotional – geführt wird, erkennt man, dass das ein Thema ist für viele Unternehmen, dass die das in Anspruch nehmen.

A.4.6 Wie sehen Sie das Risiko für europäische Daten bei US-amerikanischen Anbietern durch den CLOUD-Act und der damit einhergehenden Problematik, dass Unternehmen möglicherweise zwei widersprüchliche Gesetze befolgen müssen (Datenweitergabe an USA vs. europäische Gesetze)?

Da bin ich nicht Experte genug auf dem Thema. Also grundsätzlich einmal, nachdem ich die Diskussion jetzt auch schon seit Jahrzehnten mitverfolge:

Offenbar gibt es keine saubere Lösung. Ja, es ist anscheinend nicht gelungen, die Sachen rein nach Europa hineinzuziehen und selbst wenn sie in Europa waren, was ja die Microsoft auch teilweise gemacht hat, dann der potenziellen US-Kontrolle zu entziehen. Die Microsoft hatte einmal das Angebot, dass sie ein Rechenzentrum aufbaut in Deutschland, das dann von der, glaube ich, Deutschen Telekom betrieben wurde. Das haben sie dann, soweit ich weiß, wieder eingestellt, weil es allen zu teuer war. Das war dann wirklich nach dem Motto, wir sind gar nicht mehr zuständig, wir bauen es nur auf, ja, aber es ist ein europäisches Unternehmen dann zuständig, dementsprechend keine Möglichkeit hier für ein US-Gericht einzugreifen. Ich glaube zumindest, dass das damals die Idee war.

Es wollte nur keiner haben oder zu wenige. Ja und dementsprechend ist das immer die alte Geschichte. Man darf nicht vergessen und das ist ein Punkt, wo NIS 2 ganz massiv hineinfährt, digitale Geschäftsmodelle leben einfach dann tatsächlich davon, dass irgendetwas 1 Cent billiger ist als ein anderes Angebot. Weil wenn man das ganze dann mal 10 Milliarden macht, dann zahlt sich das aus. Ich interpretiere die Vorgangsweise von Brüssel so, dass sie sagen, alle, die nicht in der Lage sind, eine sichere Digitalisierung zu betreiben, haben nichts am europäischen Markt verloren. Und wenn euer Geschäftsmodell das nicht hergibt, dann sperrt zu.

Es nimmt ein wenig den Spaß aus der Digitalisierung, zu sagen vielleicht finde ich ein cooles Modell, digitales Angebot, eine Service-Leistung die einfach etwas schneller ist,

ein wenig schöner ist, ein bisschen besser funktioniert – und dann kommt Brüssel und sagt ja, das ist alles o. k., das ist alles nett, aber ist das auch sicher und kannst du das auch auf einer Tagesbasis nachweisen? Und das ist etwas, über das viele sich bis jetzt keine großartigen Gedanken gemacht haben, inklusive auch, können die US-Gerichte auf Daten zugreifen? Etwa in die Richtung und die Diskussion, die damals mit der DSGVO diesbezüglich losgetreten wurde, dürfte auch wieder abgeebbt sein, so wie die ganze DSGVO momentan glaube ich einfach für alle weniger ein Thema ist, zum Teil auch deswegen, weil die Aufsicht nicht nachkommt, den Fällen nachzugehen, aber das wird jetzt mit NIS wahrscheinlich noch einmal verschärft werden. Wir werden die Diskussion wahrscheinlich wieder neu erleben. Ich glaube, dass viele Unternehmen es sich trotzdem deswegen nicht leisten können oder wollen, dass sie sagen, sie verzichten auf die Cloud.

ANHANG B

Datenbasis der Sicherheitsvorfälle

B.1 Sicherheitsvorfälle bei Betreibern kritischer Infrastruktur in Österreich

Datum	Mögliche Klassifizierung	Möglicher Sektor	Art	Einstiegspunkt
04.02.2016[1]	Wichtig	Verarbeitendes Gewerbe/Herstellung von Waren	CEO Fraud	
06.03.2018[2]	Wesentlich	Verwaltung von IKT-Diensten		
09.05.2019[3]	Wesentlich	Öffentliche Verwaltung	Denial of Service	
06.01.2020[4]	Wesentlich	Öffentliche Verwaltung		
24.05.2020[5]	Wesentlich	Öffentliche Verwaltung	Ransomware Data breach	Phishing-Mails und VBScript
10.06.2020[6]	Wesentlich	Digitale Infrastruktur		
25.01.2021[7]	Wichtig	Verarbeitendes Gewerbe/Herstellung von Waren		
14.04.2021[8]	Wichtig	Verarbeitendes Gewerbe/Herstellung von Waren		
24.06.2021[9]	Wichtig	Produktion Verarbeitung und Vertrieb von Lebensmitteln	Ransomware	
17.01.2022[10]	Wesentlich	Finanzmarkt-Infrastrukturen	Ransomware	Schadsoftware
28.03.2022[11]	Wichtig	Forschung		

07.04.2022[12]	Wichtig	Verarbeitendes Gewerbe/Herstellung von Waren		
25.04.2022[13]	Wichtig	Verarbeitendes Gewerbe/Herstellung von Waren		
12.08.2022[14]	Wichtig	Verarbeitendes Gewerbe/Herstellung von Waren		
22.08.2022[15]	Wesentlich	Trinkwasser	Data breach	
06.09.2022[16]	Wesentlich	Öffentliche Verwaltung	Ransomware	Home-Office Angriff
02.11.2022[17]	Wichtig	Produktion Verarbeitung und Vertrieb von Lebensmitteln	Data breach	
25.11.2022[18]	Wichtig	Produktion Verarbeitung und Vertrieb von Lebensmitteln	Denial of Service	
16.12.2022[19]	Wesentlich	Verkehr	Denial of Service	
01.02.2023[20]	Wesentlich	Digitale Infrastruktur	Data breach	
06.02.2023[21]	Wichtig	Forschung	Versuch	
15.02.2023[22]	Wichtig	Forschung	Ransomware	
16.02.2023[23]	Wichtig	Verarbeitendes Gewerbe/Herstellung von Waren	Ransomware	
24.03.2023[24]	Wichtig	Verarbeitendes Gewerbe/Herstellung von Waren		
21.04.2023[25]	Wichtig	Verarbeitendes Gewerbe/Herstellung von Waren		
06.06.2023[26]	Wesentlich	Öffentliche Verwaltung	Data breach	Software vulnerability
09.06.2023[27]	Wesentlich	Gesundheitswesen	Ransomware	
08.07.2023[28]	Wichtig	Verarbeitendes Gewerbe/Herstellung von Waren	Data breach, Ransomware	
17.07.2023[29]	Wesentlich	Bankwesen	Data breach	Software vulnerability
25.10.2023[30]	Wesentlich	Verkehr	Data breach	
25.12.2023[31]	Wichtig	Forschung	Data breach	
11.03.2024[32]	Wesentlich	Finanzmarkt-Infrastrukturen		
13.03.2024[33]	Wesentlich	Verwaltung von IKT-Diensten		
13.03.2024[34]	Wesentlich	Verwaltung von IKT-Diensten		
27.03.2024[35]	Wesentlich	Öffentliche Verwaltung		Software vulnerability

Tabelle B.1: Sicherheitsvorfälle bei Betreibern kritischer Infrastruktur.

[1] Nachrichten.at, *Wie der FACC 50 Millionen abhanden kamen | Nachrichten.at*
[2] Kleine Zeitung, *Anexia: Größter Cyberangriff Österreichs auf Kärntner Firma*
[3] OE24, *Massiver Hacker-Angriff auf Stadt Wien - oe24.at*
[4] Kurier, *Cyberangriff auf Außenministerium läuft noch immer*
[5] Heise, *Hacker veröffentlichen Daten nach Cyberangriff auf städtische IT in Österreich | heise online*
[6] Handelsblatt, *A1 Telekom Austria wird Opfer von massivem Hackerangriff*
[7] Der Standard, *Globaler Cyberangriff auf Palfinger*
[8] Unterkaertner Nachrichten, *Geldforderung in Millionenhöhe: Bekannte Firma aus dem Lavanttal Opfer eines Hackerangriffs*
[9] Profil, *Wie Hacker SalzburgMilch lahmlegten*
[10] Kleine Zeitung, *Neuer Blümel-Arbeitgeber: Kundengelder nicht betroffen: Cyberattacke auf Superfund-Gruppe*
[11] ORF, *Uni Salzburg: Hackerangriff legt E-Mail-Server lahm - salzburg.ORF.at*
[12] Kleine Zeitung, *Straftaten im Netz steigen: Hackerangriff auf Papierfabrik Brigl & Bergmeister in Niklasdorf*
[13] ORF, *IMA Schelling Opfer eines Hackerangriffs - vorarlberg.ORF.at*
[14] Der Standard, *Cyberattacke: Offenbar Produktionsausfall bei BRP-Rotax in Oberösterreich*
[15] Futurezone, *Cyberangriff beschäftigt Wasserzähler-Hersteller Ista noch immer*
[16] Kurier, *Stadtgemeinde Feldbach von Hackerangriff betroffen*
[17] Der Standard, *Jö-Bonusclub: Betrüger hatten Zugriff auf 18.000 Konten*
[18] Mein Bezirk, *Hacker-Angriff sorgt für massive Probleme: Längere Wartezeiten im Kassenbereich bei Großhändler Metro - Hall-Rum*
[19] Futurezone, *DDoS-Attacke: Webseite der ÖBB und Ticketverkauf gestört*
[20] Kurier, *20.000 Kundendaten von Hackerangriff auf Magenta-Partner betroffen*
[21] Kurier, *Hacker versuchten Cyber-Attacke auf Uni Graz*
[22] ORF, *ISTA: Hackergruppe verlangte Lösegeld - noe.ORF.at*
[23] TroGroup, *TroGroup wurde Ziel eines Cyber-Angriffs | TroGroup*
[24] ORF, *Rosenbauer spricht über Cyberangriff - ooe.ORF.at*
[25] Kleine Zeitung, *Bestätigung im Netz: Anton Paar ist Opfer einer Cyber-Attacke geworden*
[26] Fondsprofessionell, *FMA von Hacker-Angriff betroffen | Recht | 06.06.2023 | FONDS professionell*
[27] Der Standard, *Labor Burgenland wurde Opfer eines Cyberangriffs*
[28] Krone, *An Kundendaten gelangt - Hackerangriff auf „Wien-Süd“: 50.000 Betroffene | krone.at*
[29] Kurier, *Hackerangriff auf Dienstleister: Datenleck auch bei der Bank99*
[30] Vienna.at, *Cyberangriff auf IT-System der Westbahn: Daten abgeflossen - Vienna Online - Österreich - VIENNA.AT*
[31] ORF, *Uni Innsbruck wurde Opfer von Hackern - tirol.ORF.at*
[32] Der Standard, *Kärntner Landesversicherung wurde Opfer von Cyberangriff*
[33] Der Standard, *Cyberangriff auf steirische IT-Firma*
[34] Der Standard, *Cyberangriff auf steirische IT-Firma*
[35] Kleine Zeitung, *Bereits Anfang März: Brucker Stadtwerke wurden Opfer eines Hackerangriffs*

B.2 Sicherheitsvorfälle mit Bezug Public Cloud

Datum	Potentielle Auswirkung	Potentielle Ursache
03.04.2024[1]	Data Leak	Unbekannt
20.10.2022[2]	Data Leak	Fehlkonfiguration
14.12.2020[3]	Data Leak	Supply Chain Attack
27.08.2021[4]	Data Leak	Vulnerability
15.04.2024[5]	Privilege Escalation	Fehlkonfiguration
28.03.2024[6]	Privilege Escalation	Vulnerability
05.10.2019[7]	Data Leak	Fehlkonfiguration
17.05.2023[8]	Data Leak	Fehlkonfiguration
04.01.2022[9]	Data Leak	Fehlkonfiguration
12.05.2023[10]	Data Leak	Fehlkonfiguration
11.10.2019[11]	Data Leak	Fehlkonfiguration
06.07.2022[12]	Data Leak	Fehlkonfiguration
13.12.2022[13]	Data Leak	Unbekannt
20.12.2017[14]	Data Leak	Fehlkonfiguration
23.07.2021[15]	Data Leak	Fehlkonfiguration
17.07.2017[16]	Data Leak	Fehlkonfiguration
13.07.2017[17]	Data Leak	Fehlkonfiguration
04.10.2018[18]	Unbekannt	Supply Chain Attack
27.02.2023[19]	Data Leak	Unbekannt
25.05.2023[20]	Unbekannt	Vulnerability
23.10.2020[21]	Data Leak	Fehlkonfiguration
09.04.2024[22]	Data Leak	Fehlkonfiguration
01.02.2024[23]	Data Leak	Fehlkonfiguration
15.09.2023[24]	Account Compromise	Phising
08.11.2023[25]	Account Compromise	Unbekannt
09.07.2019[26]	Data Leak	Fehlkonfiguration
11.07.2016[27]	Account Compromise	Unbekannt
30.01.2023[28]	Data Leak	Fehlkonfiguration
28.07.2020[29]	Data Leak	Unbekannt
22.02.2018[30]	Cryptojacking	Fehlkonfiguration
11.10.2019[31]	Data Leak	Fehlkonfiguration

Tabelle B.2: Sicherheitsvorfälle mit Bezug Public Cloud

[1] CRN, *Microsoft's 'Inadequate' Security Behind Cloud Email Breach: U.S. Review Board*
[2] Spiceworks, *Misconfigured Azure Blob Storage Exposed the Data of 65K Companies and 548K Users*
[3] Reuters, *Suspected Russian hackers spied on U.S. Treasury emails*
[4] The Verge, *Microsoft Azure cloud vulnerability is the 'worst you can imagine'*
[5] Datadog Security Labs, *Amplified exposure: How AWS flaws made Amplify IAM roles vulnerable to takeover*
[6] NetSPI, *Azure Site Recovery Services: Elevating Privileges*

[7] Threatpost, *Is AWS Liable in Capital One Breach?*
[8] The Register, *Another security calamity for Capita: Unsecured AWS bucket*
[9] Threatpost, *SEGA's Sloppy Security Confession: Exposed AWS S3 Bucket Offers Up Steam API Access & More*
[10] The Stack, *Toyota data breach: vehicle location data for millions leaked*
[11] Threatpost, *Imperva: Data Breach Caused by Amazon Cloud Misconfiguration*
[12] Darkreading, *Cloud Misconfig Exposes 3TB of Sensitive Airport Data in Amazon S3 Bucket*
[13] Darkreading, *Uber Breached, Again, After Attackers Compromise Third-Party Cloud*
[14] Security News, *Data on 123 Million US Households Exposed Due to Misconfigured AWS S3 Bucket*
[15] Security Magazine, *US municipalities suffer data breach due to misconfigured Amazon S3 buckets*
[16] Forbes, *Cloud Storage Error Exposes Over Two Million Dow Jones Customer Records*
[17] iTnews, *Millions of Verizon customer details exposed on misconfigured Amazon S3 server*
[18] Bloomberg, *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*
[19] 9to5mac, *LastPass says engineer's hacked computer led to security breach*
[20] Darkreading, *Google Cloud Bug Allows Server Takeover From CloudSQL Service*
[21] Spiceworks, *Pharma Giant Pfizer Suffers Patient Data Leak Due to Cloud Misconfiguration*
[22] TechCrunch, *Microsoft employees exposed internal passwords in security lapse*
[23] The Sydney Morning Herald, *Football Australia data breach exposes players' passports, contracts*
[24] Bleepingcomputer, *Retool blames breach on Google Authenticator MFA cloud sync feature*
[25] Bleepingcomputer, *Sumo Logic discloses security breach, advises API key resets*
[26] Bloomberg, *DNA Test Service Exposed Thousands of Client Records Online*
[27] Threatpost, *Datadog Forces Password Reset Following Breach*
[28] Bleepingcomputer, *U.S. No Fly list shared on a hacking forum, government investigating*
[29] Techcrunch, *Alcohol delivery service Drizly hit by data breach*
[30] Threatpost, *Cryptojacking Attack Found on Los Angeles Times Website | Threatpost*
[31] Threatpost, *Imperva: Data Breach Caused by Amazon Cloud Misconfiguration*

Übersicht verwendeter Hilfsmittel

- LanguageTool (languagetool.org) durchgehend zur Komma-, Grammatik- und Rechtschreibüberprüfung
- Overleaf Writefull (www.writefull.com) durchgehend zur Komma-, Grammatik- und Rechtschreibüberprüfung

Abbildungsverzeichnis

Tabellenverzeichnis

Glossar

Anbieter digitaler Dienste Anbieter eines Online-Marktplatzes, einer Online-Suchmaschine oder eines Cloud-Computing-Dienstes ([1]). 34, 38, 39, 41, 42, 44, 149

Autoscaling Automatische Ressourcenanpassung an den Bedarf. 12

Betreiber wesentlicher Dienste Ein Betreiber der einen kritischer Dienst der für das Funktionieren der Gesellschaft und Wirtschaft notwendig ist, zur Verfügung stellt (siehe Kapitel 4.1)[2,3]. 33–35, 37, 38, 41–44, 46, 149

CEO-Fraud Mitarbeiter:innen werden durch Betrug dazu gebracht, unerlaubte Transaktionen durchzuführen[4]. 102

Cloud-Repatriation Der Transfer von an Public Cloud-Anbieter ausgelagerte Dienste hin zu On-Premises[5]. 22

Crash Dump Speicherauszug nach einem Programmabsturz. 108

Cryptojacking Missbräuchliche Verwendung fremder Rechenressourcen um Kryptowährungen zu erzeugen[6]. 107

Cyber Kill Chain Ein vom US-amerikanischen Unternehmen Lockheed-Martin entwickeltes Modell zur Erkennung und Verhinderung von Aktivitäten im Bereich des Cyberangriffs[7]. 27

Denial-of-Service Ein Überlastungsangriff um Systeme unbenutzbar zu machen[8]. 20, 21, 102

[1] *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*, §3 Z 12.
[2] Ebd., §3 Z 9, Z 10.
[3] *Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016*, Artikel 5.
[4] Bundeskriminalamt, *CEO Fraud*.
[5] Jewargi, „Public Cloud to Cloud Repatriation Trend“, S. 1.
[6] Interpol, *Cryptojacking*.
[7] Lockheed Martin, *Cyber Kill Chain*.
[8] BSI, *Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)*.

Edge-Computing Datenverarbeitung findet bei der Datenquelle oder in direkter Nähe statt. 6

Einrichtungen der öffentlichen Verwaltung Einrichtungen des Bundes und zu bestimmende Einrichtungen der Bundesländer[9]. 34, 38, 39, 41

Fault Tolerance Robustheit gegen Benutzungsfehler. 12

Fog-Computing Datenverarbeitung findet zwischen Endgeräten und Cloud statt. 6

Gaia-X Europäisches Projekt als Grundlagen für den Aufbau einer vernetzten, offenen Dateninfrastruktur auf Basis europäischer Werte[10]. 87, 112

Gesetz über digitale Märkte Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte - Alternative Bezeichnungen: GDM, Digital Markets Act, DMA).

Grid-Computing Ressourcen werden über mehrere Organisationen hinweg geteilt und zusammengefasst, meist mit dem Ziel, Computing Kapazitäten zu maximieren, also möglichst große Rechenleistung zu erreichen[11]. 6

Hochverfügbarkeit Verfügbarkeit von 99,999 %. 12

Hyperscaling Skalierung in verteiltem und großem Ausmaß. 10

Hypervisor System zum Betrieb mehrere Gast-Betriebssysteme innerhalb eines Hosts.

Incident Response Reaktion auf IT-Sicherheitsvorfälle. 22

Innerer Kreis der Operativen Koordinierungsstruktur Struktur zur Koordination auf der operativen Ebene im Bereich der Sicherheit von Netz- und Informationssystemen bestehend aus Vertretern des Bundeskanzlers, des BMI, des Bundesministers für Landesverteidigung und des Bundesministers für Europa, Integration und Äußeres[12]. 162

Load Balancing Automatische Lastverteilung. 12

[9] *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*, §3 Z 19.

[10] Bundesministerium für Wirtschaft und Energie (BMWi), *Das Projekt GAIA-X – Eine vernetzte Dateninfrastruktur als Wiege eines vitalen, europäischen Ökosystems*, S. 2.

[11] Dillon, Wu und Chang, „Cloud computing: issues and challenges“, S. 29–30.

[12] *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*, §3 Z 4.

Micro Segmentation Netzwerk Segmentierung pro Knoten. 22

Middleware Eine Software, die zwischen Betriebssystem und Anwendungen steht, um Anwendungen zu verbinden[13]. 14

NIS Fact Sheets Unterstützungsmaterial zur Befolgung von NISG. 35, 39, 46, 92

Non-Repudiation Unabstreitbarkeit einer stattgefundenen Kommunikation. 18

On-Premises Systeme befinden sich am Standort des Betreibers und sind nicht an Dritte ausgelagert. 2, 10, 11, 13, 22, 23, 72, 82–84, 99

Ping Prüfen der Erreichbarkeit von Hosts in IP-Netzwerken. 12

Provisionierung Bereitstellung von IT-Ressourcen. 5,

Ransomware Ein Schadprogramm mit dem Ziel sämtliche Daten auf einem System zu verschlüsseln. 20, 102, 110

Reverse Proxy Ein Server der externe Anfragen an interne Server weiterleitet. 109,

Single Sign-On Zentrale Anmeldung an einem Arbeitsplatz, die automatische eine Authentifieriung an angebundenen Diensten ermöglicht. 21

Threat-Led Penetration Testing Bedrohungsorientierter Penetrationstests, bei dem es zur Nachbilung realer Angreifer kommt und kritischen Live-Produktionssysteme getest werden[14]. 64, 164

Zero Trust Sicherheitskonzept bei dem angenonnem wird, dass kein Teilnehmer (System oder Mensch) vertrauenswürdig ist. 21, 22

[13] Microsoft Azure, *Was ist Middleware – Definition und Beispiele.*

[14] *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022*, Art 3 Z 17.

Akronyme

ABAC Attribute-based Access Control. 21,

Abs Absatz.

AEUV Vertrag über die Arbeitsweise der Europäischen Union. 68,

AIaaS Artifical-Intelligence-as-a-Service. 18,

AICPA American Institute of Certified Public Accountants. 89,

AIT Austrian Institute of Technology. 25,

API Application Programming Interface. 109,

Art Artikel.

AWS Amazon Web Services. 13, 38, 85, 88, 90–92, 94,

Azure Microsoft Azure. 13, 38, 85, 88, 90–93,

B-VG Bundes-Verfassungsgesetz. 56,

BIA Business-Impact-Analyses. 63,

BKA Bundeskanzleramt. 35, 39,

BMI Bundesminister für Inneres. 37–39, 41, 42, 55, 156,

BMK Bundeskanzleramt.

BMWi Bundesministerium für Wirtschaft und Energie.

BWG Bundesgesetz über das Bankwesen. 2, 31, 69–71, 88, 90, 91, 111,

CaaS Container-as-a-Service. 17,

CASSIS Center for Advanced Security, Strategic and Integration Studies. 87,

CCM Cloud Controls Matrix. 89,

CDN Content Delivery Network. 49,

CEO Chief Executive Officer. 2,

CER Richtlinie (EU) 2022/2557 über Resilienz kritischer Einrichtungen. 2, 52, 57–59, 113,

CERT Computer-Notfallteam. 3, 79,

CIA Confidentiality (Vertraulichkeit), Integrity (Integrität) und Availability (Verfügbarkeit). 18, 19, 89, 149,

CIAA Confidentiality (Vertraulichkeit), Integrity (Integrität), Authenticity (Authentizität) und Availability (Verfügbarkeit). 62,

CIEM Cloud Infrastructure Entitlements Management. 22,

CIRA Cloud Investigation and Response Automation. 22,

CIS Center for Internet Security. 90, 91,

CISA Cybersecurity and Infrastructure Security Agency. 108, 109,

CLOUD Act Clarifying Lawful Overseas Use of Data Act. 26, 70, 73–75, 99, 112,

CMS Compliance-Management-System. 92,

CoC EU Cloud Code of Conduct. 89, 90,

CRA Cyber Resilience Act. 52,

CRM Customer Relationship Management. 6, 14,

CRV Verordnung (EU) über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen. 2, 27, 52, 53,

CSA Cloud Security Alliance. 28, 89,

CSA Verordnung (EU) 2019/881 über die ENISA und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik. 2, 50, 51, 90, 91,

CSIRT Computer Security Incident Response Team bzw. Computer-Notfallteam. 46,

CSP Cloud Service Provider.

CSPM Cloud Security Posture Management. 22, 28,

CSZG Bundesgesetz zur Einrichtung einer nationalen Behörde für die Cybersicherheitszertifizierung - Cybersicherheitszertifizierungs-Gesetz. 50,

CVE Common Vulnerabilities and Exposures. 108,

DAC Discretionary Access Control. 21,

DBaaS Database-as-a-Service. 17,

DDI Digitale Dependenz Index. 87,

DDOS Distributed Denial-of-Service. 20,

DNS Domain Name System. 18, 45, 48,

DORA Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor. 2, 31, 52, 53, 60–70, 81, 88, 90, 91, 111–113, 150,

DOS Denial-of-Service. 20,

DSGVO Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr. 75, 76, 89,

EBA Europäische Bankenaufsichtsbehörde. 2, 31, 68, 70, 71, 88, 90, 91, 111,

EBA-Verordnung Verordnung (EU) 1093/2010 zur Errichtung einer Europäischen Aufsichtsbehörde. 70,

Ebd Ebenda.

EC2 Elastic Compute Cloud.

ECCG Europäische Gruppe für Cybersicherheitszertifizierung. 50, 52,

ECG E-Commerce-Gesetz. 39,

ECUC European Cloud User Coalition. 88, 90,

EDPB European Data Protection Board. 74,

EDPS European Data Protection Supervisor. 74,

EDR Endpoint Detection and Response. 28,

EDSA Europäischer Datenschutzausschuss. 89,

EIOPA Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung. 68,

EK Europäische Kommission. 28, 31, 47, 48, 52, 53, 66, 68, 75,

ENISA Agentur der Europäischen Union für Netz- und Informationssicherheit. 47, 50, 53,

EO Executive Order. 75,

ErwGr Erwägungsgrund.

ESA Europäische Aufsichtsbehörden. 66, 68,

ESMA Europäische Wertpapier- und Marktaufsichtsbehörde. 68, 88, 90, 91,

EU Europäische Union. 1–3, 6, 8, 9, 15, 17, 25, 26, 28, 31, 41, 48, 58, 71, 74–77, 87, 88, 99, 111–113, 149, 150,

EU5G European Cybersecurity Certification Scheme for 5G. 50,

EUCC Cybersecurity-Zertifizierungsschema der Europäischen Union. 50,

EUCS Cloud Services Schema. 31, 51, 52,

EuGH Europäische Gerichtshof. 75, 77,

Eurostat Statistische Amt der Europäischen Union. 6, 17,

EZB Europäische Zentralbank. 63,

FaaS Function-as-a-Service. 17,

FISA Foreign Intelligence Surveillance Act. 70, 74, 75, 96, 98, 99, 112, 150,

FMA Österreichische Finanzmarktaufsicht. 71–73,

FPÖ Freiheitliche Partei Österreichs. 56, 57,

GCP Google Cloud Platform. 13, 38, 85, 88, 90–94,

GovCERT Computer-Notfallteam der öffentlichen Verwaltung. 39, 41,

IaaS Infrastructure-as-a-Service. 6, 12, 14, 17, 22,

IAM Identity and Access Management. 18, 20, 21,

IDC International Data Corporation. 85,

IEC Internationale Elektrotechnische Kommission. 89–91,

IKDOK Innerer Kreis der Operativen Koordinierungsstruktur. 39,

IKT Informations- und Kommunikationstechnik. 44, 45, 47, 50, 61–69, 90,

IoT Internet of Things. 6,

IPCEI CIS Important Project of Common European Interest Next Generation Cloud Infrastructure and Services. 28,

ISMS Informationssicherheitsmanagementsystem. 89,

ISO Internationale Organisation für Normung. 89–91,

IT Informationstechnik. 1, 3, 11, 13, 23, 29, 53,

KI Künstliche Intelligenz. 18,

MAC Mandatory Access Control. 21,

MSA Microsoft Account. 107,

MTTF Mean time to failure. 12,

MTTR Mean time to repair. 12,

NISG Netz- und Informationssystemsicherheitsgesetz. 2, 26, 33, 34, 37–40, 43, 46, 55, 57, 58, 102, 149, 157,

NISG 2024 Netz- und Informationssystemsicherheitsgesetz 2024. 27, 43, 53–56, 102, 150,

NISR Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. 2, 26, 33, 40, 41, 43–45, 52, 53, 60, 67, 112,

NISR2 Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union. 2, 5, 18, 27, 31, 43–48, 50, 52, 53, 55–57, 59, 60, 62, 67, 71, 73, 82, 91, 92, 101, 102, 112, 113,

NIST National Institute of Standards and Technology. 5, 14, 22,

NISV Netz- und Informationssystemsicherheitsverordnung. 35, 39, 46, 54, 55, 150,

NSL National Security Letter. 75, 96, 97, 99, 150,

ODNI Office of the Director of National Intelligence. 96,

PaaS Platform-as-a-Service. 12, 14, 17, 22,

PAYG Pay as you go. 10,

PCI 3DS Payment Card Industry 3 Domain Secure. 89, 90,

PCI DSS Payment Card Industry Data Security Standard. 22, 89, 90,

PIR Post Incident Reviews. 93,

PSD I Richtlinie 2007/64/EG über Zahlungsdienste im Binnenmarkt. 72,

PSD II Richtlinie (EU) 2015/2366 über Zahlungsdienste im Binnenmarkt. 2, 72, 73,

PSD1 Richtlinie 2007/64/EG über Zahlungsdienste im Binnenmarkt.

Q Quartal. 86, 87, 95, 97, 98, 150,

QoS Quality of Service. 5,

QUASTE Qualifizierte Stelle. 37, 41–43,

RBAC Role Based Access Control. 21,

RISAA Reforming Intelligence and Securing America Act. 75,

SaaS Software-as-a-Service. 6, 14, 17, 52, 86,

SCA Stored Communications Act. 73,

SEC Sektion.

SLA Service Level Agreement. 6, 12, 49, 92–94, 153,

SOC System and Organization Controls. 89–91,

SPÖ Sozialdemokratische Partei Österreichs. 56,

SQL Structured Query Language. 17,

STaaS Storage-as-a-Service. 17,

STAR Security, Trust, Assurance and Risk. 89,

TLD Top-Level-Domain. 45, 47, 49,

TLPT Threat-Led Penetration Testing. 64, 66,

US Vereinigten Staaten. xvi, 1, 3, 25, 26, 28, 31, 70, 71, 74–77, 82, 85, 87, 96, 109, 112, 150,

USA Vereinigten Staaten von Amerika. 26, 31, 69, 72–77, 82, 83, 87, 95, 96, 109, 112, 150,

VM virtuelle Maschine. 92–94,

Z Ziffer.

ZaDiG 2009 Bundesgesetz über die Erbringung von Zahlungsdiensten 2009. 72,

ZaDiG 2018 Bundesgesetz über die Erbringung von Zahlungsdiensten 2018. 2, 72, 73,

ÖVP Österreichische Volkspartei. 56,

Literatur

Wissenschaftliche Quellen

Michael Adelmeyer und Frank Teuteberg. „Cloud Computing Adoption in Critical Infrastructures-Status Quo and Elements of a Research Agenda“. In: *Proceedings of the Multikonferenz Wirtschaftsinformatik 2018* (2018), S. 1345–1356.

Deepali Ahir und Nuzhat Shaikh. „A Systematic Survey on Cloud Security Threats, Impacts and Remediation“. In: *2023 IEEE Engineering Informatics*. IEEE. 2023, S. 1–9.

Axel Anderl u. a. *Netz-und Informationssystemsicherheitsgesetz (NISG): Kurzkommentar*. MANZ'sche Verlags-und Universitätsbuchhandlung, 2019.

Umer Ahmed Butt u. a. „Cloud security threats and solutions: A survey“. In: *Wireless Personal Communications* 128.1 (2023), S. 387–413.

Center for Advanced Security, Strategic and Integration Studies (CASSIS). *Vermessung der digitalen Dependenz - Digital Dependence Index*. 2024. URL: https://digitaldependence.eu/ (besucht am 05. 10. 2024).

Cornell Law School. *National Security Letter*. 2023. URL: https://www.law.cornell.edu/wex/national_security_letter#:~:text=A%20National%20Security%20Letter%20is,related%20to%20national%20security%20matters. (besucht am 15. 08. 2024).

Tharam Dillon, Chen Wu und Elizabeth Chang. „Cloud computing: issues and challenges“. In: *2010 24th IEEE international conference on advanced information networking and applications*. IEEE. 2010, S. 27–33.

Philipp Eckhardt und Anastasia Kotovskaia. „The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive“. In: *International Cybersecurity Law Review* 4.2 (2023), S. 147–164.

Donald David Stewart Ferguson. „The outcome efficacy of the entity risk management requirements of the NIS 2 Directive“. In: *International Cybersecurity Law Review* 4.4 (2023), S. 371–386.

David Freet u. a. „Cloud forensics challenges from a service model standpoint: IaaS, PaaS and SaaS“. In: *Proceedings of the 7th International Conference on Management of computational and collective intElligence in Digital EcoSystems*. 2015, S. 148–155.

Douglas Guilfoyle, Tamsin Phillipa Paige und Rob McLaughlin. „The final frontier of cyberspace: The seabed beyond national jurisdiction and the protection of submarine cables“. In: *International & Comparative Law Quarterly* 71.3 (2022), S. 657–696.

Jockum Hildén. „Mitigating the risk of US surveillance for public sector services in the cloud“. In: *Internet policy review* 10.3 (2021), S. 1–24.

Jiangshui Hong u. a. „An overview of multi-cloud computing“. In: *Web, Artificial Intelligence and Network Applications: Proceedings of the Workshops of the 33rd International Conference on Advanced Information Networking and Applications (WAINA-2019) 33*. Springer. 2019, S. 1055–1068.

Mohamed K Hussein, Mohamed H Mousa und Mohamed A Alqarni. „A placement architecture for a container as a service (CaaS) in a cloud environment“. In: *Journal of Cloud Computing* 8 (2019), S. 1–15.

I Indu, PM Rubesh Anand und Vidhyacharan Bhaskar. „Identity and access management in cloud environment: Mechanisms and challenges“. In: *Engineering science and technology, an international journal* 21.4 (2018), S. 574–588.

Kiran Jewargi. „Public Cloud to Cloud Repatriation Trend“. In: *Scholars Journal of Engineering and Technology* 11.1 (2023), S. 1–3.

Shaharyar Khan u. a. „A systematic analysis of the capital one data breach: Critical lessons learned“. In: *ACM Transactions on Privacy and Security* 26.1 (2022), S. 1–29.

Gurudatt Kulkarni, Ramesh Sutar und Jayant Gambhir. „Cloud computing-Storage as service“. In: *International Journal of Engineering Research and Applications (IJERA)* 2.1 (2012), S. 945–950.

Arjun Reddy Kunduru. „THE PERILS AND DEFENSES OF ENTERPRISE CLOUD COMPUTING: A COMPREHENSIVE REVIEW“. In: *Central Asian Journal of Mathematical Theory and Computer Sciences* 4.9 (2023), S. 29–41.

Michael Lane, Anup Shrestha und Omar Ali. „Managing the risks of data security and privacy in the cloud: a shared responsibility between the cloud service provider and the client organisation“. In: *Bright Internet Global Summit 2017* (2017).

Peter Mell und Tim Grance. *The NIST definition of cloud computing*. 2011.

Ganesh Kumar Murugesan. „Cloud Services—Boon or Bane: A Comprehensive Review“. In: *SoutheastCon 2024* (2024), S. 108–112.

Mina Nabi, Maria Toeroe und Ferhat Khendek. „Availability in the cloud: State of the art“. In: *Journal of Network and Computer Applications* 60 (2016), S. 54–67.

Marc Ohm u. a. „Backstabber's knife collection: A review of open source software supply chain attacks“. In: *Detection of Intrusions and Malware, and Vulnerability Assessment: 17th International Conference, DIMVA 2020, Lisbon, Portugal, June 24–26, 2020, Proceedings 17*. Springer. 2020, S. 23–43.

Mayar A Omar u. a. „An examination of the factors affecting the adoption of cloud enterprise resource planning systems in Egyptian companies“. In: *International Journal of Economics and Management Engineering* 16.2 (2022), S. 19–28.

Justice Opara-Martins, Reza Sahandi und Feng Tian. „Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective“. In: *Journal of Cloud Computing* 5 (2016), S. 1–18.

Antony Panteli. *Examining Poly-Cloud in Enterprise Cloud Strategies: Differentiating Between Multi-Cloud and Hybrid Cloud Approaches*. 2023.

Dana Petcu. „Multi-cloud: expectations and current approaches“. In: *Proceedings of the 2013 international workshop on Multi-cloud applications and federated clouds*. 2013, S. 1–6.

Ariana Polyviou und Nancy Pouloudi. „Understanding cloud adoption decisions in the public sector“. In: *2015 48th Hawaii International Conference on System Sciences*. IEEE. 2015, S. 2085–2094.

Michael Rath, Lutz Keller und Axel Spies. „Sovereign Clouds — An overview of the current privacy challenges associated with the use of US cloud services, and how sovereign clouds can address these challenges“. In: *Computer Law Review International* 24.3 (2023), S. 78–84.

H Sabireen und VJIE Neelanarayanan. „A review on fog computing: Architecture, fog with IoT, algorithms and research challenges“. In: *Ict Express* 7.2 (2021), S. 162–176.

Hukum Saini, Abhay Upadhyaya und Manish Kumar Khandelwal. „Benefits of cloud computing for business enterprises: A review“. In: *Proceedings of International Conference on Advancements in Computing & Management (ICACM)*. 2019, S. 1005–1006.

Rajani S Sajjan und Vijay R Ghorpade. „Ransomware attacks: Radical menace for cloud computing“. In: *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE. 2017, S. 1640–1646.

Spyridon Samonas und David Coss. „The CIA strikes back: Redefining confidentiality, integrity and availability in security.“ In: *Journal of Information System Security* 10.3 (2014).

Sirshak Sarkar u. a. „Security of Zero Trust Networks in Cloud Computing“. In: *Sustainability* 14.18 (2022), S. 11213.

Mohammad Shahrad, Jonathan Balkind und David Wentzlaff. „Architectural implications of function-as-a-service computing“. In: *Proceedings of the 52nd annual IEEE/ACM international symposium on microarchitecture*. 2019, S. 1063–1075.

Jafar Shayan u. a. „Identifying Benefits and risks associated with utilizing cloud computing“. In: *arXiv preprint arXiv:1401.5155* (2014), S. 4–6.

Ashish Singh und Kakali Chatterjee. „Cloud security issues and challenges: A survey“. In: *Journal of Network and Computer Applications* 79 (2016), S. 88–115.

Lawrence Siry. „Cloudy days ahead: Cross-border evidence collection and its impact on the rights of EU citizens“. In: *New Journal of European Criminal Law* 10.3 (2019), S. 227–250. DOI: 10.1177/2032284419865608. URL: https://doi.org/10.1177/2032284419865608.

Jayachander Surbiryala und Chunming Rong. „Cloud computing: History and overview“. In: *2019 IEEE Cloud Summit*. IEEE. 2019, S. 1–7.

Andrei Tchernykh u. a. „Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability“. In: *Journal of Computational Science* 36 (2019), S. 100581.

Maria Toeroe und Francis Tam. *Service availability: principles and practice*. John Wiley & Sons, 2012, S. 36–40.

Christian Wagner u. a. „Impact of critical infrastructure requirements on service migration guidelines to the cloud“. In: *2015 3rd International Conference on Future Internet of Things and Cloud*. IEEE. 2015, S. 1–8.

Lizhe Wang u. a. „Cloud computing: a perspective study“. In: *New generation computing* 28 (2010), S. 137–146.

Rechtliche Quellen

Verordnung (EU) 2019/881 über die ENISA und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik. 2019. URL: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32019R0881 (besucht am 01. 05. 2024).

Vertrag über die Arbeitsweise der Europäischen Union. 2009. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A12012E%2FTXT (besucht am 21. 07. 2024).

Durchführungsverordnung (EU) 2018/151 der Kommission vom 30. Januar 2018. 2018. URL: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32018R0151 (besucht am 12. 11. 2023).

Bundesgesetz über das Bankwesen (Bankwesengesetz – BWG). 2013. URL: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004827&nonce=0c61e219b5d8629e (besucht am 12. 07. 2024).

Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022. 2022. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32022L2557 (besucht am 25. 12. 2023).

CLOUD Act. 2018. URL: https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf (besucht am 13. 01. 2024).

Vorschlag für eine VERORDNUNG über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen. 2024. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52022PC0454 (besucht am 30. 03. 2024).

Ministerialentwurf Gesetz: Bundesgesetz zur Einrichtung einer nationalen Behörde für die Cybersicherheitszertifizierung (Cybersicherheitszertifizierungs-Gesetz – CSZG). 2024. URL: https://www.parlament.gv.at/dokument/XXVII/ME/330/fname_1623055.pdf (besucht am 19. 05. 2024).

Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen. 2003. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32003H0361 (besucht am 29. 12. 2023).

Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022. 2022. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj (besucht am 24. 01. 2024).

COMMISSION IMPLEMENTING DECISION of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework. 2023. URL: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf (besucht am 17. 01. 2024).

Verordnung (EU) Nr. 1024/2013 des Rates vom 15. Oktober 2013. 2013. URL: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32013R1024 (besucht am 27. 02. 2024).

Foreign Intelligence Surveillance Act of 1978. 1978. URL: https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf (besucht am 12. 08. 2024).

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008. 2008. URL: https://www.govinfo.gov/content/pkg/PLAW-110publ261/pdf/PLAW-110publ261.pdf#page=3 (besucht am 12. 08. 2024).

Durchführungsverordnung (EU) 2024/482 mit Durchführungsbestimmungen zur Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates hinsichtlich der Annahme des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC). 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R0482&qid=1707312751025 (besucht am 18. 05. 2024).

Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG). 2018. URL: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536 (besucht am 02. 11. 2023).

Begutachtungsentwurf: Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024). 2024. URL: https://www.ris.bka.gv.at/Dokumente/Begut/BEGUT_42FD65C8_76B7_40F0_97E3_BB29BDFC0CE9/BEGUT_42FD65C8_76B7_40F0_97E3_BB29BDFC0CE9.pdf (besucht am 29. 04. 2024).

Anlage 3 - Begutachtungsentwurf: Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024). 2024. URL: https://www.parlament.gv.at/dokument/XXVII/ME/326/fname_1621122.pdf (besucht am 29. 04. 2024).

Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016. 2016. URL: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32016L1148 (besucht am 02. 11. 2023).

Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022. 2022. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32022L2555 (besucht am 02. 11. 2023).

DRAFT - COMMISSION IMPLEMENTING REGULATION (EU) laying down rules for the application of Directive (EU) 2022/2555. 2024. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=PI_COM%3AAres%282024%294640447 (besucht am 07. 09. 2024).

Netz- und Informationssystemsicherheitsverordnung. 2019. URL: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010722 (besucht am 06. 04. 2024).

Reforming Intelligence and Securing America Act. 2024. URL: https://www.congress.gov/bill/118th-congress/house-bill/7888/text (besucht am 12. 08. 2024).

18 USC Ch. 121: Stored Wire and Electronic Communications and Transactional Records Access. 1986. URL: https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title18-chapter121&saved=%7CKHRpdGxlOjE4IHNlY3Rpb246MjcwMSBlZGl0aW9uOnByZWxpbSkgT1IgKGdyYW51bGVpZDpVU0MtcHJlbGltLXRpdGxlMTgtc2VjdGlvbjI3MDEp%7CdHJlZXNvcnQ%3D%7C%7C0%7Cfalse%7Cprelim&edition=prelim (besucht am 14. 01. 2024).

Rechtssache C-311/18. 2020. URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=3820159 (besucht am 19. 01. 2024).

Delegierte Verordnung (EU) 2024/1772 der Kommission. 2024. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401772 (besucht am 12. 07. 2024).

Delegierte Verordnung (EU) 2024/1773 der Kommission. 2024. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401773 (besucht am 12. 07. 2024).

Delegierte Verordnung (EU) 2024/1774 der Kommission. 2024. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401774 (besucht am 12. 07. 2024).

Bundesgesetz über die Erbringung von Zahlungsdiensten 2018 (Zahlungsdienstegesetz 2018 – ZaDiG 2018). 2018. URL: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010182 (besucht am 13. 03. 2025).

Sonstige Quellen

9to5mac. *LastPass says engineer's hacked computer led to security breach*. 2023. URL: https://9to5mac.com/2023/02/27/lastpass-devops-engineers-hacked/ (besucht am 01. 06. 2024).

Adesso. *Schrems II ad acta? Das neue Data Privacy Framework und seine Auswirkungen*. 2023. URL: https://www.adesso.de/de/news/blog/schrems-ii-ad-acta-das-neue-data-privacy-framework-und-seine-auswirkungen.jsp (besucht am 06. 06. 2024).

AICPA & CIMA. *System and Organization Controls: SOC Suite of Services*. 2024. URL: https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services (besucht am 08. 07. 2024).

Alphabet. *GOOG Exhibit 99.1 Q1 2024*. 2024. URL: https://abc.xyz/assets/91/b3/3f9213d14ce3ae27e1038e01a0e0/2024q1-alphabet-earnings-release-pdf.pdf (besucht am 11. 07. 2024).

Amazon. *Amazon Compute Service Level Agreement*. 2024. URL: https://aws.amazon.com/compute/sla/ (besucht am 27. 07. 2024).

Amazon. *Amazon Information Request Report H1*. 2022. URL: https://d1.awsstatic.com/certifications/Information_Request_Report_H1_2022.pdf (besucht am 28. 07. 2024).

Amazon. *Amazon Information Request Report H2*. 2022. URL: https://d1.awsstatic.com/Security/pdfs/Amazon_Information_Request_Report.pdf (besucht am 28. 07. 2024).

Amazon. *AWS Customer Agreement*. 2024. URL: https://aws.amazon.com/agreement/?nc1=h_ls (besucht am 27. 07. 2024).

Amazon. *AWS plans to invest €7.8B into the AWS European Sovereign Cloud*. 2024. URL: https://aws.amazon.com/de/blogs/security/aws-plans-to-invest-e7-8b-into-the-aws-european-sovereign-cloud-set-to-launch-by-the-end-of-2025/#German (besucht am 16. 08. 2024).

Amazon. *AWS responds to European Supervisory Authorities' second consultation on technical standards under the Digital Operational Resilience Act (DORA) | AWS for Industries*. 2024. URL: https://aws.amazon.com/de/blogs/industries/aws-responds-to-european-supervisory-authorities-second-consultation-on-technical-standards-under-the-digital-operational-resilience-act-dora/ (besucht am 10. 07. 2024).

Amazon. *Dedicated Local Zones FAQs Page*. 2024. URL: https://aws.amazon.com/de/dedicatedlocalzones/faqs/ (besucht am 16. 08. 2024).

Amazon. *NIS2 Considerations for Customers*. 2023. URL: https://d1.awsstatic.com/whitepapers/compliance/NIS_2_Considerations_for_AWS_Customers.pdf (besucht am 11. 07. 2024).

Amazon Web Services (AWS). *Compliance-Programme*. 2024. URL: https://aws.amazon.com/de/compliance/programs/ (besucht am 16. 06. 2024).

Amazon.com, Inc. *Amazon.com Announces First Quarter Results*. 2024. URL: https://ir.aboutamazon.com/news-release/news-release-details/2024/Amazon.com-Announces-First-Quarter-Results-68b9258cd/default.aspx (besucht am 11. 07. 2024).

Austrian Standards. *Compliance: Definitionen, Begriffe, Standards und Richtlinien — austrian-standards.at*. 2023. URL: https://www.austrian-standards.at/de/themengebiete/management-qualitaet-risiko/compliance (besucht am 18. 11. 2023).

BaFin. *DORA*. 2024. URL: https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html (besucht am 12. 07. 2024).

Bleepingcomputer. *Retool blames breach on Google Authenticator MFA cloud sync feature*. 2023. URL: https://www.bleepingcomputer.com/news/security/retool-blames-breach-on-google-authenticator-mfa-cloud-sync-feature/ (besucht am 01. 06. 2024).

Bleepingcomputer. *Sumo Logic discloses security breach, advises API key resets*. 2023. URL: https://www.bleepingcomputer.com/news/security/sumo-logic-discloses-security-breach-advises-api-key-resets/ (besucht am 01. 06. 2024).

Bleepingcomputer. *U.S. No Fly list shared on a hacking forum, government investigating*. 2023. URL: https://www.bleepingcomputer.com/news/security/us-no-fly-list-shared-on-a-hacking-forum-government-investigating/ (besucht am 01. 06. 2024).

Bloomberg. *DNA Test Service Exposed Thousands of Client Records Online*. 2019. URL: https://www.bloomberg.com/news/articles/2019-07-09/dna-testing-service-exposed-thousands-of-customer-records-online?utm_source=website&utm_medium=share&utm_campaign=copy&embedded-checkout=true (besucht am 01. 06. 2024).

Bloomberg. *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*. 2018. URL: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies?embedded-checkout=true (besucht am 01. 06. 2024).

Broadcom. *The Future of the Enterprise is Private*. 2024. URL: https://www.broadcom.com/blog/the-future-of-the-enterprise-is-private (besucht am 12. 10. 2024).

BSI. *Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)*. 2024. URL: https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/DoS-Denial-of-Service/dos-denial-of-service_node.html (besucht am 18. 10. 2024).

Bundeskriminalamt. *CEO Fraud*. 2024. URL: https://www.bundeskriminalamt.at/202/Betrug_verhindern/files/CEO_fraud_AT_2_20201001.pdf (besucht am 27. 05. 2024).

Bundesministerium für Arbeit und Wirtschaft. *OE-Cloud Initiative*. 2021. URL: https://www.bmaw.gv.at/Presse/Archiv/Pressemeldungen-BMDW/2021/Juli-2021/%C3%96-Cloud-Initiative.html (besucht am 05. 10. 2024).

Bundesministerium für Wirtschaft und Energie (BMWi). *Das Projekt GAIA-X – Eine vernetzte Dateninfrastruktur als Wiege eines vitalen, europäischen Ökosystems*. 2019. URL: https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/das-projekt-gaia-x.pdf?__blob=publicationFile&v=22 (besucht am 05. 10. 2024).

CADO. *Why is CIRA (Gartner) all the Hype for Cloud Incident Response?* 2023. URL: https://www.cadosecurity.com/blog/why-is-cira-all-the-hype-for-cloud-incident-response (besucht am 06. 06. 2024).

Check Point Software Technologies Ltd. *Cloud Security Report*. 2023. URL: https://pages.checkpoint.com/2023-cloud-security-report.html (besucht am 30. 05. 2024).

CIS. *CIS Benchmarks*. 2024. URL: https://www.cisecurity.org/cis-benchmarks (besucht am 10. 07. 2024).

Cloud Security Alliance. *Current Corporate Members*. 2024. URL: https://cloudsecurityalliance.org/membership/current (besucht am 17. 08. 2024).

Cloud Security Alliance. *STAR | CSA*. 2024. URL: https://cloudsecurityalliance.org/star (besucht am 23. 06. 2024).

Cloud Security Alliance. *Top Threats to Cloud Computing 2024*. 2024. URL: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024 (besucht am 17. 08. 2024).

LIBE Committee letters to the EDPS and to the EDPB regarding legal assessment of the impact of the US Cloud Act on the European legal framework for personal data protection. 2019. URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_joint_response_us_cloudact_coverletter.pdf (besucht am 15. 01. 2024).

CRN. *Microsoft's 'Inadequate' Security Behind Cloud Email Breach: U.S. Review Board*. 2024. URL: https://www.crn.com/news/security/2024/microsoft-s-inadequate-security-behind-cloud-email-breach-us-review-board (besucht am 01. 06. 2024).

Europäische Kommission. *Gestaltung der digitalen Zukunft Europas*. 2024. URL: https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-policies (besucht am 20. 05. 2024).

Cybersecurity and Infrastructure Security Agency (CISA). *Review of the Summer 2023 Microsoft Exchange Online Intrusion*. 2024. URL: https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf (besucht am 01. 06. 2024).

Darkreading. *Cloud Misconfig Exposes 3TB of Sensitive Airport Data in Amazon S3 Bucket*. 2022. URL: https://www.darkreading.com/application-security/cloud-misconfig-exposes-3tb-sensitive-airport-data-amazon-s3-bucket (besucht am 01. 06. 2024).

Darkreading. *Google Cloud Bug Allows Server Takeover From CloudSQL Service*. 2023. URL: https://www.darkreading.com/cloud-security/google-cloud-bug-server-takeover-cloudsql-service (besucht am 01. 06. 2024).

Darkreading. *Uber Breached, Again, After Attackers Compromise Third-Party Cloud*. 2022. URL: https://www.darkreading.com/cyberattacks-data-breaches/uber-breached-again-attackers-compromise-third-party-cloud (besucht am 01. 06. 2024).

Datadog Security Labs. *Amplified exposure: How AWS flaws made Amplify IAM roles vulnerable to takeover*. 20224. URL: https://securitylabs.datadoghq.com/articles/amplified-exposure-how-aws-flaws-made-amplify-iam-roles-vulnerable-to-takeover/ (besucht am 01. 06. 2024).

Der Standard. *Cyberangriff auf steirische IT-Firma*. 2024. URL: https://www.derstandard.at/story/3000000211558/cyberangriff-auf-steirische-it-firma (besucht am 07. 04. 2024).

Der Standard. *Cyberangriff auf steirische IT-Firma*. 2024. URL: https://www.derstandard.de/story/3000000211558/cyberangriff-auf-steirische-it-firma (besucht am 07. 04. 2024).

Der Standard. *Cyberattacke: Offenbar Produktionsausfall bei BRP-Rotax in Oberösterreich*. 2022. URL: https://www.derstandard.de/story/2000138241706/cyberattacke-offenbar-produktionsausfall-bei-brp-rotax-in-oberoesterreich (besucht am 07. 04. 2024).

Der Standard. *Globaler Cyberangriff auf Palfinger*. 2021. URL: https://www.derstandard.at/story/2000123591737/globaler-cyber-angriff-auf-palfinger (besucht am 07. 04. 2024).

Der Standard. *Jö-Bonusclub: Betrüger hatten Zugriff auf 18.000 Konten*. 2022. URL: https://www.derstandard.at/story/2000140466657/joe-bonusclub-betrueger-hatten-zugriff-auf-18-000-konten (besucht am 07. 04. 2024).

Der Standard. *Kärntner Landesversicherung wurde Opfer von Cyberangriff*. 2024. URL: https://www.derstandard.de/story/3000000211124/kaerntner-landesversicherung-wurde-opfer-von-cyberangriff (besucht am 07. 04. 2024).

Der Standard. *Labor Burgenland wurde Opfer eines Cyberangriffs*. 2023. URL: https://www.derstandard.at/story/3000000173935/labor-burgenland-wurde-opfer-eines-cyber-angriffs (besucht am 07. 04. 2024).

Developing Certification Schemes - European Union. 2024. URL: https://certification.enisa.europa.eu/about-eu-certification/developing-certification-schemes_en (besucht am 20. 05. 2024).

Content Directorate-General for Communications Networks und Technology. *Cyber Resilience Act*. 2025. URL: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act (besucht am 05. 03. 2025).

EBA. *EBA BS 2019 Guidelines on outsourcing arrangements*. 2019. URL: https://www.eba.europa.eu/sites/default/files/documents/10180/2761380/5546a705-bff2-43eb-b382-e5c7bed3a2bc/EBA%20revised%20Guidelines%20on%20outsourcing_DE.pdf (besucht am 14. 07. 2024).

ECUC Group. *ECUC Group – European Cloud User Coalition*. 2024. URL: https://ecuc.group/ (besucht am 08. 07. 2024).

ESMA. *ESAs publish first set of rules under DORA for ICT and third-party risk management and incident classification*. 2024. URL: https://www.esma.europa.eu/press-news/esma-news/esas-publish-first-set-rules-under-dora-ict-and-third-party-risk-management (besucht am 12. 07. 2024).

EU Cloud CoC. *EU Cloud CoC*. 2024. URL: https://eucoc.cloud/en/about/about-eu-cloud-coc (besucht am 08. 07. 2024).

EUCS – Cloud Services Scheme. 2020. URL: https://www.enisa.europa.eu/sites/default/files/publications/EUCS%20%E2%80%93%20Cloud%20Service%20candidate%20cybersecurity%20certification%20scheme.pdf (besucht am 01. 03. 2025).

European Commission. *Common European Interest in computing technologies*. 2023. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6246 (besucht am 16. 08. 2024).

European Commission. *SEcure Cloud computing for CRitical infrastructure IT*. 2017. URL: https://cordis.europa.eu/project/id/312758/ (besucht am 25. 02. 2023).

Federal Bureau of Investigation. *NSL-21-538695-request-redacted.pdf*. 2021. URL: https://storage.googleapis.com/transparencyreport/legal/NSLs/21-538695/NSL-21-538695-request-redacted.pdf (besucht am 17. 08. 2024).

Fondsprofessionell. *FMA von Hacker-Angriff betroffen | Recht | 06.06.2023 | FONDS professionell*. 2023. URL: https://www.fondsprofessionell.at/news/recht/headline/fma-von-hacker-angriff-betroffen-224962/ (besucht am 07. 04. 2024).

Forbes. *Cloud Storage Error Exposes Over Two Million Dow Jones Customer Records*. 2017. URL: https://www.forbes.com/sites/lconstantin/2017/07/17/cloud-storage-error-exposes-over-two-million-dow-jones-customer-records/ (besucht am 01. 06. 2024).

Futurezone. *Cyberangriff beschäftigt Wasserzähler-Hersteller Ista noch immer*. 2022. URL: https://futurezone.at/digital-life/ista-wasserzaehler-stromzaehler-cyberangriff-offline-kundendaten/402118833 (besucht am 07. 04. 2024).

Futurezone. *DDoS-Attacke: Webseite der ÖBB und Ticketverkauf gestört*. 2022. URL: https://futurezone.at/digital-life/oebb-oebb-website-down-stoerung-hacker-ddos/402261678 (besucht am 07. 04. 2024).

Gartner. *Definition of Cloud Security Posture Management*. 2022. URL: https://www.gartner.com/en/information-technology/glossary/cloud-security-posture-management (besucht am 06. 06. 2024).

Gartner. *Emerging Tech: Security — Cloud Investigation and Response Automation Offers Transformation Opportunities*. 2023. URL: https://www.gartner.com/en/documents/4424199 (besucht am 06. 06. 2024).

Google. *Auskunftsersuchen zu Nutzerdaten – Google Transparenzbericht*. 2022. URL: https://transparencyreport.google.com/user-data/overview (besucht am 28. 07. 2024).

Google. *Auskunftsersuchen zu Nutzerdaten – Google Transparenzbericht*. 2022. URL: https://transparencyreport.google.com/user-data/us-national-security (besucht am 10. 08. 2024).

Google. *BWG (Österreich) – Compliance*. 2024. URL: https://cloud.google.com/security/compliance/austrian-fma-bwg?hl=de (besucht am 08. 07. 2024).

Google. *BWG (Österreich) – Compliance*. 2024. URL: https://cloud.google.com/security/compliance/austrian-fma-bwg?hl=de (besucht am 11. 07. 2024).

Google. *Cloud Compliance – Vorschriften und Zertifizierungen*. 2024. URL: https://cloud.google.com/security/compliance/offerings?hl=de (besucht am 16. 06. 2024).

Google. *Compute Engine Service Level Agreement (SLA)*. 2024. URL: https://cloud.google.com/compute/sla (besucht am 27. 07. 2024).

Google. *ESMA (EU)*. 2024. URL: https://cloud.google.com/security/compliance/esma-eu?hl=de (besucht am 08. 07. 2024).

Google. *EU DORA – Compliance*. 2024. URL: https://cloud.google.com/security/compliance/dora?hl=de (besucht am 10. 07. 2024).

Google. *Google Cloud Service Health*. 2024. URL: https://status.cloud.google.com/summary (besucht am 28. 07. 2024).

Google. *How Google Cloud is preparing for NIS2 and supporting a stronger European cyber ecosystem*. 2023. URL: https://cloud.google.com/blog/products/identity-security/how-google-cloud-is-preparing-for-nis2-and-protecting-europe-from-cyber-threats?hl=en (besucht am 11. 07. 2024).

Google. *PCI 3DS – Compliance*. 2024. URL: https://cloud.google.com/security/compliance/pci-3ds?hl=de (besucht am 10. 07. 2024).

Handelsblatt. *A1 Telekom Austria wird Opfer von massivem Hackerangriff*. 2020. URL: https://www.handelsblatt.com/technik/it-internet/cybersicherheit-a1-telekom-austria-wird-opfer-von-massivem-hackerangriff/25904556.html (besucht am 07. 04. 2024).

Heise. *Hacker veröffentlichen Daten nach Cyberangriff auf städtische IT in Österreich | heise online*. 2020. URL: https://www.heise.de/news/Hacker-veroeffentlichen-Daten-nach-Cyberangriff-auf-staedtische-IT-in-Oesterreich-4727538.html (besucht am 15. 01. 2024).

IDC. *IDC Says European Public Cloud Spending Will Reach $142 Billion This Year, Defying Budget Cuts Amid an Economic Downturn*. 2023. URL: https://www.idc.com/getdoc.jsp?containerId=prEUR151144823 (besucht am 11. 07. 2024).

IKT-Sicherheitsportal. *Informationssicherheits-Managementsystem (ISMS)*. 2017. URL: https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Sicherheitsmanagement/Informationssicherheits-Managementsystem.html (besucht am 10. 07. 2024).

IKT-Sicherheitsportal. *Payment Card Industry Data Security Standard*. 2022. URL: https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards/PCI-DSS.html (besucht am 10. 07. 2024).

Interpol. *Cryptojacking*. 2020. URL: https://www.interpol.int/Crimes/Cybercrime/Cryptojacking (besucht am 01. 06. 2024).

IONOS. *Fog-Computing – Dezentraler Ansatz für IOT-Clouds*. 2019. URL: https://www.ionos.de/digitalguide/server/knowhow/fog-computing-definition-und-erklaerung/ (besucht am 07. 10. 2023).

ISO. *ISO/IEC 27001:2022 - Information security management systems*. 2022. URL: https://www.iso.org/standard/27001 (besucht am 23. 06. 2024).

ISO. *ISO/IEC 27017:2015 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. 2015. URL: https://www.iso.org/standard/43757.html (besucht am 23. 06. 2024).

ISO. *ISO/IEC 27018:2019 - Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*. 2019. URL: https://www.iso.org/standard/76559.html (besucht am 23. 06. 2024).

iTnews. *Millions of Verizon customer details exposed on misconfigured Amazon S3 server*. 2017. URL: https://www.itnews.com.au/news/millions-of-verizon-customer-details-exposed-on-misconfigured-amazon-s3-server-468246 (besucht am 01. 06. 2024).

Mark Jackley. *Data Sovereignty vs. Data Residency: 3 Key Differences*. 2024. URL: https://www.oracle.com/it/security/saas-security/data-sovereignty/data-sovereignty-data-residency/ (besucht am 07. 03. 2025).

Kleine Zeitung. *Anexia: Größter Cyberangriff Österreichs auf Kärntner Firma*. 2018. URL: https://www.kleinezeitung.at/wirtschaft/5382678/Anexia_Groesster-Cyberangriff-Oesterreichs-auf-Kaerntner-Firma (besucht am 07. 04. 2024).

Kleine Zeitung. *Bereits Anfang März: Brucker Stadtwerke wurden Opfer eines Hackerangriffs*. 2024. URL: https://www.kleinezeitung.at/steiermark/muerztal/18314503/brucker-stadtwerke-wurden-opfer-eines-hackerangriffs (besucht am 07. 04. 2024).

Kleine Zeitung. *Bestätigung im Netz: Anton Paar ist Opfer einer Cyber-Attacke geworden*. 2023. URL: https://www.kleinezeitung.at/steiermark/graz/6278296/Bestaetigung-im-Netz_Anton-Paar-ist-Opfer-einer-CyberAttacke-geworden (besucht am 07. 04. 2024).

Kleine Zeitung. *Neuer Blümel-Arbeitgeber: Kundengelder nicht betroffen: Cyberattacke auf Superfund-Gruppe*. 2022. URL: https://www.kleinezeitung.at/wirtschaft/6086840/Neuer-BluemelArbeitgeber_Kundengelder-nicht-betroffen_ (besucht am 07. 04. 2024).

Kleine Zeitung. *Straftaten im Netz steigen: Hackerangriff auf Papierfabrik Brigl & Bergmeister in Niklasdorf*. 2022. URL: https://www.kleinezeitung.at/steiermark/leoben/6121843/Straftaten-im-Netz-steigen_Hackerangriff-auf-Papierfabrik-in (besucht am 07. 04. 2024).

Krone. *An Kundendaten gelangt - Hackerangriff auf „Wien-Süd“: 50.000 Betroffene | krone.at*. 2023. URL: https://www.krone.at/2754870 (besucht am 07. 04. 2024).

Kurier. *20.000 Kundendaten von Hackerangriff auf Magenta-Partner betroffen*. 2023. URL: https://kurier.at/wirtschaft/20000-kundendaten-von-hackerangriff-auf-magenta-partner-betroffen/402313508 (besucht am 07. 04. 2024).

Kurier. *Cyberangriff auf Außenministerium läuft noch immer*. 2020. URL: https://kurier.at/politik/inland/cyberangriff-auf-aussenministerium-laeuft-noch-immer/400718463 (besucht am 07. 04. 2024).

Kurier. *Hacker versuchten Cyber-Attacke auf Uni Graz*. 2023. URL: https://kurier.at/chronik/oesterreich/hacker-versuchten-cyber-attacke-auf-uni-graz/402318302 (besucht am 07. 04. 2024).

Kurier. *Hackerangriff auf Dienstleister: Datenleck auch bei der Bank99*. 2023. URL: https://kurier.at/wirtschaft/hackerangriff-auf-dienstleister-datenleck-auch-bei-der-bank99/402526051 (besucht am 07. 04. 2024).

Kurier. *Stadtgemeinde Feldbach von Hackerangriff betroffen*. 2022. URL: https://kurier.at/chronik/oesterreich/stadtgemeinde-feldbach-von-hackerangriff-betroffen/402136620 (besucht am 07. 04. 2024).

Lockheed Martin. *Cyber Kill Chain*. 2024. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (besucht am 12. 10. 2024).

Mein Bezirk. *Hacker-Angriff sorgt für massive Probleme: Längere Wartezeiten im Kassenbereich bei Großhändler Metro - Hall-Rum*. 2022. URL: https://www.meinbezirk.at/hall-rum/c-wirtschaft/laengere-wartezeiten-im-kassenbereich-bei-grosshaendler-metro_a5731771 (besucht am 07. 04. 2024).

Microsoft. *Analysis of Storm-0558 techniques for unauthorized email access*. 2023. URL: https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/ (besucht am 01. 06. 2024).

Microsoft. *Azure status history*. 2024. URL: https://azure.status.microsoft/en-gb/status/history/ (besucht am 28. 07. 2024).

Microsoft. *Cross-region replication in Azure*. 2023. URL: https://learn.microsoft.com/en-us/azure/reliability/cross-region-replication-azure (besucht am 23. 09. 2023).

Microsoft. *Dokumentation zur Azure-Compliance*. 2024. URL: https://learn.microsoft.com/de-de/azure/compliance/ (besucht am 16. 06. 2024).

Microsoft. *Europäische Bankenaufsichtsbehörde (EBA) - Microsoft Compliance*. 2024. URL: https://learn.microsoft.com/de-de/compliance/regulatory/offering-eba-eu (besucht am 08. 07. 2024).

Microsoft. *Get started guide for Azure IT operators — learn.microsoft.com*. 2022. URL: https://learn.microsoft.com/en-us/azure/guides/operations/azure-operations-guide (besucht am 16. 09. 2023).

Microsoft. *Law Enforcement Request Report*. 2022. URL: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report (besucht am 28. 07. 2024).

Microsoft. *Microsoft Financial Data - FY24Q1*. 2024. URL: https://view.officeapps.live.com/op/view.aspx?src=https://c.s-microsoft.com/en-us/CMSFiles/FinancialStatementFY24Q1.xlsx?version=211598b9-ca27-24b9-5e08-63704dc91054 (besucht am 11. 07. 2024).

Microsoft. *Office 365 GCC - Service Descriptions — learn.microsoft.com*. 2023. URL: https://learn.microsoft.com/de-de/office365/servicedescriptions/office-365-platform-service-description/office-365-us-government/gcc (besucht am 04. 09. 2024).

Microsoft. *Results of Major Technical Investigations for Storm-0558 Key Acquisition*. 2023. URL: https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/ (besucht am 02. 06. 2024).

Microsoft. *Service Level Agreement for Microsoft Online Services*. 2024. URL: https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services?lang=1 (besucht am 21. 07. 2024).

Microsoft. *US National Security Orders Reports | Microsoft CSR*. 2022. URL: https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report?activetab=pivot_1%3aprimaryr2#tabs1-2 (besucht am 28. 07. 2024).

Microsoft Azure. *Was ist Middleware – Definition und Beispiele*. 2024. URL: https://azure.microsoft.com/de-de/resources/cloud-computing-dictionary/what-is-middleware#:~:text=Im%20Prinzip%20fungiert%20Middleware%20als,%22Pipe%22%20weitergegeben%20werden%20k%C3%B6nnen. (besucht am 18. 10. 2024).

Nachrichten.at. *Wie der FACC 50 Millionen abhanden kamen | Nachrichten.at*. 2016. URL: https://www.nachrichten.at/wirtschaft/wirtschaftsraumooe/Wieder-FACC-50-Millionen-abhanden-kamen;art467,2109585 (besucht am 07. 04. 2024).

NetSPI. *Azure Site Recovery Services: Elevating Privileges*. 2024. URL: https://www.netspi.com/blog/technical-blog/cloud-penetration-testing/elevating-privileges-with-azure-site-recovery-services/ (besucht am 01. 06. 2024).

Netwrix. *Cloud Data Security Report*. 2022. URL: https://www.netwrix.com/2022_cloud_data_security_report.html (besucht am 30. 05. 2024).

New Jersey Office of Homeland Security and Preparedness. *2024 Threat Assessment*. 2024. URL: https://www.njohsp.gov/home/showpublisheddocument/728/638447013225300000 (besucht am 18. 09. 2024).

NIS Fact Sheet 9/2022. 2022. URL: https://www.nis.gv.at/dam/jcr:bbe1c393-ba27-43b3-8d38-890610cfcc75/NIS_Factsheet_9_2022_1_0.pdf (besucht am 18. 11. 2023).

Umsetzungsleitfaden für Einrichtungen des Bundes. 2019. URL: https://www.nis.gv.at/dam/jcr:188f0654-393f-4bfd-96db-33f8577182dc/NIS_Fact_Sheet_2019_09_1_0.pdf (besucht am 09. 12. 2023).

Rechtliches und Dokumente — nis.gv.at. 2023. URL: https://www.nis.gv.at/rechtliches-und-dokumente.html (besucht am 18. 11. 2023).

NOYB. *23 years of illegal data transfers due to inactive DPAs and new EU-US deals*. URL: https://noyb.eu/en/23-years-illegal-data-transfers-due-inactive-dpas-and-new-eu-us-deals (besucht am 20. 01. 2024).

OE24. *Massiver Hacker-Angriff auf Stadt Wien - oe24.at*. 2019. URL: https://www.oe24.at/oesterreich/chronik/wien/massiver-hacker-angriff-auf-stadt-wien/379389876 (besucht am 07. 04. 2024).

Office of the Director of National Intelligence. *Annual Statistical Transparency Report*. 2022. URL: https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf (besucht am 10. 08. 2024).

Capital One. *2019 Capital One Cyber Incident*. 2019. URL: https://www.capitalone.com/digital/facts2019/ (besucht am 02. 06. 2024).

Oracle. *Oracle sovereign cloud solutions: Providing transparent review of data access requests*. 2023. URL: https://blogs.oracle.com/cloud-infrastructure/post/oracle-sovereign-cloud-solutions-data-access (besucht am 16. 08. 2024).

ORF. *IMA Schelling Opfer eines Hackerangriffs - vorarlberg.ORF.at*. 2022. URL: https://vorarlberg.orf.at/stories/3153454/ (besucht am 07. 04. 2024).

ORF. *ISTA: Hackergruppe verlangte Lösegeld - noe.ORF.at*. 2023. URL: https://noe.orf.at/stories/3194765/ (besucht am 07. 04. 2024).

ORF. *Rosenbauer spricht über Cyberangriff - ooe.ORF.at*. 2023. URL: https://ooe.orf.at/stories/3200075/ (besucht am 07. 04. 2024).

ORF. *Uni Innsbruck wurde Opfer von Hackern - tirol.ORF.at*. 2023. URL: https://tirol.orf.at/stories/3238064/ (besucht am 07. 04. 2024).

ORF. *Uni Salzburg: Hackerangriff legt E-Mail-Server lahm - salzburg.ORF.at*. 2023. URL: https://salzburg.orf.at/stories/3149476/ (besucht am 07. 04. 2024).

Liste der "Betreiber wesentlicher Dienste"gem § 16 Abs 4 Z 3 NIS-Gesetz | Parlament Österreich. 2020. URL: https://www.parlament.gv.at/gegenstand/XXVII/AB/799 (besucht am 06. 11. 2023).

Parlament Österreich. *Informationen über den Nationalrat*. 2024. URL: https://www.parlament.gv.at/verstehen/nationalrat/ (besucht am 21. 07. 2024).

Parlament Österreich. *Nationalrat: Absage für Informationssystemsicherheitsgesetz (PK0785/04.07.2024)*. 2024. URL: https://www.parlament.gv.at/aktuelles/pk/jahr_2024/pk0785#XXVII_NRSITZ_00270 (besucht am 21. 07. 2024).

Profil. *Wie Hacker SalzburgMilch lahmlegten*. 2021. URL: https://www.profil.at/gesellschaft/you-are-fucked-wie-hacker-salzburgmilch-lahmlegten/401471785 (besucht am 07. 04. 2024).

Rechnungshof Österreich. *Koordination der Cyber–Sicherheit*. 2022. URL: https://www.rechnungshof.gv.at/rh/home/home/2022-13_Koordination_Cyber-Sicherheit.pdf (besucht am 13. 03. 2025).

Reuters. *Suspected Russian hackers spied on U.S. Treasury emails*. 2020. URL: https://www.reuters.com/article/us-usa-cyber-amazon-com-exclsuive-idUSKBN28N0PG/ (besucht am 01. 06. 2024).

RIS - NISG 2024 - Begutachtungsentwürfe. 2024. URL: https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=7599a912-d8df-4fb6-a2ed-8da09cb27783&Position=1&SkipToDocumentPage=True&Abfrage=Begut&Einbringer=&Titel=&DatumBegutachtungsfrist=29.04.2024&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ImRisSeitChangeSet=Undefined&ImRisSeitForRemotion=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=BEGUT_42FD65C8_76B7_40F0_97E3_BB29BDFC0CE9 (besucht am 29. 04. 2024).

Salesforce. *Salesforce Compliance*. 2024. URL: https://compliance.salesforce.com/en (besucht am 11. 07. 2024).

Salesforce. *UPDATED: DORA FAQ (March 2023)*. 2023. URL: https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/dora-external-faq.pdf (besucht am 11. 07. 2024).

Security Insider. *Was ist AI-as-a-Service (AIaaS)?* 2023. URL: https://www.security-insider.de/was-ist-ai-as-a-service-aiaas-a-be1a69c4eccd5a54ec4c4b1ec092395a/ (besucht am 11. 06. 2024).

Security Magazine. *US municipalities suffer data breach due to misconfigured Amazon S3 buckets*. 2021. URL: https://www.securitymagazine.com/articles/95704-us-municipalities-suffer-data-breach-due-to-misconfigured-amazon-s3-buckets (besucht am 01. 06. 2024).

Security News. *Data on 123 Million US Households Exposed Due to Misconfigured AWS S3 Bucket*. 2017. URL: https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/data-on-123-million-us-households-exposed-due-to-misconfigured-aws-s3-bucket (besucht am 01. 06. 2024).

Spiceworks. *Misconfigured Azure Blob Storage Exposed the Data of 65K Companies and 548K Users*. 2022. URL: https://www.spiceworks.com/it-security/cloud-security/news/microsoft-azure-cloud-misconfiguration/ (besucht am 01. 06. 2024).

Spiceworks. *Pharma Giant Pfizer Suffers Patient Data Leak Due to Cloud Misconfiguration*. 2020. URL: https://www.spiceworks.com/it-security/cloud-security/news/pharma-giant-pfizer-suffers-patient-data-leak-due-to-cloud-misconfiguration/ (besucht am 01. 06. 2024).

Statista. *Global cloud infrastructure market share 2024*. 2024. URL: https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/ (besucht am 30. 05. 2024).

Statista. *Global cloud software market vendor share 2022*. 2022. URL: https://www.statista.com/statistics/540525/worldwide-cloud-saas-revenue-share-by-vendor/ (besucht am 11. 07. 2024).

Statista. *Österreich: Umsatz im Markt für Public Cloud 2029*. 2024. URL: https://de.statista.com/prognosen/968191/prognose-zum-umsatz-mit-cloud-services-in-oesterreich (besucht am 11. 07. 2024).

Statista. *Public Cloud - Europe | Statista Market Forecast*. 2024. URL: https://www.statista.com/outlook/tmo/public-cloud/europe#revenue (besucht am 11. 07. 2024).

Statista. *Public cloud services end-user spending worldwide from 2017 to 2025*. 2025. URL: https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/ (besucht am 12. 03. 2025).

Statista. *Umsatz Branchen Österreich 2022*. 2024. URL: https://de.statista.com/statistik/daten/studie/319461/umfrage/umsatz-ausgewaehlter-industriezweige-des-verarbeitenden-gewerbes-in-oesterreich/ (besucht am 27. 05. 2024).

Statistisches Amt der Europäischen Union. *Cloud computing - statistics on the use by enterprises*. 2023. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises#Cloud_computing_as_a_service_model_for_meeting_enterprises.E2.80.99_ICT_needs (besucht am 15. 06. 2024).

Statistisches Amt der Europäischen Union. *Enterprises buying cloud computing services by size class, EU, 2021 and 2023*. 2023. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Enterprises_buying_cloud_computing_services_by_size_class,_EU,_2021_and_2023_(%25_of_enterprises).png (besucht am 15. 06. 2024).

Statistisches Amt der Europäischen Union. *Enterprises buying cloud computing services by type of cloud service, EU, 2021 and 2023*. 2023. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Enterprises_buying_cloud_computing_services_by_type_of_cloud_service,_EU,_2021_and_2023_(%25_of_enterprises_buying_cloud_services).png (besucht am 15. 06. 2024).

Statistisches Amt der Europäischen Union. *Types of cloud computing services purchased by service model and size class, EU, 2023*. 2023. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Types_of_cloud_computing_services_purchased_by_service_model_and_size_class,_EU,_2023_(%25_of_enterprises_buying_cloud_services).png (besucht am 15. 06. 2024).

Synergy Research Group. *Cloud is a Global Market - Apart from China*. 2024. URL: https://www.srgresearch.com/articles/cloud-is-a-global-market-apart-from-china (besucht am 12. 10. 2024).

Synergy Research Group. *European Cloud Providers Continue to Grow but Still Lose Market Share*. 2022. URL: https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share (besucht am 05. 10. 2024).

TechCrunch. *Microsoft employees exposed internal passwords in security lapse*. 2024. URL: https://techcrunch.com/2024/04/09/microsoft-employees-exposed-internal-passwords-security-lapse/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAADH3b7tcQM4vN6-kgHooBvpp-df-q_EEOQi0QOKqP5gT8bs2ggm8JtnvloIAVCyd3NXcVgJJwVmZfLPEovfmUzCBVmDp6Ayzx4fXDi9FEcKCRfvWiQw6xmECYGZipVOZ_9eeZXrbGrYJ8c4aNTSebVXcQyF36YKbeq1ijqlyIfk8 (besucht am 01. 06. 2024).

TechCrunch. *Why Dropbox decided to drop AWS and build its own infrastructure and network*. 2017. URL: https://techcrunch.com/2017/09/15/why-dropbox-decided-to-drop-aws-and-build-its-own-infrastructure-and-network/ (besucht am 08. 06. 2024).

Techcrunch. *Alcohol delivery service Drizly hit by data breach*. 2020. URL: https://techcrunch.com/2020/07/28/drizly-data-breach/ (besucht am 01. 06. 2024).

The Register. *Another security calamity for Capita: Unsecured AWS bucket*. 2023. URL: https://www.theregister.com/2023/05/17/another_security_calamity_for_capita/ (besucht am 01. 06. 2024).

The Stack. *Toyota data breach: vehicle location data for millions leaked*. 2023. URL: https://www.thestack.technology/toyota-data-breach-2023-t-connect-cloud/ (besucht am 01. 06. 2024).

The Sydney Morning Herald. *Football Australia data breach exposes players' passports, contracts*. 2024. URL: https://www.smh.com.au/technology/players-passports-contracts-exposed-in-football-australia-data-breach-20240201-p5f1kr.html (besucht am 01. 06. 2024).

The Verge. *Microsoft Azure cloud vulnerability is the 'worst you can imagine'*. 2021. URL: https://www.theverge.com/2021/8/27/22644161/microsoft-azure-database-vulnerabilty-chaosdb (besucht am 01. 06. 2024).

Threatpost. *Cryptojacking Attack Found on Los Angeles Times Website | Threatpost*. 2018. URL: https://threatpost.com/cryptojacking-attack-found-on-los-angeles-times-website/130041/ (besucht am 01. 06. 2024).

Threatpost. *Datadog Forces Password Reset Following Breach*. 2016. URL: https://threatpost.com/datadog-forces-password-reset-following-breach/119179/ (besucht am 01. 06. 2024).

Threatpost. *Imperva: Data Breach Caused by Amazon Cloud Misconfiguration*. 2019. URL: https://threatpost.com/imperva-data-breach-cloud-misconfiguration/149127/ (besucht am 01. 06. 2024).

Threatpost. *Imperva: Data Breach Caused by Amazon Cloud Misconfiguration*. 2019. URL: https://threatpost.com/imperva-data-breach-cloud-misconfiguration/149127/ (besucht am 01. 06. 2024).

Threatpost. *Is AWS Liable in Capital One Breach?* 2019. URL: https://threatpost.com/capital-one-breach-senators-aws-investigation/149567/ (besucht am 01. 06. 2024).

Threatpost. *SEGA's Sloppy Security Confession: Exposed AWS S3 Bucket Offers Up Steam API Access & More*. 2022. URL: https://threatpost.com/sega-security-aws-s3-exposed-steam/177352/ (besucht am 01. 06. 2024).

TroGroup. *TroGroup wurde Ziel eines Cyber-Angriffs | TroGroup*. 2023. URL: https://www.trogroup.com/de/news/trogroup-cyberangriff/ (besucht am 07. 04. 2024).

Unterkaertner Nachrichten. *Geldforderung in Millionenhöhe: Bekannte Firma aus dem Lavanttal Opfer eines Hackerangriffs*. 2021. URL: https://unterkaerntner.at/index.php?id=5480 (besucht am 07. 04. 2024).

Vienna.at. *Cyberangriff auf IT-System der Westbahn: Daten abgeflossen - Vienna Online - Österreich - VIENNA.AT*. 2023. URL: https://www.vienna.at/cyberangriff-auf-it-system-der-westbahn-daten-abgeflossen/8372323 (besucht am 07. 04. 2024).

Wirtschaftkammer Österreich. *Zahlungsdienstegesetz und Zahlungsinstitute*. 2020. URL: https://www.wko.at/oe/information-consulting/finanzdienstleister/artikel-zahlungsdienstegesetz.pdf (besucht am 13. 03. 2025).