FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

IKT-Sicherheitsrisiken an Schulen – Analyse und Darstellung möglicher Handlungsempfehlungen für ein Schul-CERT

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Magister

im Rahmen des Studiums

Informatikmanagement

eingereicht von

Timo Mischitz
Matrikelnummer 0548503

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung
Betreuer/in: Prof. Dr. A Min Tjoa
Mitwirkung: Univ.-Ass. Dr. Stefan Fenz

Wien, 01.04.2014

(Unterschrift Verfasser) (Unterschrift Betreuer)

Kurzfassung

IT-Sicherheit und Datenschutz ist aktuell ein bestimmendes Thema, sowohl im privaten als auch im beruflichen Alltag. Innovative Technologien bringen für alle Lebensbereiche Erleichterungen und ermöglichen die Aufschließung von neuen Anwendungsbereichen für die Benutzer, welche bis zu diesem Zeitpunkt nicht denkbar waren. Allzu oft wird dabei jedoch der Aspekt der Sicherheit unterschätzt und die Folgen daraus sind zumeist erst im Nachhinein bitter spürbar. Die Vergangenheit hat gezeigt, dass durch die Vernachlässigung von sicherheitstechnischen Maßnahmen im technischen, organisatorischen und rechtlichen Bereich gravierende Sicherheitslücken entstehen können, welche nachträglich nur schwer behebbar sind.

Als ein aktuelles Beispiel führt der Autor die ungewollte Veröffentlichung der Testergebnisse der informellen Kompetenzmessung von österreichischen Schülern im Internet an. Eine Veröffentlichung der Daten war möglich, da die Testergebnisse auf nicht ausreichend gesicherten rumänischen Servern gespeichert wurden. Als Konsequenz der Veröffentlichung wird Österreich an dem bereits geplanten PISA-Test 2015 nicht teilnehmen.

An Österreichs Schulen wird eine Vielzahl von sensiblen, personenbezogenen Daten verarbeitet. Diese wissenschaftliche Arbeit erhebt anhand einer Literaturanalyse und Experteninterviews welche Daten dies sind und welche Maßnahmen zum Schutz vor unbefugten Zugriff ergriffen werden. Weiters stellt der Autor die Frage nach dem Handlungspotential für ein schulisches Computer Emergency Response Team um die österreichischen Schulen im Bereich der IT-Sicherheit und des Datenschutzes zu unterstützen.

Anhand der in dieser Arbeit erzielten Untersuchungsergebnisse kommt der Autor zum Schluss, dass an Österreichs Schulen sowohl im Verwaltungsbereich, als auch im pädagogischen Bereich sensible personenbezogene Daten verarbeitet werden. Obwohl das Bewusstsein zum sicheren Umgang mit Schülerdaten bei den Lehrkräften noch nicht sehr stark

ausgeprägt ist, werden die Daten durch die Ergreifung von sicherheitstechnischen Schutzmaßnahmen gut abgesichert. Es ist ein Trend zu erkennen, dass pädagogischen Daten über soziale Medien und kommerzielle Cloud-Services ausgetauscht werden. Dahingegen gibt es Anzeichen, dass in naher Zukunft schulische Verwaltungsdaten über zentrale Services verwaltet und bearbeitet werden.

Die Analysen zeigen, dass das Handlungsfeld für ein Schul-CERT breit gestreut ist. Vorwiegend sehen die Experten hier die Möglichkeit proaktive Services zu entwickeln um den EDV-Kustoden an Österreichs Schulen konzeptionelle Arbeiten zu erleichtern. Auch die Aufgabe einer Meldestelle für IT-Sicherheitsvorfälle kann durch ein Schul-CERT erfüllt werden.

Damit ein Schul-CERT seine Aufgaben wahrnehmen kann ist es wesentlich, dass dieses durch die Schulen als Dienstleister für IT-Sicherheitsservices akzeptiert wird. Es ist notwendig, dass ein Schul-CERT eine klare Beauftragung durch das zuständige Fachministerium erhält und eine finanzielle Absicherung des finanziellen Budgets garantiert ist. Für einen erfolgreichen Start ist es hilfreich, wenn die Mitarbeiter eines Schul-CERTs bereits Erfahrungen im schulischen Bereich aufweisen und über technisches Fachwissen verfügen.

Abstract

Currently, ICT security and data protection are dominant topics in both the private and professional aspects of our daily lives. Innovative technologies facilitate some of these aspects and allow for the unlocking of new areas of application, which may not have been feasible up to this point. However, too often the aspect of security is underestimated and, in retrospect, the consequences of doing so are felt painfully by those affected. The past has shown that neglecting of security measures in technical, organizational and legal areas can cause serious security vulnerabilities which may be difficult to correct subsequently.

As a recent example, the author presents an incident of accidental release of test results of the informal competency measurement of Austrian students on the Internet. The unintended disclosure of these test results was made possible due to storage on insecure and not appropriately configured servers. As a consequence of this disclosure, Austria will not take part in the upcoming PISA tests in 2015.

In Austrian schools a variety of sensitive personal data is being processed. This thesis combines literature analysis and expert interviews to examine what kinds of data are being processed and what measures are being taken to protect this data against unauthorized access. Furthermore, the author investigates options for a School Computer Emergency Response Team (i.e. a 'school-CERT') in supporting Austrian schools regarding ICT security and data protection.
Based on the results of this thesis, the author comes to the conclusion that in Austrian schools, both the administrative and educational areas, sensitive, personal information is being processed. While awareness of teaching personnel regarding the secure processing of personal data of pupils is somewhat lacking, the data itself is adequately secured through the application of technical measures.

A movement towards the exchange of educational data through social media and commercial cloud services can be noticed. In contrast, the responsible ministry plans to manage administrative data via centralized ICT services.

The results of this thesis show that the field of action for a school-CERT is widely spread. Primarily, the interviewed experts see a possibility for the development of proactive services to support ICT supervisors in Austrian schools with conceptual tasks. Additionally, the task to serve as a registration office for cyber incidents can be met by a school-CERT.

In order to perform its tasks it is essential that a school-CERT becomes accepted by the Austrian schools as a service provider for IT security services. This requires a clear remit for a school-CERT assigned by the responsible ministry, as well as a guarantee for the required financial budget. For a successful start, it is also helpful that the staff of a school-CERT has already some experience of working in schools and brings in the necessary technical expertise.

Inhaltsverzeichnis

1 Problemstellung

Sicherheit und Vertrauen in die vernetzte Welt von heute ist ein wesentlicher Faktor für die Aufrechterhaltung der digitalen Geschäftsprozesse der Wirtschaft, Wissenschaft, Behörden und der Kommunikation im privaten Umfeld[1]. Wir alle profitieren von dieser engmaschigen Vernetzung in den Bereichen E-Government, E-Business oder auch Social Media. Auch die stark steigende, weitverbreitete Nutzung von mobilen Endgeräten wie Notebooks, Netbooks und Smartphones trägt zur intensiveren Verschränkung von Mensch und Technik bei und eröffnet allen Benutzern weitere interessante Möglichkeiten die vernetzten Informationen weltweit zu nutzen.

In den Bereichen Bildung und Forschung hat der Bereich der Informationstechnologie (IT) einen wesentlichen Stellenwert eingenommen. Sei es in den nationalen und internationalen Forschungsprogrammen der nationalen Regierung und der Europäischen Union wie KIRAS oder Horizon 2020, welche auch einen besonderen Schwerpunkt im Bereich der IT-Sicherheit gelegt haben oder in der täglichen Verarbeitung von Schüler- und Lehrerdaten an den österreichischen Schulen und der multimedialen Unterstützung in der Unterrichtsgestaltung.

In den Schulen wird das medial sehr breite Medium IT bereits seit einigen Jahren zur Unterstützung der Verwaltungsaufgaben genutzt. So wird bereits seit Jahren die Führung eines elektronischen Klassebuches ermöglicht. Klassebucheintragungen werden digital eingepflegt, Anwesenheitslisten der Schüler online kontrolliert und auch die Ausbildungsinhalte können über diese neue Technologie eingetragen werden. Dies erleichtert den Lehrkräften die Erfüllung der administrativen Aufgaben und ermöglicht der Schulleitung vereinfachte Kontrolle des Lehrkörpers. Auch für die Schüler und Eltern ergeben sich durch die Einführung der elektronischen Klassenbücher

[1] Vgl. http://www.ots.at/presseaussendung/OTS_20120305_OTS0184/am-weg-zu-einer-nationalen-cyber-strategie-fuer-oesterreich, abgerufen am 04.01.2013

wesentliche Vorteile. So kann zum Beispiel aus dem Internet der aktuelle Stundenplan und mögliche Supplierstunden abgerufen werden.

So wird im Wiener Neustädter Bundesoberstufen Realgymnasium bereits seit dem Schuljahr 2009/2010 auf den Einsatz des digitalen Klassenbuches gesetzt[2]. Somit haben die Lehrer die Möglichkeit direkt in das elektronische System einzuloggen um zum Beispiel Fehlstunden einzutragen, aber auch um sich die aktuellen Stundenpläne der einzelnen Klassen anzusehen. Technisch setzt man dabei die Implementierung der österreichischen Firma Gruber & Petters GmbH, welche die Lösung Untis anbietet.

Untis ist ein Stundenplangenerator, welcher dem Benutzer die Möglichkeit bietet auch Vertretungskonzepte und Kursplanungen zu gestalten, sowie diese Daten auch statistisch auszuwerten. Über die diverse Zusatzmodule und der webbasierten Schnittstelle Webuntis wird das elektronische Klassenbuch für Lehrer und Schüler angeboten, Die Daten dieses Systems sind exportierbar und können auch über ein Smartphones synchronisiert werden[3].
Auch zur didaktischen Unterstützung in der Unterrichtsgestaltung werden IT-Komponenten eingesetzt. Vom punktuellen Einsatz als Unterstützung in speziellen Fächern mittels interaktiven Whiteboards bis hin zu vollausgestatteten und interaktiven Notebook- und IPad-Klassen reicht die Bandbreite an möglichen Einsatzszenarien.

Interaktive Whiteboards werden zur multimedialen Unterstützung im Unterricht eingesetzt und ermöglichen es dem Lehrpersonal einerseits die Medienkompetenz der Schüler in diesem Bereich zu stärken, aber auch die Schüler verstärkt in den Unterricht einzubinden. So hat eine österreichische Studie des Bundesministeriums für Unterricht, Kunst und Kultur „Einführung und Evaluation von Interaktiven Whiteboards (IWBs) in der LehrerInnen Aus- und Fortbildung im Bereich Sprachenausbildung“ ergeben, dass der Einsatz eine Vielzahl von unterschiedlichen Medien in der Unterrichtgestaltung ermöglicht und unterschiedliche Sinneskanäle der Schüler angesprochen werden. Das

[2] Vgl. http://www.borg2700.at/php/projekt.php?projekt=Schulbeginn&schuljahr_id=0910; aufgerufen am 20.10.2013
[3] Vgl. http://www.grupet.at/de/produkte/untis/uebersicht_untis.php,, abgerufen am 20.10.2013

erzeugt eine verstärkte Konzentrationsmöglichkeit und eine intensivere Partizipation der Schüler am Unterricht (vgl. dazu auch BMUKK Evaluationsstudie 2009).

Auf freiwilliger Basis werden bereits seit 2000 in einigen österreichischen Schulen Schulklassen mit mobilen Endgeräten und Internetzugang ausgestattet. Die bisherigen Evaluierungsstudien haben gezeigt, dass diese neue Form des Unterrichts positive Auswirkungen auf die schulische Entwicklung des Kindes hat (vgl. Spiel et al, 2003). Einerseits verändert sich durch den Einsatz neuer Medien der didaktische Ansatz des Lehrenden, weg vom Frontalunterricht, hin zum integrativen Lehransatz durch eine verstärkte Einbindung der Schüler in der Aufarbeitung der Themen. Das hat wiederrum Auswirkungen auf die Motivation des Schülers den zu lernenden Schulstoff zu antizipieren. Es wurde auch nachgewiesen, dass SchülerInnen von Notebook-Klassen im Bereich der Informationsmanagement-Kompetenz: Erkennen, Verarbeiten und Wiedergeben von Informationen, besser abschneiden (vgl. dazu Spiel et al, 2003).

1.1 Zunehmende Internetnutzung

Sowohl im Bildungsbereich, als auch im privaten und geschäftlichen Sektor hat die Nutzung des Internets wesentlich zugenommen. Die verstärkte Nutzung von mobilen und ultramobilen Endgeräten, wie Notebooks, Tablets, Handhelds und Smartphones in den unterschiedlichsten Bereichen hat zu einer verstärkten Digitalisierung der Informationen und Vernetzung der Benutzer geführt.

So zeigt auch der ITU-ICT Facts and Figures Report für 2011 (vgl. International Telecommunication Union, 2011, S.4) dass das Internet aufgrund der Verbreitung von Smartphones und des Ausbaus des mobilen Breitbandes massiv expandiert. Im europäischen Raum ist die Verbreitung sehr stark ausgeprägt. Über 50 Prozent der Bevölkerung nutzen bereits die Möglichkeit des mobilen Breitbandes. Dagegen nutzen lediglich 25 Prozent den

kabelgebundenen Breitbandanschluss. In Österreich sind die Zahlen sogar noch höher. Die Nutzung des mobilen Breitbandes beträgt derzeit 67 Prozent[4].

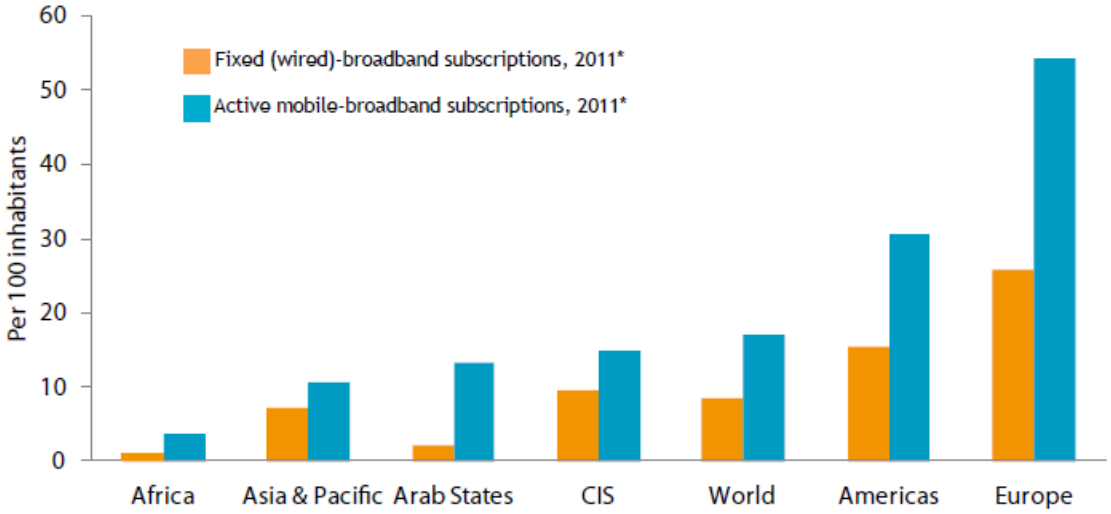

Abbildung 1 Einsatz von mobilen Endgeräten- Quelle ITU[5]

Parallel mit dem rasanten Anstieg der Nutzung des Mobilen Breitbandes und dem Ausbau des 3G[6] Netzes stieg in den letzten Jahren auch die verfügbare internationale Bandbreite exponentiell (siehe dazu Abbildung 6). 2011 betrug die internationale Bandbreite circa 80.000 Gigabit pro Sekunde. Das entspricht dem Inhalt von 2100 DVDs, die innerhalb von einer Sekunde weitergegeben werden können.

[4] Vgl. International Telecommunication Union, 2011, ITU-ICT Facts and Figures Report
[5] Vgl. a.a.O.
[6] http://wirtschaftslexikon.gabler.de/Archiv/569859/umts-3g-v2.html

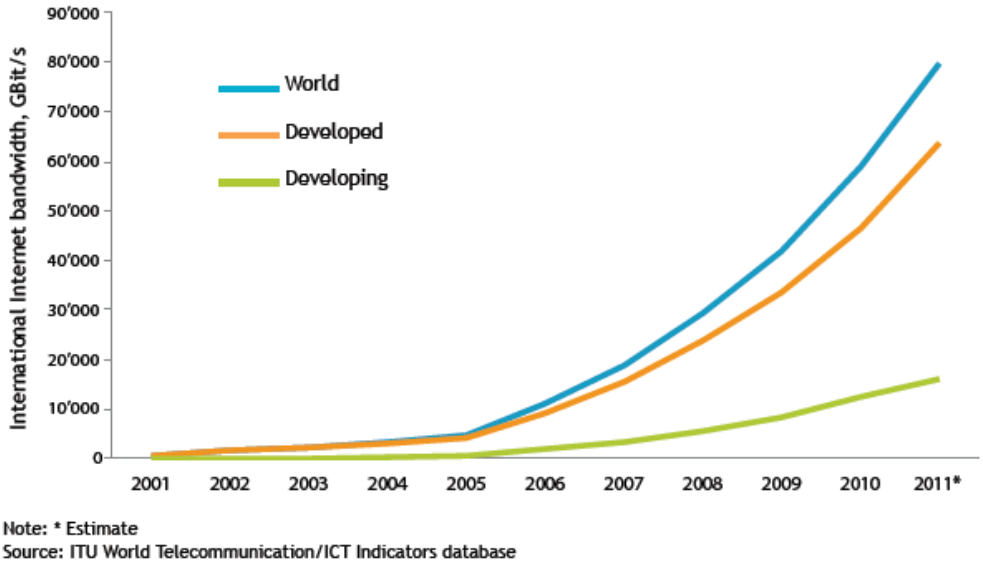

Abbildung 2: Ausbau des Internet[7]

1.2 Risiken im Internet

So vielfältig das umfassende Internet in Verwendung ist, uns inzwischen in alle Lebensbereich begleitet und das Leben erleichtert, desto größer ist auch die Abhängigkeit der Benutzer von dieser Technologie. Sei es die computergestützte Trinkwasseraufbereitungsanlage, die elektronischen Finanztransaktionen, der tägliche Kontakt über Facebook, Twitter, Skype und ähnlichen Social Media-Anwendungen oder die Bereitstellung von schulischen Services an Lehrer, Schüler und Eltern. Die vielseitigen Aspekte in der Nutzung der Informations- und Kommunikationstechnik verbreitert auch die Risiko- und Gefährdungslage im Internet.

Waren es bis vor einigen Jahren noch im Wesentlichen *SPAM (*vgl. National Institute of Standards and Technology Interagency or Internal Report 7298r2, S.190*)-, Phishing* (vgl. National Institute of Standards and Technology Interagency or Internal Report 7298r2, S.146) und *Denial of Service-Attacken (*vgl. National Institute of Standards and Technology Interagency or Internal Report 7298r2, S.66*)*, die mehr oder weniger gut aufbereitet, die größten Bedrohungen im Internet darstellten, so hat sich die Bedrohungslage in den letzten Jahren noch mehr verschärft.

[7] Vgl. http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf

Unternehmen, Behörden und Privathaushalte die in den Fokus von Attacken über das Internet geraten, müssen sich mit komplexen und vielschichtigen Angriffsmustern auseinandersetzen. Gezielte Angriffe, abgestimmt auf die technischen Gegebenheiten der Zielorganisation, kombiniert mit Social Engineering (vgl. National Institute of Standards and Technology Interagency or Internal Report 7298r2, S.189) prägen das Bild der aktuellen Bedrohungslage.
Eine der medienwirksamsten Angriffe gelang einem Hacker im Jahr 2011 durch die Kompromittierung des staatlichen, niederländischen Zertifikatsdienstanbieters DIGINOTAR (CERT.at, 2011). Dem Angreifer gelang es über die IKT-Infrastruktur von DIGINOTAR gefälschte Webserver-Zertifikate, unter anderem für die Domain google.com, auszustellen. Durch die missbräuchliche Verwendung der Zertifikate kann dem Internetbenutzer eine gefälschte Website der Firma Google untergeschoben werden, um so Benutzerdaten abzugreifen.

Abbildung 3: erste öffentliche Meldung zu Diginotar-Vorfall; Veröffentlicht auf Twitter[8]

1.3 IT-Sicherheitsrisiken in Schulen

Speziell im schulischen Bereich steht das IKT-Sicherheitsverantwortliche Personal vor besonderen Herausforderungen. Für die Unterrichtsgestaltung und

[8] Vgl. https://twitter.com/hkashfi/status/107758824810758144

die Verwaltung der Schuldaten werden immer mehr, immer komplexere IT-Systeme eingesetzt, welche eine höhere Flexibilität in der Verwaltung und im Unterricht ermöglicht und eine stärkere Einbindung der SchülerInnen fördert, welche aber auch größere Risikopotentiale und Gefährdungslagen fördern.
Im schulischen Bereich müssen eine Vielzahl von Daten mit welche unterschiedlichen Schutzniveaus verarbeitet und gespeichert. Seien es personenbezogene Daten von LehrerInnen und Schülern, Noten, Verhaltensbeurteilungen, Beschwerden, Schularbeits- und Maturadaten.

Ein Sicherheitsvorfall im schulischen Bereich, welcher großer medialer Aufmerksamkeit zu Teil wurde, war der Hacking-Angriff auf die IT-Infrastruktur des niederösterreichischen Landesschulrates im Jahr 2011. Teil dieses Angriffes war die Bereitstellung von Zugangsinformationen zum Webmailsystem, auf dem personenbezogene, zum Teil sensible personenbezogene Daten, verarbeitet wurden.

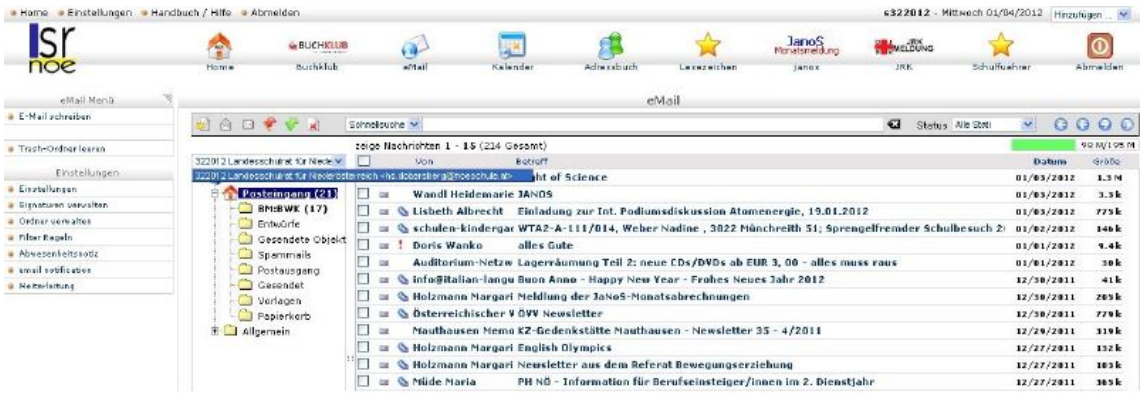

Abbildung 4: illegaler Zugriff auf Webmail LSR NÖ[9]

Ein weiterer Vorfall betraf das österreichische Bundesinstitut für Bildungsforschung, welches die Daten der informellen Kompetenzmessung verwaltet. Laut Medienaussagen wurden mehr als 37.000 personenbezogene E-Mailadressen und eine unbestimmte Anzahl von anonymisierten Testergebnissen im Internet veröffentlicht. Nach derzeitigem Stand handelte es sich hierbei um Originaldatensätze, welche als Testdaten auf rumänischen Servern gespeichert wurden. Bis dato ist noch nicht bekannt, ob es sich hierbei

[9] Vgl. http://img855.imageshack.us/img855/6792/nswer.jpg

um eine Attacke aus dem Internet gehandelt hat, oder ob die Daten von einem Insider veröffentlicht wurden[10].

Die Konsequenz aus diesem Vorfall ist, dass die für 2015 geplanten und bereits in der Vorbereitung befindlichen PISA-Tests für Österreich abgesagt wurden, da die Sicherheit der Schülerdaten nicht gewährleistet werden kann[11].

Diese Vorfälle haben gezeigt, dass auch IT-Systeme der Schulen und der Schulverwaltung in den Fokus der Angreifer gerückt ist. Die Angriffe passieren aber nicht immer nur von extern. Auch der Angreifer von innen muss in die Risikobetrachtung der IT-Sicherheitsverantwortlichen einbezogen werden.

Schüler, welche bereits als Digital Natives aufwachsen, eine hohe Affinität zu neuen Medien und zu neuen Technologien haben und diese auch gerne ausprobieren, werden so oft ungewollt zum potentiellen Risikofaktor und stellen ein Einfallstor für Viren, Trojanern und Würmern dar.

1.4 Forschungsfragen

Basierend auf dieser Problemstellung stellt sich die Frage nach dem Erkenntnisstand über den Status der Datensicherheit an den österreichischen Schulen. Dabei sollen in dieser Arbeit folgende, konkrete Fragestellungen berücksichtigt werden:

1. Welche sensiblen Daten werden im Schulbereich verarbeitet?
2. Welche Sicherheitsrisiken existieren?
    a. Gibt es spezifische Auswirkungen durch den Einsatz von Computerklassen und Bring Your Own Device-Endgeräten?
    b. Gibt es spezifische IT-Sicherheitsrisiken an Schulen?

[10] Vgl. http://derstandard.at/1392686483213/Bifie-Datenleck-gestopft-Tests-gestoppt , zuletzt aufgerufen am 19.3.2014
[11] Vgl. http://derstandard.at/1392687781758/Schuelerdaten-Heurige-Bildungsstandard-Testungen-abgesagt, zuletzt aufgerufen am 19.3.2014

3. Gibt es bereits genügende Maßnahmen Schutz der Schulen und wie wird die Einhaltung dieser eingefordert?
    a. Welche technischen, organisatorischen und rechtlichen Maßnahmen werden getroffen um die Risiken zu senken?
4. Welche Rolle kommt den Computer Emergency Response Teams (CERTs) dabei zu?

1.4.1 Zu erwartendes Ergebnis Forschungsfrage 1

Das föderale System Österreichs spiegelt sich auch im Schulsektor wieder. Abhängig von Schultyp, ob Primär-, Sekundarschule oder Akademie[12] ist eine entsprechende Verwaltungszuständigkeit auf Bundes-, Landes oder Gemeinde-Ebene festgelegt.

Basierend auf der Kenntnis der bisher analysierten Informationen ist davon auszugehen, dass im schulischen Betrieb eine große Menge an Daten tagtäglich elektronisch in Schulnetzen verarbeitet wird. Die Sensibilität der Daten zieht sich von eher unkritischen Unterrichtsdaten wie Hausaufgaben, digitale Stunden- und Supplierpläne, über sensible Schüler- und Lehrerverwaltungsdaten bis hin zu sehr sensiblen, schulärztlichen Daten.

1.4.2 Zu erwartendes Ergebnis Forschungsfrage 2

IKT-Systeme werden im schulischen Bereich sehr breit eingesetzt. Einerseits werden die Schüler- und Lehrpersonaldaten über ein administratives Netzwerk verwaltet und verarbeitet, andererseits unterstützen IKT-Systeme auch die Unterrichtsgestaltung durch den Einsatz von Notebooks, Whiteboards und ähnlichem.

Die Integration der IKT in die Unterrichtsgestaltung zur Stärkung und Förderung der Medienkompetenz der SchülerInnen ist ein Kernelement im täglichen Schulbetrieb. Hierbei werden all jene digitalen Fähigkeiten erlernt, welche auch

[12] Vgl. Schulorganisationsgesetz §3 Abs.2, Rechtsinformationssystem ris.bka.gv.at

späteren Berufsleben von Bedeutung sind. Auch der Bereich Bewusstseinsbildung im IKT-Sicherheitskontext nimmt hierbei einen wesentlichen Teil der Unterrichtsgestaltung ein. Das bedeutet aber auch, dass Schüler und Schülerinnen die Möglichkeit haben müssen im Internet so frei wie möglich zu agieren und mit neuen Medien zu experimentieren. Die entstehenden Anforderungen stehen oft im Widerspruch zu den sicherheitstechnischen Vorgaben und Einstellungen. In diesem Kontext entsteht ein ausgeprägtes Spannungsfeld zwischen Benutzerfreundlichkeit und Sicherheit, welches es aufzulösen gilt.

Eine besondere Herausforderung an die Sicherheitstechnik stellt die kommende standardisierte, kompetenzorientierte Reifeprüfung, auch Zentralmatura genannt, dar. Die Zentralmatura sieht vor, dass Prüfungsunterlagen und Prüfungsergebnisse über ein zentrales Webportal angeboten werden, von dem das Lehrpersonal in Zukunft die aktuellen Unterlagen runterladen muss. Durch die Bereitstellung dieser Informationen über das Internet ergeben sich eine Reihe von Herausforderungen hinsichtlich der Vertraulichkeit, Verfügbarkeit und Integrität der Daten. Im Gegensatz zur bisherigen dezentralen Verwaltung der Maturadaten eröffnet die zentrale Wartung des Internetportals aber auch Möglichkeiten zur Durchsetzung einer starken technischen und organisatorischen Sicherheitsrichtlinie zum Schutz der Reifeprüfungsdaten. So können zum Beispiel stärkere Richtlinien im Bereich der Datenverschlüsselung und des Passwortmanagements umgesetzt werden.

1.4.3 Zu erwartendes Ergebnis Forschungsfrage 3

Schuldaten unterliegen nationalen und bundesländerspezifischen gesetzlichen Bestimmungen sowie organisatorischen Regelungen, welche deren Verarbeitung, Aufbewahrung und Weiterleitung regeln. Beispielhaft können hierfür das Schulunterrichtsgesetz, das Datenschutzgesetz sowie der Informationserlass 2010 „Digitale Kompetenz an Österreichs Schulen“, welcher durch das Bundesministerium für Unterricht, Kunst und Kultur veröffentlicht wurde, genannt werden.

Es existieren eine Vielzahl von Regelungen und Handlungsempfehlung, welche zu einer erhöhten Sicherheit an den österreichischen Schulen beitragen. Aus Sicht des Verfassers sind diese Unterlagen jedoch noch nicht konkret genug und können aufgrund fehlender Personalressourcen und budgetärer Mittel, sowie der fehlender Priorität im schulischen Alltag nicht umfassend umgesetzt werden.

1.4.4 Zu erwartendes Ergebnis Forschungsfrage 4

Als ein Computer Emergency Response Team bezeichnet man eine Organisation oder ein Team von Sicherheitsspezialisten, das sich mit sicherheitstechnischen Vorfällen beschäftigt. Die meisten Computer Emergency Response Teams benutzen die Abkürzung CERT oder CSIRT[13].

Die Aufgaben eines CERTs sind vielfältig und umfassen von reaktiven, präventiven und qualitätssichernden Maßnahmen ein sehr breitgefächertes Spektrum an Aktivitäten.

Reactive Services	Proactive Services	Security Quality Management Services
Alerts and Warnings Incident Handling – Incident analysis – Incident response on site – Incident response support – Incident response coordination Vulnerability Handling – Vulnerability analysis – Vulnerability response – Vulnerability response coordination Artifact Handling – Artifact analysis – Artifact response – Artifact response coordination	Announcements Technology Watch Security Audits or Assessments Configuration and Maintenance of Security Tools, Applications, and Infrastructures Development of Security Tools Intrusion Detection Services Security-Related Information Dissemination	Risk Analysis Business Continuity and Disaster Recovery Planning Security Consulting Awareness Building Education/Training Product Evaluation or Certification

Abbildung 5: CERT/CSIRT Services[14]

Unter reaktiven Services versteht man die Koordination und technische Unterstützungsleistung bei sicherheitstechnischen Vorfällen. Auch die Informationsverteilung von Alarm- und Warnmeldungen fallen in diese Kategorie. Reaktive Services stellen die Kernaktivitäten eines CERTs dar.

[13] CSIRT steht für Computer Security Incident Response Team, inhaltlich gibt es aber keine Unterscheidung zu einem CERT.
[14] http://www.cert.org/csirts/services.html

Die proaktiven Services umfassen all jene Tätigkeiten, die bereits im Vorfeld von sicherheitstechnischen Vorfällen helfen die IKT-Infrastruktur abzusichern. Dazu zählt Technologiefolgeabschätzung, Aufbau und Betrieb von Sicherheits-Monitoring-Systemen usw.

Qualitätssichernde Maßnahmen im Sicherheitskontext sind kein Alleinstellungsmerkmal von CERTs. Services wie zum Beispiel Risikoanalyse und Notfallmanagement im IKT-Bereich sind wesentliche Qualitätsmerkmale zur Steigerung der umfassenden Sicherheit eines hochentwickelten Unternehmens oder einer Behörde. Aus dem CERT-Kontext heraus versteht man darunter die Einbindung einer CERT-Struktur in die bestehenden Prozesse und Abläufe sowie die damit verbundene Anreicherung der bestehenden IKT-Services durch Zusatzinformationen aus diesen Bereichen.

Im schulischen Kontext sind CERTs bis heute noch nicht etabliert, obwohl gerade im schulischen Bereich der Einsatz von IKT-Systemen wächst und die eingesetzten Systeme aufgrund der hohen Flexibilitätsanforderung im administrativen und pädagogischen Einsatzbereich einer Vielzahl von Sicherheitsrisiken ausgesetzt sind. Auch aus personaltechnischer und budgetärer Sicht stellt die Implementierung eines Schul-CERTs als zentrale Anlaufstelle für sicherheitstechnische Fragestellungen, im Sinne einer Bündelung der IKT-Sicherheitsexpertise, eine sinnvolle Investition dar. So könnte ein Schul-CERT als erste Anlaufstelle für Kompromittierungen an IKT-Schulsystemen sein und so einen Bündelungseffekt in qualitativer und quantitativer Hinsicht bewirken.

Weiters wäre es möglich, dass ein Schul-CERT im Bereich der Bewusstseinsbildung zum Thema IKT-Sicherheit für Lehrer und Schüler Schulungen konzipiert. Ebenso ist eine Multiplikatorwirkung im Sinne einer „Train the Trainer“-Ausbildung im Bereich Aus- Fort- und Weiterbildung des Lehrpersonals vorstellbar.

3 Methodisches Vorgehen

Die hier vorliegende wissenschaftliche Arbeit gliedert sich in zwei methodische Teilstücke. Der erste Teil behandelt die relevante Theorie, welche für diese Arbeit zur Verfügung steht, und soll dabei vorab eine Begriffsbestimmung als Einführung in die Thematik geben.

Der zweite Teil der Arbeit umfasst eine empirische Erhebung des Forschungsgegenstandes in Form einer Serie von qualitativen Interviews. Der Verfasser der Arbeit hat sich dazu entschieden die Interviews in Form einer Serie von Experteninterviews zu führen. Die Experten werden aus den Bereichen Schule, Schulverwaltung und Computer Emergency Response Team anhand von zuvor festgelegten Kriterien ausgewählt.

Das folgende Kapitel beschreibt die theoretische Herangehensweise an die Dokumentenanalyse, sowie die Durchführung und Auswertung der Experteninterviews.

3.1 Dokumentenanalyse

Im Bereich der qualitativen Sozialforschung zählt die Dokumentenanalyse zu den quantitativen inhaltsanalytischen Forschungstechniken (vgl. Lamnek 1995, S.193). Es werden hierbei bestehende Informationsträger, wie Bücher, Ton- oder Videoaufzeichnungen, Zeugnisse und ähnliches anhand qualitativer Kriterien untersucht. Es wird empirisches Material analysiert, welches nicht erst durch den Forscher neu erschlossen werden muss (vgl. Mayring 1996, S.33).

Im quantitativen Forschungsbereich werden für die Durchführung von Dokumentenanalysen bereits im Vorfeld detaillierte Richtlinien für die Bearbeitung des Forschungsmaterials definiert. Zu Beginn dieses systematisierten Ansatzes bestimmt der Autor, welche Dokumentenart Teil der Untersuchung wird. Weiters wird festgelegt, wie groß die zu untersuchenden Analyseeinheiten sind. Diese Festlegung kann sehr konkret sein. So wird

beispielsweise jeder Satz oder jedes Wort analysiert. Es kann aber auch ein interpretativer Ansatz gewählt werden und zum Beispiel alle Artikel über den Forschungsgegenstand einer Fachzeitschrift analysiert werden (vgl. Mayer, 2002, S.146).

Unter der Analysedimension versteht man die an die Analyseeinheit zu stellende Fragestellung. Die Analysedimension kann in weitere Kategorien unterteilt und detailliert beschrieben werden (ebd., S.146).

Im Gegensatz zur quantitativen Dokumentenanalysen wird bei der qualitativen Dokumentenanalyse im Vorfeld kein fixes Raster hinsichtlich der Analyseeinheit und Analysedimension definiert. Konkrete Richtlinien werden während der Aufarbeitung der einzelnen Dokumente festgelegt und werden im weiteren Verlauf detaillierter gefasst (ebd., S.148).

Für den weiteren Forschungsprozess wird nur mehr die Methodik der qualitativen Dokumentanalyse berücksichtigt.

3.2 Das Experteninterview

Der zweite Teil der Arbeit umfasst die empirische Erhebung und Auswertung von Informationen anhand von qualitativen Interviews zu den im Kapitel 2 angeführten Forschungsfragen. Nachdem es nach derzeitigen Kenntnisstand keine breite Datenbasis zur Messung von IKT-Sicherheit und keine expliziten Zahlen über sicherheitstechnische Vorfälle an österreichischen Schulen gibt, wird im empirischen Teil der Diplomarbeit als Vorgehensweise die qualitative Erhebungsmethode des halb standardisierten Interviews mit Interviewleitfaden gewählt (vgl. dazu auch Mayer, Hanna, 2002, S.124).

Im folgenden Kapitel soll die Methodenauswahl begründet werden sowie die Technik und dessen Forschungsverlauf kurz dargestellt werden. Überdies werden Auswahlkriterien für die Interviewpartner definiert und die Auswahl der Experten anhand dieser begründet.

Die Experteninterviews stellen für die Hypothesenfindung eine große Bedeutung dar. Darum wird im folgenden Kapitel die methodische Herangehensweise an das Interviews näher erklärt.

3.2.1 Experteninterviews als Spezialform eines halb standardisierten Interviews

Als Variante des halb standardisierten Leitfrageninterview stellt das Experteninterview keine eigene Interviewform dar (vgl. dazu auch Flick, Uwe, 2006).

Experteninterviews werden in den verschiedensten Forschungsfeldern zum Einsatz genommen, oft werden sie im Rahmen eines Methodenmix, aber auch als eigenständiges Verfahren angewendet, allerdings herrscht ein Mangel an methodischer Reflexion darüber, selbst in Lehrbüchern die explizit sich der Methode des Interviews widmen, werden sie nicht speziell thematisiert (vgl. dazu auch Meuser, M. / Nagel, U. S. 72).

Das Experteninterview stellt in der qualitativen Interviewtechnik keine hohen Ansprüche an die Gesprächsführung und an die Interpretation. Die gewonnenen Informationen stellen grundsätzlich eher Hintergrundwissen dar. Ziel des Experteninterviews ist die Gewinnung von empirischem Wissen und nicht die theoretische Erklärung und Generalisierung der „empirischen Tatsachen“. (vgl. Froschauer, U/Lueger M., das qualitative Interview, 2003, S.92)

Beim Experteninterview stehen nicht die Experten als Personen im Mittelpunkt des Forschungsinteresses, sondern das Betriebswissen über ihr Handlungsfeld. Sie repräsentieren Handlungs- und Sichtweisen einer bestimmten Gruppe. (vgl. dazu auch Flick, Uwe, 2006, S.5).

Unter Experten versteht man Führungsspitzen aus den Bereichen Politik, Wirtschaft, Justiz, Verbänden, Wissenschaft, aber auch Lehrer, Sozialarbeiter und Personalräte. Der Expertenstatus wird vom Forscher in gewisser Weise verliehen, begrenzt auf seine spezifische Fragestellung (ebd. S. 73).

„Als Experte wird angesprochen,

- wer in irgendeiner Weise Verantwortung trägt für den Entwurf, die Implementierung oder die Kontrolle einer Problemlösung
- wer über einen privilegierten Zugang zu Informationen über Personengruppen oder Entscheidungsprozesse verfügt.“ (Meuser, M / Nagel, U. 1991, S. 78)

Bei der Auswahl der Experten ist es besonders wichtig sorgfältig Auswahlkriterien zu definieren um die Vergleichbarkeit der Interviewpartner zu gewährleisten. Hierbei muss auf die Hierarchieebene der Experten Rücksicht genommen werden. Man kann davon ausgehen, dass eine hohe hierarchische organisatorische Verankerung der ausgesuchten Experten zwar auf viel Wissen, Erfahrung und Kompetenz schließen lässt, jedoch auch die Bereitschaft zur Teilnahme an den Interviews sinkt.

3.2.3 Interviewleitfaden

Um eine gute Voraussetzung für qualitativ hochwertige und vergleichbare Interviewergebnisse zu schaffen, wird für die Experteninterviews ein Interviewleitfaden entwickelt. Das folgende Kapitel beschreibt die wesentlichen Charaktermerkmale eines Interviewleitfadens und hebt die Vorteile eines solchen hervor.

Unter einem Interviewleitfaden versteht man ein verschriftlichest Fragenschema, welches dem Interviewer als Orientierungshilfe und Gedächtnisstütze in der Planung, Durchführung und Auswertung von qualitativen Interviews dient (vgl. Stigler und Felbinger in Stigler und Reicher, 2005, S129).

Bei der Interviewform des Experteninterviews ist ein gut vorbereiteter Interviewleitfaden ein hilfreiches Instrument, da er für den Interviewer eine stark strukturierende und steuernde Funktion hat. Ebenso dient ein Interviewleitfaden als qualitätssicherndes Element, da der Interviewer bereits im Vorfeld inhaltlich

gut in das Thema eingearbeitet sein muss um den Leitfaden zu erstellen. Es ist damit ausgeschlossen, dass wesentliche Themenaspekte in der Vorbereitung der Fragen übersehen werden (vgl. Stiegler/Felbinger in Stigler/Reicher, 2005 S.130).

Ein Interviewleitfaden erfüllt unterschiedliche Funktionen in der Vorbereitung und in der Durchführung der Experteninterviews. „Die in die Entwicklung eines Leitfadens eingehende Arbeit schließt aus, dass sich der Forscher als inkompetenter Gesprächspartner darstellt. […] Die Orientierung an einem Leitfaden schließt auch aus, dass das Gespräch sich in Themen verliert, die nichts zur Sache tun, und erlaubt zugleich dem Experten, seine Sache und Sicht der Dinge zu extemporieren.“ (Meuser / Nagel, 1991, S. 77)

Die Auswahl der Experten wurde unter dem Aspekt getroffen wurde, dass sie möglichst unterschiedliche Blickwinkeln auf die zu erforschende Thematik eröffnen. Um trotz der unterschiedlichen Perspektiven eine thematische Vergleichbarkeit der Expertenaussagen zur gewährleisten, wird ein Interviewleitfaden entwickelt.

Der Interviewleitfaden wurde im Vorfeld hinsichtlich seiner Anwendbarkeit getestet werden um mögliche logische Brüche in den einzelnen Fragestellungen aber auch der Gesamtstruktur aufzufinden und zu beseitigen. (vgl. Stigler und Felbinger in Stigler und Reicher, 2005, S132)

Für den Aufbau des Leitfadens wurde berücksichtigt, dass für ein 1stündiges Interview etwa 8-15 Fragen ausreichend sind. Als Einleitungsfrage ist eine Eisbrecherfrage vorgesehen, um den Experten in einer sympathischen Atmosphäre an das eigentliche Thema heranzuführen.

3.2.4 Auswertung der Experteninterviews

Die Analyse der einzelnen Interviews und die vergleichende Zusammenführung dieser ist ein wesentlicher Bestandteil für die Gewinnung der notwendigen Hintergrundinformation zur Beantwortung der Forschungsfragen. Im folgenden

Kapitel beschreibt der Autor die wesentlichen Schritte zur Auswertung des in den einzelnen Experteninterviews gewonnenen kommunikativen Datenmaterials.

Ziel der Auswertung von Experteninterviews ist es, die Gemeinsamkeiten der einzelnen inhaltlichen Positionen herauszuarbeiten, aber auch die repräsentative Einzelaussagen der Experten zu erfragen, um die gewonnenen Ergebnisse schlussendlich zu Generalisieren und um Interpretationen und Ableitungen für die im Kapitel 2 dargestellten Forschungsfragen zu konzipieren (Meuser, M / Nagel, U. 1989, S. 11).

Im Zuge der Auswertung ist es von besonderer Wichtigkeit, dass der Interviewer ein großes Vorwissen über den Forschungsgegenstand hat, um mögliche Anomalien oder Auffälligkeiten im Gespräch zu entdecken und aufzuzeigen. Das über ein qualitatives Interview gewonnene Wissen entspricht nicht immer zwangsläufig den Überzeugungen, oder auch dem Wissensstand des Interviewers und öffnet so den Wissenshorizont.

Paradoxerweise ist es ebenso notwendig, dass in der methodischen Auswertung des Datenmaterials der Interviewer sein Vorwissen über den zu untersuchenden Gegenstand bewusst ignorieren muss. Im Zuge der methodischen Auswertung kommt es zu einer Dekonstruktion des vorhandenen Wissens unter Hinzugabe der neuen Erkenntnisse. Diese Auswertemethodik ermöglicht eine Neustrukturierung des Wissens (vgl. Froschauer, U/Lueger M., das qualitative Interview, 2003, S.85).

Im Zuge der Auswertung der Experteninterviews werden folgende Detailschritte durchlaufen, welche im Folgenden beschrieben werden:

- Transkription
- Paraphrase
- Überschriften
- Thematischer Vergleich
- Kategorienbildung
- Theoretische Generalisierung

In der Phase der Transkription werden die aufgezeichneten Experteninterviews schriftlich übertragen. Die Transkription gilt als eines der wesentlichen Grundvoraussetzungen für die Auswertung von Experteninterviews. Das Ausmaß der Verschriftlichung hängt in der Regel vom Erfolg des Interviews ab. Gelingt es dem Interviewer im Rahmen des Diskursverlaufes viel Hintergrundwissen zu erlangen, ist eine wortgetreue Transkription sinnvoll.

Das Ziel der Paraphrase ist das Verdichten von Inhalten und das Erstellen erster Erfahrungs- und Argumentationsmuster, sowie die Reduktion von Komplexität der Inhalte. Dabei ist es wichtig, dass die Chronologie des Gespräches berücksichtigt wird. Ob der Interviewer sich dazu entscheidet zusammenfassende oder detaillierte Paraphrasen zu entwickeln, hängt in der Regel vom Experten ab. Ob dieser dem Inhalt große oder kleine Bedeutung im Diskusverlauf beimisst.

Im nächsten Schritt der Verdichtung werden die einzelnen paraphrasierten Passagen Überschriften zugeordnet. In dieser Phase kann die Sequenzialität unterbrochen werden um einzelne Passagen auch mehreren Überschriften zuzuordnen oder umgekehrt. Es stehen primär die Themen und Informationen im Vordergrund, nicht mehr mögliche Einzelfallbeispiele. Passagen mit gleichen oder ähnlichen Inhalten werden zusammengestellt und einer Hauptüberschrift zugeordnet.

In den vorherigen Schritten hat sukzessive die Inhaltsmasse und die Komplexität der Inhalte der Einzelinterviews abgenommen. Es erscheint daher notwendig nun in die Auswertung der Texteinheiten hinaus einzusteigen. Dazu wird nach sinngemäßen Übereinstimmungen in den Textpassagen der einzelnen Experteninterviews gesucht, übergreifend zusammengestellt und die Überschriften vereinheitlicht. Das führt zwangsläufig zu einer weiteren Reduktion der Inhalte, bietet aber auch die Möglichkeit Redundanzen zu tilgen.

Der nächste Schritt in der Auswertung – die Kategorienbildung - ermöglicht die Systematisierung der zuvor gewonnenen Inhalte. Durch die Kategorisierung der

Inhalte werden zuvor entnommene Begriffe und Überschriften abstrahiert um eine generalisierte Interpretation zu ermöglichen – man spricht von einer empirischen Generalisierung.

Im letzten Schritt der Auswertung, der theoretischen Generalisierung, werden die einzelnen Kategorien in einen Zusammenhang gebracht um Theorien zu überprüfen. Ziel der Generalisierung ist es das Wissen der Experten in neue Zusammenhänge zu setzen und gegebenenfalls neue Theorien zu entwickeln und zu überprüfen (Meuser, M / Nagel, U. 1989, S. 11).

3.2.5 Auswahl der Experten

Aufgrund der spezifischen Forschungsthematik und der geringen, vorhandenen Datenbasis aus dem IKT-Sicherheitssektor an österreichischen Schulen wird im Rahmen der Erhebung auf sechs ausgewählte Experten aus den Bereichen der österreichischen, kommunalen Schulnetzbetreiber, der Computer Emergency Response Teams und der österreichischen Bundesverwaltung als Interviewpartner zurückgegriffen.

Für die Auswahlstrategie fassen Gläser/Laudel (2004) vier hilfreiche Fragen zusammen:
„1. Wer verfügt über die relevanten Informationen?
2. Wer ist am ehesten in der Lage, präzise Informationen zu geben?
3. Wer ist am ehesten bereit, Informationen zu geben?
4. Wer von den Informanten ist verfügbar?“ (Gläser/Laudel 2004: 113)

Zusätzlich zu den von Gläser/Laudel (2004) verfassten Kriterien sollen die ausgewählten Experten eine langjährige Erfahrung im Bereich

- der operativen Schulnetzwerkbetreuung,
- IKT-Sicherheit und
- operative Erfahrung im Bereich der Vorfallsbehandlung aufweisen.

3.2.6 Vorstellung der Interviewpartner

Mag. Robert SCHISCHKA, CERT.at

Aus dem CERT-Bereich wird um einen Interviewtermin beim Leiter des nationalen Computer Emergency Response Team, CERT.at, Mag. Robert SCHISCHKA, angefragt. Schischka ist seit dem Jahr 2008 Leiter des nationalen CERT.at und ausgewiesener CERT-Experte. Weiters ist Schischka Mitglied des Steering Comittees und Mitglied des Board of Directors des Forum of Incident Response and Security Teams, der weltweiten Dachorganisation von etablierten CERTs.

Aus der Formulierung des Leitbildes ist das Aufgabengebiet von CERT.at klar ersichtlich:

„CERT.at ist das österreichische nationale CERT (Computer Emergency Response Team). Als solches ist CERT.at der Ansprechpartner für IT-Sicherheit im nationalen Umfeld. Es vernetzt andere CERTs und CSIRTs (Computer Security Incident Response Teams) aus den Bereichen kritische Infrastruktur, IKT (Informations- und Kommunikationstechnik) und gibt Warnungen, Alerts und Tipps für KMUs (kleine und mittlere Unternehmen) heraus.“ (CERT.at, Zugriff vom 04.08.2013)

Ing. Roland LEDINGER, Bundeskanzleramt

Als zweiter Experte wurde Ing. Roland LEDINGER ausgewählt. Ledinger ist im Bundeskanzleramt Bereichsleiter für den Bereich „IKT-Strategie des Bundes“ und Geschäftsführer der Plattform Digitales Österreich. Im Rahmen seiner Tätigkeiten ist er im Bundeskanzleramt federführend für die strategischen Elemente der nationalen und internationalen Cyber Security, sowie des Government Computer Emergency Response Team, GovCERT Austria, verantwortlich.

Das Aufgabenumfeld des GovCERT Austria umfasst folgende Aspekte: „Auf nationaler Ebene erfüllt GovCERT eine Koordinationsfunktion zwischen den einzelnen Stellen der öffentlichen Verwaltung und den Betreibern kritischer Infrastruktur:

- Sammlung und Bewertung von Vorfällen aus dem operativen IKT-Betrieb der Bundes-, Landes-, Städte- und Gemeindeverwaltungen
- Koordinierung von Gegenmaßnahmen
- Beschaffung und Bewertung von Nachrichten aus öffentlich und nicht-öffentlich zugänglichen Quellen“ (govcert.gv.at, Zugriff am 04.08.2013)

Alexander TALOS-ZENS, Universität Wien

Als dritter Experte wurde Alexander TALOS-ZENS ausgewählt. Talos-Zens ist Leiter des ACOnet-Computer Emergency Response Team, ACOnet-CERT. ACOnet ist der Betreiber des österreichischen Wissenschaftsnetzes und somit ein wesentlicher Netzwerk-Dienstleister für die Betreiber der österreichischen Schulnetze. Die CERT-Aktivitäten werden durch den Zentralen Informatik Dienst der Universität Wien erbracht.

Das Aufgabenportfolio des ACOnet-CERT stellt sich wie folgt dar:
„Der Zuständigkeitsbereich (Constituency) des ACOnet-CERT umfasst alle am ACOnet teilnehmenden Netze. Das CERT hat zwei Aufgabenbereiche:

- konkrete Sicherheitsvorfälle einer Lösung zuzuführen
- allgemein die Computersicherheit zu fördern.

Die Bearbeitung von Sicherheitsvorfällen, international als *Incident Handling* bezeichnet, nimmt den breitesten Raum ein und wird unter Lösen von Sicherheitsvorfällen beschrieben.
Daneben trägt das CERT zur Entwicklung der Security-Landschaft durch Fachvorträge bei, sowohl in nationalem als auch internationalem Rahmen.
Durch die Doppelidentität als CERT eines Backbone-Netzes einerseits und als Security-Team einer Universität andererseits ergibt sich die Möglichkeit, für den Eigenbedarf entwickelte Tools und Methoden zur Verfügung zu stellen.“[15]

[15] Vgl. https://wiki.univie.ac.at/display/CERT/ACOnet-CERT, abgerufen am 04.08.2013

Raphaela PSIHODA, Bundesministerium für Bildung und Frauen

Frau Raphaela PSIHODA ist langjährige Expertin für das nationale Bildungsnetzwerk an Österreichs Schulen. Als Ansprechpartnerin für die IP-Adressverwaltung an den Schulen weist sie große Erfahrung im Bereich der Netzwerk- und Informationssicherheit auf.

Das Bundesministerium für Bildung und Frauen koordiniert den Auf- und Ausbau des österreichischen Bildungsnetzwerks, dem EDUNET. Das EDUNET ist ein flächendeckendes, auf Glasfaser basierendes Netzwerk zur Anbindung Österreichs Schulen an das Internet. Weiters stellt das Ministerium über das Microsoft Austrian College and Highschool Agreement Softwarelizenzen für den Bildungsbereich zur Verfügung.

DI Barbara Buchegger, ÖIAT

DI Barbara Buchegger hat als Expertin im Bereich E-Learning, Medienkompetenzförderung und Digitale Medien der Saferinternet.at Initiative eine langjährige Erfahrung im nationalen und internationalen Bereich der IKT-Sicherheit, mit speziellem Fokus auf Bildungseinrichtungen.

„Saferinternet.at unterstützt vor allem Kinder, Jugendliche, Eltern und Lehrende beim sicheren, kompetenten und verantwortungsvollen Umgang mit digitalen Medien.
Die Initiative wird im Auftrag der Europäischen Kommission im Rahmen des Safer Internet Programms umgesetzt.
Saferinternet.at bildet gemeinsam mit der Stopline (Meldestelle gegen Kinderpornografie und nationalsozialistische Wiedebetätigung) und 147 Rat auf Draht (Telefonhilfe für Kinder, Jugendliche und deren Bezugspersonen) das „Safer Internet Centre Austria“. Es ist der österreichische Partner im Safer Internet Netzwerk der EU (Insafe).“ (saferinternet.at am 11.8.2013)

Mag. Gerald STACHL, BRG Gröhrmühlgasse, Wiener Neustadt

Mag. Gerald STACHL ist langjähriger EDV-Kustos im Bundesrealgymnasium Gröhrmühlgasse. Ihm obliegt in dieser Funktion die fachlich-pädagogische Betreuung der schulweiten IKT-Infrastruktur für einige hundert Schüler und Lehrer. Die Aufgaben eines Kustos umfasst laut BGBl. II Nr. 481/2004[16] folgende Aufgaben:

- die anwendungsnahe Hard- und Softwareunterstützung einschließlich Internetanbindung und Anwenderprogramme,
- unterrichtsorganisatorische Arbeiten,
- die Betreuung der Lehrer und der Schüler im IT-Betrieb der Schule,
- Mitwirkung am facheinschlägigen Beschaffungswesen,
- die Führung der Fachbibliothek und

die Erstellung eigener und die Evidenthaltung elektronischer Publikationen des Fachgebietes.

Das BRG Gröhrmühlgasse verfügt über eine Vielzahl elektronischer Schüler-, Lehrer- und Eltern-Services welche über das Internet angeboten werden. Unter anderem das elektronische Klassenbuch, aktuelle Supplierpläne, e-Learning Module, etc. … . Für die Planung und Umsetzung von sicherheitstechnischen Maßnahmen zur Absicherung der Systeme ist ein tiefes, technisches Verständnis erforderlich. Neben den technischen Sicherheitsmaßnahmen ist ein verantwortungsvoller Umgang der User mit den elektronischen Services ein wesentlicher Bestandteil des Sicherheitsmanagements.

Als erfahrener EDV-Kustos verfügt Stachl über ein detailliertes und breitgefächertes Wissen über den Einsatz von EDV als unterstützendes Element im Unterricht und elektronischen Services für Schüler, Eltern und Lehrer, sowie über Einführungsschwierigkeiten und Probleme im täglichen Betrieb. Weiters ist davon auszugehen, dass der Interviewpartner bereits bei einer Vielzahl von sicherheitstechnischen Vorfällen federführend an der Systemwiederherstellung gewirkt hat und somit eine große Expertise im praktischen Bereich und auf dem Gebiet der Awareness-Bildung einbringt.

[16] Vgl. https://www.ris.bka.gv.at/showdata/?targetURL=https://moa-sl.bka.gv.at/showdata;jsessionid=C9B6DF692C187E82A83BE2F49A038429?hidCount=0 am 11.8.2013

3.3 Interviewleitfaden

Interviewleitfaden -
IKT-Sicherheitsrisiken an Schulen – Analyse und Darstellung möglicher Handlungsempfehlungen für ein Schul-CERT

Einleitung:

Vielen Dank, dass Sie mir die Möglichkeit eröffnen mit Ihnen dieses Interview zu führen. Ich schreibe derzeit an meiner Magisterarbeit zum Thema „IKT-Sicherheitsrisiken an Schulen – Analyse und Darstellung möglicher Handlungsempfehlungen für ein Schul-CERT“ und führe in diesem Zusammenhang einige Experteninterviews durch.
Ziel dieser Arbeit ist den Status der IT-Sicherheit an den österreichischen Schulen zu erheben, sowie mögliche Potentiale und Entwicklungsmöglichkeiten eines Schul-Computer Emergency Response Teams aufzuzeigen.
Das Interview wird in etwa 60 Minuten dauern
Bevor ich Ihnen nun die Fragen stelle, möchte ich noch auf einige allgemeine Punkte hinweisen. Das Interview wird zur Kontrolle meiner Mitschrift über ein Audio-Aufnahmegerät aufgezeichnet – sind Sie damit einverstanden? Falls es von Ihnen gewünscht ist, werden die transkribierten Teile des Interviews anonymisiert.
Das Interview ist in folgende vier Abschnitte gegliedert:

- Verarbeitung von sensiblen Daten an Schulen
- IT-Sicherheitsrisiken an Schulen
- Schutzmaßnahmen und Kontrolle
- Mögliche Aufgaben eines Schul-CERT

Haben Sie noch Fragen bevor wir mit dem Interview beginnen?

Forschungsfrage 1: Welche sensiblen Daten werden im Schulbereich verarbeitet?

1. Welche IT-Services bieten Sie Schülern und Eltern an?
2. Welche IT-Services bieten Sie Lehrern an?

3. Welche Daten im Schulbereich würden Sie als sensibel ansehen?
4. Nach welchen Kriterien beurteilen Sie sensible Daten?
5. Werden sensible Daten im Bereich des Unterrichts verarbeitet (Bsp. Smartboards und Datenintegrität)?
6. Unterliegen diese Daten speziellen Gesetzen oder sonstigen Regelungen?
7. Werden sensible Daten im Bereich der öffentlichen Services verarbeitet (Bsp. Klassenbuch und Datenintegrität, Verfügbarkeit)?
8. Unterliegen diese Daten speziellen Gesetzen oder sonstigen Regelungen?
9. Werden sensible Daten im Bereich der Schulverwaltung verarbeitet (Bsp. Lehrer/Schülerdaten, Noten, etc.)?
10. Unterliegen diese Daten speziellen Gesetzen oder sonstigen Regelungen?
11. Führen Sie vor dem Einsatz sensibler IT-Systeme eine Schutzbedarfsanalyse/Risikoanalyse durch?

Forschungsfrage 2: Welche IT-Sicherheitsrisiken existieren an Schulen? Welche davon sind schulspezifisch? Welche neuen Herausforderungen ergeben sich durch Computerklassen?

1. Welchen IT-Sicherheitsrisiken sind Ihre Systeme im täglichen Betrieb ausgesetzt?
2. Welche speziellen IT-Sicherheitsrisiken sehen Sie im Bezug auf den Einsatz von IT-Systemen im Unterricht (Bsp. Smartboard)
3. Welche speziellen IT-Sicherheitsrisiken sehen Sie im Bezug auf den Einsatz von IT-Systemen im Verwaltungsbereich (Bsp. Personaldaten von Lehrer)?
4. Existieren unterschiedliche Risikoprofile von IT-Systemen für den Einsatz im Unterricht und für den Einsatz in der Verwaltung?
5. Welcher dieser IT-Sicherheitsrisiken würden Sie als schulspezifisch ansehen?
6. Welche IT-Sicherheitsrisiken sehen Sie durch den verstärkten Einsatz von Computerklassen?

7. Welchen Einfluss auf die IT-Sicherheit hat der Einsatz von persönlichen Endgeräten (BYOD – Bring Your Own Device) im Unterricht?
8. Welche neuen Anforderungen entstehen durch den Einsatz von Computerklassen an Lehrer und Schüler?
9. Nach welchen Kriterien beurteilen Sie IT-Sicherheitsrisiken
10. Wie viel Zeit pro Monat nimmt das Thema IT-Sicherheit im Hinblick auf präventive, reaktive und qualitätssichernde Maßnahmen in Anspruch?

Forschungsfrage 3: Gibt es bereits genügend Maßnahmen zum IT-Schutz der Schulen und wie wird die Einhalt dieser eingefordert? Welchen technischen, organisatorischen und rechtliche Maßnahmen werden getroffen um Risiken zu senken?

1. Welche technischen und organisatorischen Schutzmaßnahmen treffen Sie um den Risiken zu begegnen?
2. Welche Maßnahmen würden Sie als schulspezifisch ansehen?
3. Existieren geforderte Mindeststandards in Form von Richtlinien, Standards, etc. (Bsp. Erlässe BMUKK)?
4. Welche Hilfestellungen erhalten Sie von außen (Bsp. Staat, Safer Internet, etc.)?
5. Wird die Umsetzung staatlicher Maßnahmen/Erlässe ausreichend kontrolliert?
6. Wie viele Stunden pro Monat investieren Sie in die Überprüfung der Wirksamkeit von Schutzmaßnahmen?
7. Empfinden Sie Ihre getroffenen Maßnahmen als ausreichend?
8. Wo besteht aus Ihrer Sicht noch Verbesserungsbedarf?

Forschungsfrage 4: Welche Rolle kommt den Computer Emergency Response Teams (CERTs) dabei zu? Welche Auswirkungen haben die Tätigkeiten von CERTs auf den Unterricht?

1. Erhalten Sie Unterstützung im Falle einer Kompromittierung eines IT-Systems?
2. Falls ja, von wem? (Bsp. Lehrer, Schüler, externe Dienstleister, staatliche Stellen, Interessensgemeinschaften, etc.)

3. Erachten Sie die Unterstützung als ausreichend?
4. Wo würden Sie noch Verbesserungsbedarf sehen
5. Haben Sie die Möglichkeit sich mit anderen IT-Verantwortlichen über Ihre Erfahrungen auszutauschen?
6. Über welche Inhalte tauschen Sie sich bereits aus, oder über welche Inhalte würden Sie sich gerne austauschen?
7. Kennen Sie den Begriff des Computer Emergency Response Teams?
8. Falls ja, woher?
9. Hatten Sie bereits Kontakt mit einem CERT? Falls ja, in welchen Zusammenhang?
10. Kennen Sie in Österreich bereits CERTs oder CERT-ähnliche Strukturen für den Schulbereich?
11. Welche Aufgaben könnte ein Schul-CERT im Bereich der technischen und organisatorischen Sicherheit übernehmen?
12. Welche Aufgaben könnte ein Schul-CERT im Bereich der Unterrichtsgestaltung übernehmen?
13. Welche Aufgaben könnte ein Schul-CERT im Bereich der Aus-, Fort- und Weiterbildung übernehmen?
14. Wie müsste ein solches Schul-CERT institutionalisiert werden um erfolgreich arbeiten zu können?
15. Welche Fähigkeiten müssten die Mitarbeiter eines Schul-CERT aufweisen?
16. Welche konkrete Hilfestellung würden Sie sich von einem Schul-CERT erwarten?
17. Gibt es von Ihrer Seite aus weitere Anmerkungen, welche nicht im Rahmen des Interviews angesprochen wurden?

4 State of the art

Im folgenden Kapitel gibt der Autor einen Überblick über das gesichtete Material der Primär- und Sekundärliteratur zu den Themen Computer Emergency Response Teams und IT-Sicherheit an Österreichs Schulen.

Er beschreibt anhand einiger grundlegender Dokumente, verwandten Berichten und Studien die wesentlichen Inhalte und Ergebnisse zu den Themen IT-Sicherheit an Schulen und Computer Emergency Response Teams.. Das Kapitel 4 soll dem Leser einen Überblick über die vorhandene Literatur geben und die wesentlichsten Ergebnisse darstellen. Die vorliegende Beschreibung stellt keine abschließende Aufzählung der verwendeten Lektüre dar.

4.1 ITU: Report ICT Facts and Figures 2011

Der jährlich erscheinende ITU-Bericht über globale IKT-Entwicklungen und neue Trends untersucht den Einsatz von IKT weltweit und gibt Aufschluss über das länderspezifische, technische Entwicklungspotential.

Relevante Ergebnisse

Der Report zeigt, dass der Anteil der Internet-User global stark zunimmt. Bereits ein Drittel der Weltbevölkerung ist bereits online. Über 40 Prozent der weltweiten Internet-Benutzer ist unter 25 Jahre alt. Über 36 Prozent der unter 25-jährigen nutzt bereits das Internet. Auf Basis der vorliegenden Ergebnisse kann man davon ausgehen, dass gerade für die Altersklasse der Schüler das Internet einen wesentlichen Faktor im Leben bereits darstellt und auch in Zukunft darstellen wird. Ob im Privatleben oder beruflich, die vernetzte IKT-Infrastruktur wird ein fixer Bestandteil in allen Lebenslagen.

Vor allem der Bereich der mobilen Datenkommunikation hat im Jahr 2011 stark zugenommen. Bereits mehr als 50 Prozent der Einwohner von Europa haben einen mobilen Internetzugang. Während der mobile Internetzugang in den entwickelten Ländern als zusätzlicher Zugang zum Internet verwendet wird, ist dieser in den Entwicklungsländern der einzige Zugang.

Der Bericht zeigt, dass die internationale Internet-Bandbreite in den letzten Jahren signifikant gestiegen ist. Betrug diese im Jahr 2006 noch 11.000 Gigabit pro Sekunde, stieg sie im Jahr 2011 auf 90.000 Gigabit pro Sekunde. Die Internetbandbreit ist global jedoch nicht gleich verteilt. So verzeichnet der Report eine Bandbreite pro User von 90.000 Bit pro Sekunde in Europa und lediglich 2000 Bit pro Sekunde in Afrika.

4.2 Panda Security: Kindergarten 12 Education IT Security Study

Im Mai 2011 hat das Sicherheitsunternehmen PANDA-Security eine Studie[17] zur Computer-Sicherheit an Schulen veröffentlicht. Diese Studie untersucht die IT-Sicherheitsrisiken Schulen aktuell ausgesetzt sind und stellt die Frage welche Maßnahmen schulseitig umsetzbar sind um die Risiken zu minimieren.

Relevante Ergebnisse

Die Untersuchung wurde über den Zeitraum von einem Monat an 100 Kindergärten und Schulen in den USA durchgeführt und hat aufgezeigt, dass das Internet heutzutage ein unschätzbarer Faktor für die Unterrichtsgestaltung darstellt. Ohne die Umsetzung entsprechender IT-Sicherheitsmaßnahmen kann die Nutzung des Internets im Unterricht jedoch zu einer Bedrohung der IKT-Infrastruktur werden. Diese Maßnahmen erfordern viel Zeit in der Planung, Umsetzung und Kontrolle.

Eines der bemerkenswertesten Ergebnisse dieser Umfrage ist, dass bereits 59 Prozent der IT-Verantwortlichen an öffentlichen Schulen mehrmals die Woche einen Schadsoftware-Alarm vermerken. An bereits mehr als 82% der untersuchten Schulen konnten die Schüler und das Lehrpersonal private Endgeräte in den Unterricht mitbringen und verwenden. Nur 15% dieser Schulen verzichten auf den Einsatz von zusätzlichen IKT-

[17] http://press.pandasecurity.com/wp-content/uploads/2011/03/Panda-K12-Education-IT-Security-Study_03.23.11.pdf

Sicherheitsmaßnahmen zum Schutz der privaten Endgeräte. Als Hauptgrund für die Nicht-Weiterentwicklung und das Update von IKT-Sicherheitsmaßnahmen geben 72% der Befragten Budget-Beschränkungen an, weitere 38% verweisen auf Personalknappheit und 29% unterstreichen, dass der Einsatz von IKT andere Prioritäten als die Sicherheit verfolgt.

In der Studie wurde festgehalten, dass der Einsatz von Social Media Applikationen in den Unterricht ein kommender Schwerpunkt in den nächsten Jahren sein wird. Bereits 95% der Schulen haben eine Policy für den Einsatz von Social Media Applikationen umgesetzt. Diese sind jedoch nicht schulübergreifend abgestimmt oder vereinheitlicht.

Der Autor der Studie kommt zu dem Schluss, dass das vermehrte Auftreten von IKT-Sicherheitsvorfällen das Lehrpersonal vom eigentlichen Unterricht ablenkt. Daher müssen, durch den Einsatz zentral gemanagten Sicherheits-Services, die Lehrenden von der täglichen Arbeit entlastet werden. Weiters soll der Zugang zu und Zugriff auf Social Media Applikationen über eine Policy administriert werden um möglichen Angriffen über Schadsoftware oder Cyber-Bulling bereits im Vorfeld zu unterbinden. Ebenso müssen zusätzliche Sicherheitsmaßnahmen für die Integration von privaten Endgeräten in ein Schulnetzwerk getroffen werden, um einen entsprechenden Sicherheitsstand aufrechterhalten zu können.

4.3 Bundeskanzleramt: Handfolder - Sind Sie sicher

Ende des Jahres 2011 veröffentlichte das Bundeskanzleramt einen Handfolder zum Thema IKT-Sicherheit. Dieser Folder wurde als eine Sensibilisierungsmaßnahme nach den zahlreichen Anonymous-Angriffen 2011 umgesetzt und richtet sich an die Mitarbeiter der österreichischen, öffentlichen Verwaltung. Der Folder beschreibt wesentliche Risiken im Umgang mit dem Medium Internet und bei der Nutzung von IKT-Infrastruktur am Arbeitsplatz und schlägt Handlungsempfehlungen für einen sicheren Umgang vor. Auch der oberösterreichische Landesschulrat griff diese Initiative auf um das Lehrpersonal über die aktuellen Aktivitäten zu informieren.

Relevante Ergebnisse

Sensible Daten, welche offen am Schreibtisch liegen gelassen werden, oder die Verwendung von unsicheren Passwörtern sind offensichtliche Risiken, welche mittels entsprechender Sensibilisierungsmaßnahmen vermieden werden können. Dieser Handfolder stellt eine Hilfe zur Selbsthilfe des Endbenutzers dar und listet eine Vielzahl von möglichen Maßnahmen auf, welche eigenständig, ohne großen Aufwand, das Risiko einer Kompromittierung minimieren. Die Handlungen umfassen die Bewusstseinsbildung im Bereich der Arbeitsplatzgestaltung, über die Verwendung von Passwörtern bis hin zur sicheren E-Mail Kommunikation.

Weiters bietet der Handfolder weitere Hilfe durch die Bereitstellung von Kontaktdaten des österreichischen Government Computer Emergency Response Team, GovCERT Austria. Das GovCERT Austria ist das CERT der österreichischen Verwaltung und stellt die primäre Anlaufstelle für Fragen zu IKT-Sicherheitsvorfällen aus dem Behördensektor dar.

4.4 Bundesministerium für Unterricht, Kunst und Kultur: Empfehlung - Digitale Kompetenz an Österreichs Schulen

Die Empfehlung zur Entwicklung von digitaler Kompetenz an Österreichs Schulen wurde im Auftrag des Bundesministeriums für Unterricht, Kunst und Kultur im Jahr 2010 veröffentlicht. Sie umfasst Anleitungen und Darstellung von Best Practíce Beispielen zur Mediennutzung im Unterricht, zur Implementierung einer Internetpolicy an Schulen, sowie Empfehlungen zum einfachen und sicheren Betrieb eines umfassenden Schulnetzes.

Relevante Ergebnisse

Der rasche Fortschritt im Bereich der Informations- und Kommunikationstechnologie macht auch an den österreichischen Schulen nicht halt. Gerade im Bildungswesen ist daher der Bereich der digitalen

Medienkompetenz wesentlich. Lernen über und mit dem Computer steht damit auch im Mittelpunkt dieses Berichtes. Es werden Strategien und Handlungsempfehlungen aufgezeigt wie Schüler und Lehrer lernen und verstehen neue Medien im Sinne einer reflektierten Mediennutzung im Bildungsalltag einzusetzen um auch in Zukunft ein aktives Mitglied in der Informationsgesellschaft zu sein.

Einen besonderen Schwerpunkt setzt dieser Bericht auf den legistischen Rahmen der Mediennutzung im Unterricht und der Bereitstellung der IKT-Infrastruktur für die Schule im Allgemeinen. Konkret wir dabei auf das Urheberrechtsgesetz, den Bildnisschutz, das Jugendschutzrecht, sowie auf das Datenschutzgesetz, E-Commerce Gesetz und das Mediengesetz verwiesen, welche die wesentlichen Inhalte für dieses Gebiet darstellen.

Weiters werden notwendige Richtlinien und Empfehlungen für die Nutzer der schulischen IKT-Infrastruktur diskutiert. Das organisatorische Rahmenwerk in Form einer Internetpolicy wird als probates Mittel für eine Festschreibung der organisatorischen, anwenderbezogenen, kommunikationstechnische und informationstechnischen Maßnahmen empfohlen.

Abschließend stellt die Empfehlung noch unterschiedliche Umsetzungsmodelle für das Schulnetz vorgestellt. Es wird hierbei auf die notwendigen Hard- und Softwarekomponenten eingegangen, sowie der erforderliche IKT-Serviceumfang und -Servicegrad diskutiert. Der Serviceumfang umfasst die Bereitstellung von schuleigener Hard- und Software, über die Verfügbarkeit eines Internetzuganges bis hin zu Wartung von Fernzugängen für Schüler und Lehrer. Serviceumfang und Servicegrad können und sollen schulautonom, nach Maßgabe der Verfügbarkeit von Personal- und Budgetressourcen entschieden werden.

5 Computer Emergency Response Team

Im folgende Kapitel gibt der Autor auf Basis einer Dokumentenanalyse einen Überblick über Computer Emergency Response Teams und deren Aufgaben. Anhand des österreichischen Government Computer Emergency Response Teams wird ein Beispiel gegeben, wie ein CERT arbeitet und welche konkreten Aufgabengebiete bedient, sowie welche Services erbracht werden. Die vierte Forschungsfrage beschäftigt sich mit den potentiellen Aufgaben eines CERTs im schulischen Bereich. Kapitel 5 gibt dem Leser einen Einblick in die CERT-Thematik um darauf aufbauend die Empfehlungen für ein Schul-CERT geben zu können.

Im Folgenden beschreibt der Autor die formalen Definition eines Computer Emergency Response Teams (CERT) und dessen Aufgaben. Dazu werden im ersten Teil die wesentlichen Merkmale und Eigenschaften beschrieben, sowie die wichtigsten Aktivitäten anhand eines Servicekatalogs dargestellt.

Der zweite Teil umfasst die Verankerung der CERT-Aktivitäten in die gesamteuropäische Strategie für Wachstum - Europa 2020 - Eine Strategie für intelligentes, nachhaltiges und integratives Wachstum, und beantwortet die Frage nach der Notwendigkeit von Sicherheit und Vertrauen in die digitalen Geschäftsprozesse für die europäische Binnenmarktwirtschaft (vgl. MITTEILUNG DER KOMMISSION - EUROPA 2020 - Eine Strategie für intelligentes, nachhaltiges und integratives Wachstum, http://ec.europa.eu/eu2020/pdf/COMPLET%20%20DE%20SG-2010-80021-06-00-DE-TRA-00.pdf, zuletzt aufgerufen am 06.10.2013).

Im dritten Teil dieses Kapitels stellt der Autor die österreichische CERT-Landschaft vor. Als Beispiel für ein national und international etabliertes CERT beschreibt er dazu die Strukturen und Aufgaben des nationalen Government Computer Emergency Response Team, sowie dessen Verankerung in die österreichischen Sicherheitsarchitektur.

5.1 Allgemein

Als ein Computer Emergency Response Team bezeichnet man eine Organisation oder ein Team von Sicherheitsspezialisten, das sich mit sicherheitstechnischen Vorfällen beschäftigt. Die meisten Computer Emergency Response Teams benutzen die Abkürzung CERT oder CSIRT. CSIRT steht als Abkürzung für Computer Security Incident Response Team (vgl. ENISA, 2006, S.6).

Die Entwicklung der CERTs steht in einem sehr engen Zusammenhang mit der Entwicklung einer der ältesten Bedrohungen im Internet – dem sogenannten Internetwurm. 1988 legte der erste Internetwurm weltweit eine beträchtliche Anzahl von IT-Systemen lahm. Angesichts der offensichtlichen Notwendigkeit eines raschen und effizienten Informationsaustausches zwischen Systembetreibern in solchen Krisenfällen, wurde kurz darauf das erste Computer Emergency Response Team (CERT) an der Carnegie Mellon University in Pittsburgh gegründet (vgl. Moira J. West-Brown, Don Stikvoort et. al., 2003, S.1).

1992 entstand das erste Computer Emergency Response Team auf europäischen Boden in den Niederlanden. Heute zählt die Europäische Agentur für Netzwerk- und Informationssicherheit[18] in ihrem „Inventory of CERT activities“ (vgl. ENISA, 2013) in Europe weit über 100 Organisationen dieser Art auf.

Abbildung 3 zeigt die aktuelle ENISA CERT-Landkarte aus dem Jahr 2013.

[18] ENISA – European Network and Information Security Agency

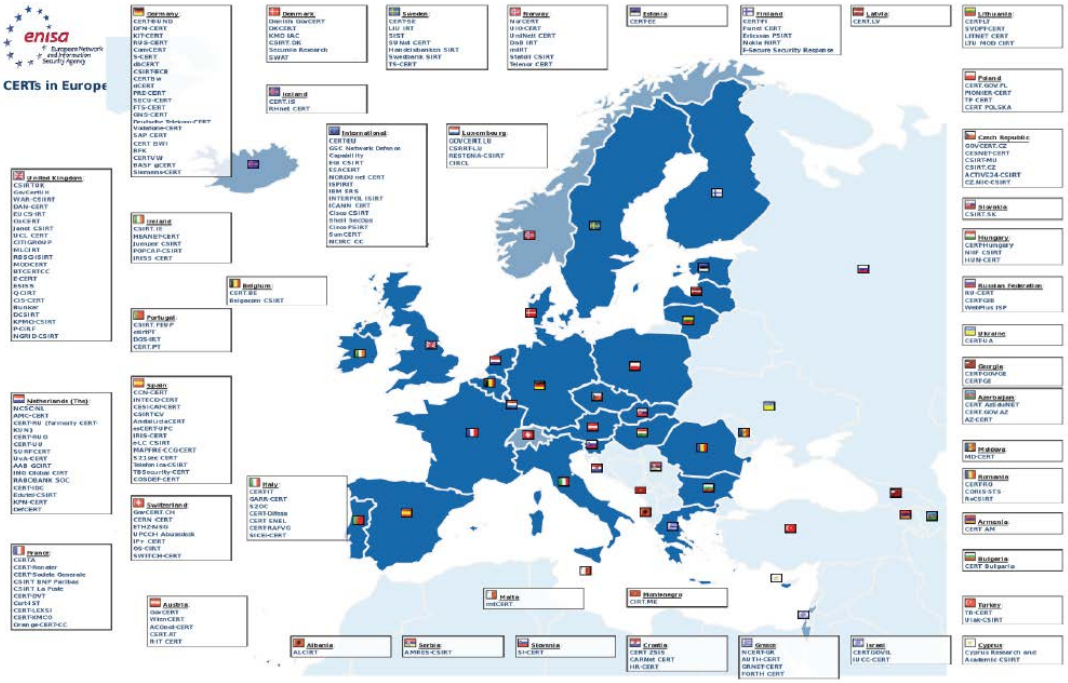

Abbildung 6: CERT-Landkarte ENISA[19]

Wie aus Abbildung 3 ersichtlich existieren derzeit fünf offizielle CERTs in Österreich, welche von ENISA erfasst worden sind. Durch diese Auflistung darf man sich nicht täuschen lassen. Es gibt eine Vielzahl von weiteren CERT-ähnlichen Strukturen und Organisationen, die aber nicht als offizielle CERTs in Erscheinung treten. Nicht alle Organisationen wollen ein vollständig etabliertes CERT, mit allen technischen, personellen und strukturellen Ressourcen, sowie den einhergehenden formalen Verpflichtungen in ihrer Organisation institutionalisieren.

5.1 Eigenschaften von CERTs

Das folgende Kapitel widmet sich den wesentlichsten Eigenschaften von Computer Emergency Response Teams in Bezug auf die Ausrichtung der Services und dessen Basisaktivitäten. Der Autor beschreibt dazu die unterschiedlichen Zielgruppen von CERTs, sowie die wichtigsten Aufgaben und Services anhand des CERT Service-Katalogs der Carnegie Mellon Universität.

[19] https://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map

5.1.1 Zielgruppen

Eine der wesentlichen Eigenschaften von CERTs ist, dass diese zielgruppenorientiert strukturiert sind. Die Bandbreite der Zielgruppe kann durch die Festlegung der Parameter sehr breit oder sehr eng gesetzt werden. Mögliche Parameter um die Zielgruppe zu definieren sind die geografische Einschränkung der Zielgruppe, die technische Orientierung der Services und die organisationsspezifische Ausrichtung.

Ein CERT muss nicht ausschließlich auf eine Zielgruppe fixiert sein. Abhängig von den angebotenen Services kann ein CERT auch unterschiedliche Zielgruppe gleichzeitig bedienen. Es können sowohl öffentliche, für jedermann verfügbare, Services angeboten werden, als auch zielgruppenspezifische Services, zum Beispiel ein technisches Services für eine spezielle Software-Anwendung (vgl. Moira J. West-Brown, Don Stikvoort et. al., 2003, S.35) angeboten werden.

Die europäische Agentur für Netzwerk und Informationssicherheit hat dazu 2006 in der Studie „CERT cooperation and ist further facilitation by relevant stakeholders“ folgende CERT-Zielgruppen definiert (vgl. ENISA, 2006, S8):

- Anbieterbereich
- CIP/CIIP-Bereich[20]
- Hochschulbereich
- Interner Bereich
- KMU-Bereich[21]
- Kommerzieller Bereich
- Militärischer Bereich
- Nationaler Bereich
- Staatlicher Bereich

[20] Critical Infrastructure Protection/Critical Information Infrastructure Protection
[21] Kleine und mittlere Unternehmen

5.1.2 Aufgaben und Services

Die Aufgaben eines CERTs sind vielfältig und umfassen von reaktiven, präventiven und qualitätssichernden Maßnahmen ein sehr breitgefächertes Spektrum an Aktivitäten. Die Carnegie Mellon University hat in ihrer Publikation „CSIRT-Handbook“ die in Abbildung vier dargestellte Tabelle mit veröffentlicht. Zur Veranschaulichung liefert die Abbildung vier eine detaillierte Übersicht über reaktive, proaktive und qualitätssichernde CERT-Services.

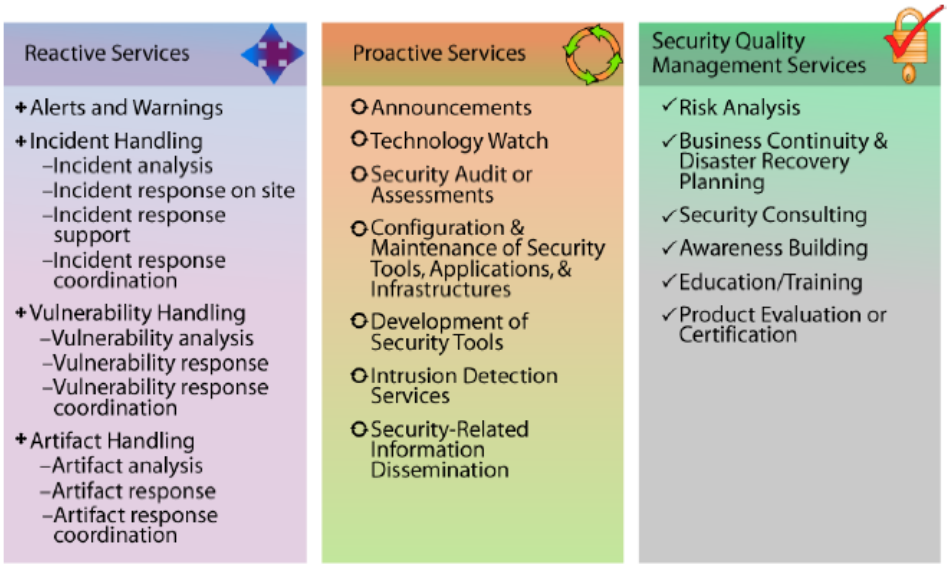

Abbildung 7: CERT/CSIRT Services[22]

Reaktive Services

Reaktive Services stellen die Kernaktivitäten eines CERTs dar. Unter reaktiven Services versteht man jene Aktivitäten, welche nach einem tatsächlichen sicherheitstechnischen Vorfall notwendig sind. Dazu zählen die Notfall-Koordination im Anlassfall und die technische Unterstützungsleistung bei sicherheitstechnischen Vorfällen. Auch die Informationsverteilung von Alarm- und Warnmeldungen fallen in diese Kategorie (vgl. Moira J. West-Brown,Don Stikvoort et. al., 2003, S.25)

[22] http://www.enisa.europa.eu/activities/cert/support/guide/files/s10.jpg

Proaktive Services

Die proaktiven Services umfassen all jene Tätigkeiten, die bereits im Vorfeld von sicherheitstechnischen Vorfällen helfen die IT-Infrastruktur abzusichern und deren IT-Services zu härten. Ziel dieser Maßnahmen ist es Sicherheitsvorfälle bereits im Vorfeld abzuwenden, beziehungsweise deren Auswirkungen zu minimieren (vgl. ebd.). Zu den proaktiven Tätigkeiten zählen Aufgaben wie Technologiefolgeabschätzung, Aufbau und Betrieb von Sicherheits-Monitoring-Systemen und Sicherheitsaudits.

Qualitätssichernde Maßnahmen

Qualitätssichernde Maßnahmen im Sicherheitskontext sind kein Alleinstellungsmerkmal von CERTs, zählen aber auch zu den klassischen CERT-Aufgaben. Services wie zum Beispiel Risikoanalyse und Notfallmanagement im IKT-Bereich sind grundsätzliche, wesentliche Qualitätsmerkmale zur Steigerung der umfassenden Sicherheit eines hochentwickelten Unternehmens oder einer Behörde. Aus dem CERT-Kontext heraus versteht man darunter die Einbindung einer CERT-Struktur in die bestehenden Prozesse und Abläufe sowie die damit verbundene Anreicherung der bestehenden Services durch Zusatzinformationen aus diesen Bereichen. Weitere Themen im Bereich der qualitätssichernden Maßnahmen sind Bewusstseinsbildung, Anbieten von Schulungen, etc. (vgl. ebd.).

5.2 CERTs in Europa

Das folgende Kapitel beschreibt die Anstrengungen der Europäischen Union im Hinblick auf die Etablierung eines nachhaltig resilienten, digitalen pan-europäischen Binnenmarktes. Der Autor stellt dazu die Europäische Strategie für nachhaltiges Wachstum in Europa vor, sowie die daraus abgeleitete Leitlinie Digitale Agenda.

EU 2020

Die Europäische Strategie für nachhaltiges Wachstum in Europe – Europa 2020 ist eine gesamteuropäisches Wirtschaftsstrategie und wurde 2010 vom Europäischen Rat, auf Vorschlag der Europäischen Kommission, angenommen (vgl. Europäischer Rat, EUCO 13/10, 2010, S.1).

Als Nachfolgeprogramm der Lissabon-Strategie, welche in den Jahren von 2000 bis 2010 galt, stellt die EU 2020 Strategie ein Wirtschaftsprogramm dar, um eine verbesserte Koordination der wirtschaftspolitischen Maßnahmen innerhalb der EU zu verbessern (vgl. Europäische Kommission, 2010, KOM(2010) 2020 S.4).

„Die EU muss festlegen, was sie bis 2020 erreichen will. Dazu schlägt die Kommission folgende EU-Kernziele vor:

1. 75 % der Bevölkerung im Alter von 20 bis 64 Jahren sollten in Arbeit stehen.
2. 3 % des BIP der EU sollten für F&E aufgewendet werden.
3. Die 20-20-20-Klimaschutz-/Energieziele sollten erreicht werden (einschließlich einer
4. Erhöhung des Emissionsreduktionsziels auf 30 %, falls die entsprechenden
5. Voraussetzungen erfüllt sind).
6. Der Anteil der Schulabbrecher sollte auf unter 10 % abgesenkt werden, und mindestens
7. 40 % der jüngeren Generation sollten einen Hochschulabschluss haben.
8. Die Zahl der armutsgefährdeten Personen sollte um 20 Millionen sinken.“ (Europäische Kommission, 2010, KOM(2010) 2020 S.3)

5.2.1 Digitale Agenda

Die Digitale Agenda ist eine der sieben Leitinitiativen der EU 2020 Strategie, der Strategie für intelligentes, nachhaltiges und integratives Wachstum in

Europa (vgl. Europäische Kommission, 2010, KOM(2010) 2020). In Europa werden derzeit circa 660 Milliarden Euro direkt durch die IKT-Branche erwirtschaftet. Das entspricht 5% des gesamteuropäischen Bruttoinlandsproduktes. Darin nicht erfasst ist die indirekte Produktivitätssteigerung durch den Einsatz von IKT. Schätzungen haben jedoch ergeben, dass diese bei 20-30% liegt (vgl. Europäische Kommission, Digitale Agenda, 2010, S.4).

Auch die Europäische Kommission hat der Notwendigkeit von funktionierenden CERTs in den europäischen Nationalstaaten durch die Verankerung in der Digitalen Agenda für Europa Nachdruck verliehen.

Ziel der Digitalen Agenda für Europa ist es, aus dem europäischen digitalen Binnenmarkt einen nachhaltigen wirtschaftlichen und sozialen Nutzen zu ziehen. Dabei wurden folgende wesentliche Hindernisse zur Erreichung des Zieles identifiziert:

- Fragmentierung der digitalen Märkte
- Mangelnde Interoperabilität
- Zunahme der Cyberkriminalität und Gefahr mangelnden Vertrauens in Computernetzwerke
- Mangelnde Investitionen in Computernetzwerke
- Unzureichende Forschung und Innovation
- Mangelnde digitale Kompetenzen und Qualifikationen

Zur Vermeidung der Entstehung dieser Hindernisse wurden 16 Schlüsselaktionen definiert, die sowohl die Zielerreichung als auch die nachhaltige Absicherung garantieren sollen.

Zwei dieser Schlüsselaktionen beziehen sich explizit auf die Sicherung der Netze und der Stärkung des Vertrauens der BürgerInnen in diese Netzwerkinfrastruktur.

- Schlüsselaktion 6:

Schlüsselaktion 6 beinhaltet Vorschläge für Maßnahmen, die eine Politik zur Stärkung der Netz- und Informationssicherheit auf hohem Niveau zum Ziel haben, einschließlich Legislativinitiativen. Darunter fallen unter anderen Maßnahmen für eine modernisierte Europäische Agentur für Netz- und Informationssicherheit, welche eine schnellere Reaktion auf Cyberangriffe ermöglichen, einschließlich eines CERT-Teams für die EU-Organe.

- Schlüsselaktion 7:

Schlüsselaktion 7 enthält Vorschläge für Maßnahmen, einschließlich Legislativinitiativen, zur Bekämpfung von Cyberangriffen auf Informationssysteme bis 2010 sowie entsprechende Vorschriften zur Gerichtsbarkeit im virtuellen Raum auf europäischer und internationaler Ebene bis 2013.

Dazu sollen alle EU-Mitgliedstaaten:

- ein nationales oder staatliches CERT funktionsfähig eingerichtet haben
- die nationalen oder staatlichen CERTs international vernetzen
- gemeinsame Cyber Exercices durchführen.

5.3 CERTs in Österreich

Das vorliegende Kapitel beschreibt die österreichischen Aktivitäten im CERT-Bereich und geht dabei im ersten Teil auf den nationalen CERT-Verbund als erste nationale CERT-Vereinigung ein. Im zweiten Teil geht der Autor im Detail auf das österreichische GovCERT.at als ein bereits im nationalen und internationalen Kontext etabliertes CERT ein.

Das erste österreichische CERT wurde 2003 im Hochschulbereich gegründet und wird vom Zentralen Informatikdienst der Universität Wien betrieben - das Austrian Academic Computer Network CERT (vgl. https://www.aco.net/cert.html?&L=0, aufgerufen am 15.10.2013). Darauf folgte das erste CERT im Finanzsektor, das Raiffeisen-IT CERT und schlussendlich wurde 2008 durch das Bundeskanzleramt in Kooperation mit der Firma NIC.at

das nationale CERT - CERT.at und das Government CERT – GovCERT.at ins Leben gerufen.

5.3.1 Nationaler CERT-Verbund

Mit dem raschen Wachstum der österreichischen CERT-Community wurde auch der Bedarf bei den einzelnen CERT-Betreibern geweckt, die nationale Vernetzung voranzutreiben. Als eine der wesentlichen Maßnahmen wurde dazu 2011 der nationale CERT-Verbund, eine Vereinigung aller österreichischen Computer Emergency Response Teams unter der Federführung von GovCERT.at gegründet.

Der nationale CERT-Verbund ist das Ergebnis der Initiative zu Schaffung einer nationalen CERT-Plattform. Ziel dieser Initiative ist die Identifizierung von nationaler Expertise, um Bündelungseffekte im Bereich der IKT-Sicherheit über die Grenzen der öffentlichen Verwaltung hinweg zu identifizieren und nutzbar zu machen. Der Informationsaustausch auf dieser Ebene adressiert primär den strategischen Sektor und ist nicht als ein operativer Zusammenschluss zu sehen Der nationale CERT-Verbund soll dazu dienen den Erfahrungs- und Informationsaustausch zwischen den einzelnen CERT-Betreibern zu ermöglichen. Ebenso dient er Organisationen, welche sich in der Aufbauphase eines CERTs befinden als Anlaufpunkt um Unterstützung in der Aufbereitung der einzelnen CERT-Prozesse und der Vernetzung zu erhalten. (vgl. Bericht Internet Sicherheit Österreich 2012, http://www.cert.at/static/downloads/reports/cert.at-jahresbericht-2012.pdf, aufgerufen am 15.10.2013).

Schwerpunkte dieses Austausches sind:

- Best Practices/Methoden
- Einsatz von Hard- und Software
- Nationale und internationale Initiativen im CERT-Umfeld
- Finden von nationaler Expertise in spezifischen Bereichen

5.4 GovCERT.at

Das folgende Kapitel beschreibt das österreichische GovCERT als beispielgebende Etablierung eines österreichischen CERTs. Der Autor geht dazu detailliert auf das definierte Leistungsspektrum, die Aufgaben und Services, sowie auf die nationale CERT-Koordinationsrolle ein.

Das österreichische Government Computer Emergency Response Team GovCERT.at wurde 2008 auf Initiative des Bundeskanzleramtes in Kooperation mit der Firma NIC.at, der österreichischen Registrierungsstelle für die Top Level Domain .at, als erste nationale Public-Private-Partnership im Cyber Security Kontext gegründet.

GovCERT.at vereint hierbei das strategische Know-How und die koordinierende Kompetenz des Bundeskanzleramtes mit den technischen Ressourcen und der technische Qualifikation der Mitarbeiter der Firma NIC.at.

5.4.1 Zielgruppe des GovCERT.at

Wie bereits in Kapitel 5.1.1 erläutert, agieren CERTs zielgruppenorientiert. Als staatliches CERT adressiert das GovCERT.at auf der operativ die österreichische Verwaltung auf allen Ebenen (vgl. Mischitz Timo, ACOnet-Roadshow, 2008):

- Bundesministerien und nachgeordnete Dienststellen
- Oberste Organe
- Bundesländer
- Städte und Gemeinden
- Private Unternehmen mit staatlichen Funktionen

5.4.2 Leistungsspektrum des GovCERT.at

Das Leistungsspektrum des GovCERT.at besteht aus einer Reihe von präventiven, reaktiven und qualitätssichernden Diensten (vgl. govcert.gv.at, letzter Aufruf am 15.10.2013):

- Behandlung eines sicherheitsrelevanten Vorfalles
  - Analyse des Vorfalls
  - Aufbereitung von Gegenmaßnahme
  - Informationsverteilung an die Zielgruppe

- Vorbeugende Maßnahmen:
  - Mechanismen zur Früherkennung
  - Vorbereitung von Gegenmaßnahmen für Notfälle
  - Koordinierung von themenspezifischen Arbeitsgruppen

- Qualitätssichernde Maßnahmen:
  - Aufbereitung von Awareness-Maßnahmen
  - Öffentlichkeitsarbeit und Awarenesstätigkeit

5.4.3 Aufgaben und Services des GovCERT.at

Im Rahmen dieser Leistungen zum Schutz der Informationsinfrastruktur bietet das GovCERT.at seiner Zielgruppe eine Reihe von Aktivitäten an. Diese reichen von proaktiven Services über Unterstützungsleistung vor Ort im Anlassfall bis hin zum Aufbau und Koordination von IT-Notfallstrukturen. Das folgende Kapitel beschreibt dazu die wichtigsten Services und Aufgaben des österreichischen GovCERT.

Anonymisierungsstelle

Eine der Hauptaufgaben des GovCERTs ist die einer Anonymisierungsstelle für betroffene Organisationen, die ihre Erfahrungen und Informationen zu sicherheitstechnischen Vorfällen mit anderen teilen möchten, ohne selber

öffentlich in Erscheinung treten zu müssen. Betroffene können sich hierzu über die etablierten Kontaktmöglichkeiten an die Mitarbeiter des GovCERT wenden und einen Sicherheitsvorfall melden. Das GovCERT anonymisiert die Informationen und schickt eine Vorfallsmeldung mit den technischen Angriffsvektoren und möglichen Erkennungsmustern an die Teilnehmer.

IT-Feuerwehr

Im Falle einer Kompromittierung von IKT-Systemen mit Schadsoftware, die sich rasch über weite Teile der Infrastruktur ausbreitet, hat sich gezeigt, dass die Betroffenen kurzfristig eine große Anzahl von qualifizierten Fachkräften für die Beseitigung des Problems benötigen. In der Regel können diese Ressourcen nicht eigenständig in der benötigten Menge und vor allem zeitnahe aufgestellt werden.

Das GovCERT.at hat daher bereits 2009 die Initiative der freiwilligen IT-Feuerwehr gestartet. Dazu wurden in den Teilnehmerorganisationen die IT-Sicherheitsverantwortlichen kontaktiert und um eine freiwillige Einmeldung von Fachpersonal ersucht. Dieser Personenpool kann die betroffene Organisation im Bedarfsfall über das GovCERT.at aktiviert werden.

Schwachstellenanalyse

Bereits vor den ersten Aktivitäten der Anonymous Hacktivisten standen die Websites der öffentlichen Verwaltung als digitale Repräsentanz im Internet im Fokus von Angriffen. Heutige Websites bieten durch die Unterstützung von ausführbarem Programmcode bereits eine Fülle von Möglichkeiten, um eine Interaktion zwischen Benutzer und Website zuzulassen. Diese Funktionalitäten stellen jedoch zusätzliche Angriffsflächen dar, die zumeist in Form von Cross Site Scripting (vgl. National Institute of Standards and Technology Interagency or Internal Report 7298r2, S.56) - oder SQL Injection-Attacken (vgl. http://cwe.mitre.org/data/definitions/89.html, aufgerufen am 15.10.2013) ausgenutzt werden.

GovCERT.at bietet als präventive Maßnahme ein kostenloses Service an, um die bestehenden Websites automatisiert auf Schwachstellen untersuchen zu lassen – einen sogenannten Website-Check. Die Ergebnisse der Überprüfung werden mit dem Betreiber der Website besprochen und gegebenenfalls Maßnahmen zur qualitativen Erhöhung der Sicherheit gemeinsam eingeleitet.

Defacement-Überwachung

Eine weitere, öffentlichkeitswirksame Attacke ist das Defacement von Websites. Dabei werden Websites gehackt und die Inhalte durch andere Inhalte ersetzt. Nachdem diese Attacke für alle Internetbenutzer leicht erkennbar ist, ist der Imageschaden in solchen Fällen hoch. Um diese Form von Angriffen rasch zu erkennen und die betroffenen Organisationen zu informieren, wird seitens GovCERT.at die .gv.at-Domäne im Internet permanent nach Defacements gescannt. Abbildung 10 zeigt ein aktuell häufig anzutreffendes Motiv für ein gelungenes Defacement.

Abbildung 8: Defacement-Logo von Anonymous[23]

23

http://diepresse.com/images/uploads/0/d/0/680144/orfgebuehren_anonymous_kapern_gishomepage_tmp20110722112126.jpg aufgerufen am 15.10.2013

Koordination themenspezifischer Arbeitskreise

GovCERT.at bietet für die IKT-Sicherheitsverantwortlichen der öffentlichen Verwaltung die Plattform zum Erfahrungs- und Informationsaustausch. Auf Wunsch der Teilnehmer koordiniert das österreichische GovCERT themenspezifische Arbeitskreise. Die Teilnehmer bringen dazu bereits ein detailliertes Experten-Know How in diversen Spezialmaterien ein, wie zum Beispiel Awarenessbildung, Firewalls, Forensik, ISO[24]-Zertifizierungen, etc. Um diesen Wissenspool bestmöglich zu nutzen, werden themenspezifische Arbeitskreise gegründet. Das Einzelwissen wird somit dem gesamten GovCERT-Teilnehmerkreis zugänglich gemacht und eine gemeinsame Wissensbasis etabliert.

So wurde im Jahr 2011 eine GovCERT-Arbeitsgruppe zum Thema Informationssicherheits-Managementsystem gegründet. Angesichts der zunehmenden Bedeutung der IKT für die Verarbeitung der umfassenden Informationen und das ordnungsgemäße Funktionieren der IKT-unterstützten Verfahren der öffentlichen Verwaltung besteht für diese die Verpflichtung, eine angemessene und nachhaltige Informationssicherheit zu gewährleisten.

Mehr als 13 Teilnehmervertreter tauschen in dieser Arbeitsgruppe das bisher erarbeitete Wissen und die gewonnenen Erfahrungen aus dem täglichen Betrieb aus. Ein erstes Ergebnis aus dieser Arbeitsgruppe ist die Veröffentlichung der Informationsunterlagen „GovCERT Einführung eines Informationssicherheits-Managementsystems“ (vgl. http://www.ref.gv.at/uploads/media/TOP-10_GovCERT__Einfuehrung_eines_Informationssicherheits-Managementsystems.pdf, aufgerufen am 15.10.2013).

[24] Internationale Organisation für Normierung

Weitere Aktivitäten

Weitere aktuelle Aktivitäten sind:

- GovDNS – Betrieb einer sicheren, geschützten Instanz des Domain Name Service für die öffentliche Verwaltung
- Aufbereitung von Sensibilisierungs-Foldern „Sind Sie sicher“[25]

5.4.4 GovCERT.at als internationale Kontaktstelle

Das GovCERT.at als CERT der öffentlichen Verwaltung nimmt aufgrund dieser Funktion in der nationalen CERT-Landschaft eine Sonderstellung ein. Zusätzlich zu den allgemeinen CERT-Aufgaben ist das GovCERT.at die österreichische Kontaktstelle für ausländische Regierungen und internationale Organisationen zu Fragen der IKT-Sicherheit und Cyber Security.

In dieser Funktion vertritt GovCERT.at Österreich bei folgenden Institutionen:

- Europäische Agentur für Netz- und Informationssicherheit[26]
- United Nations - International Multilateral Partnership Against Cyber Threats[27]
- Generalsekretariat des Europäischen Rates[28]
- European Government CERT Group[29]

ENISA

Die Europäische Agentur für Netz- und Informationssicherheit ist eine Agentur der Europäischen Union und gilt als die erste Anlaufstelle für Fragen der IKT- und Informationssicherheit im europäischen Raum.

---

[25] http://www.lsr-ooe.gv.at/pdf_doc/erlass_2012/rs160112_Hackerangriffe_auf_Bildungseinrichtungen_Folder.pdf
[26] ENISA, vgl. www.enisa.eu
[27] IMPACT, vgl. www.impact-alliance.org
[28] GSC, vgl. ec.europa.eu/dgs/secretariat_general/index_en.htm
[29] EGC, vgl www.egc-group.org/

GovCERT.at ist der Ansprechpartner für die Europäischen Union und deren Organe zu Fragen, die die CERT-Thematik betreffen. GovCERT.at ist daher in einigen internationalen Arbeitsgruppen und Workshops der ENISA vertreten, zum Beispiel in „Cooperation Law Enforcement and CERTs“ und nimmt auch regelmäßig an den weiteren Veranstaltungen teil.

IMPACT

Die International Multilateral Partnership Against Cyber Threats ist eine Organisation der Vereinten Nationen - der International Telecommunication Union – und bildet den operativen Teil im Bereich Cyber Security. IMPACT bietet ein zentrales Portal zu den aktuellen Bedrohungen im internationalen Cyber Space und ein reichhaltiges Fortbildungsprogramm im sicherheitstechnischen Bereich. Diese Fortbildungsprogramme werden allen teilnehmenden Organisationen aus dem GovCERT zugänglich gemacht. GovCERT.at ist seit 2009 aktives IMPACT-Mitglied.

Generalsekretariat des Europäischen Rates

Das Generalsekretariat des Europäischen Rates betreibt unter anderem auch einige IKT-Netzwerke für den Austausch von klassifizierten Informationen gemäß dem geltenden Informationssicherheitsgesetz (vgl. Informationssicherheitsgesetz, www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003054, abgerufen am 15.10.2013). Zum Schutz dieser gesicherten Infrastruktur wurde ein spezielles Meldeverfahren bei sicherheitsrelevanten Vorfällen aufgesetzt. Diese Informationen werden zwischen den Mitgliedstaaten der Europäischen Union ausgetauscht und auch national an die relevanten Teilnehmer verteilt. GovCERT.at ist im Falle einer Kompromittierung der Informationen oder der Infrastruktur der nationale und internationale Ansprechpartner für Österreich.

European Government CERT Group

Die Europäische Governmenct CERT Group ist eine informelle Vereinigung der nationalen GovCERTs aus dem europäischen Raum. Hierbei handelt es sich um ein Gremium von GovCERT-Vertretern, das auf einer etablierten Vertrauensbasis beruht. Primär werden in dieser Gruppe Informationen und Erfahrungen zu aktuellen Sicherheitsvorfällen ausgetauscht. Ein weiterer Schwerpunkt ist das Finden von Expertise für spezifische Aktivitäten, zum Beispiel Domain Name Service (vgl. Mockapetris, 1987), Malware Analyse (vgl. National Institute of Standards and Technology Interagency or Internal Report 7298r2, S.122), IT-Forensik (vgl. ebd., S45), etc., die den anderen Teilnehmern im Anlassfall zur Verfügung gestellt werden kann. GovCERT.at ist seit 2010 aktives Mitglied dieser Vereinigung.

5.4.5 Nationale Koordination

Aufgrund der in den Kapitel 5.4.3 und 5.4.4 angeführten Aufgaben und Aktivitäten übernimmt das GovCERT.at im Falle einer Cyber-Notfallsituation die Funktion einer Koordinationsplattform.

Über das GovCERT.at werden sowohl die nationalen, als auch die internationalen Informationen zu sicherheitsrelevanten Vorfälle aus öffentlichen und nicht öffentlichen Quellen gesammelt, analysiert und aufbereitet. Die aufbereiteten Informationen werden zeitnah den Teilnehmern zur Verfügung gestellt.

In Absprache mit den Betroffenen werden geeignete Gegenmaßnahmen entwickelt, welche einer Auf nationaler Ebene stellt GovCERT.at im Anlassfall die nationale Koordinationsplattform für die öffentliche Verwaltung und die Betreiber der kritischen Infrastruktur dar (vgl Mischitz Timo, GovCERT.at und CERT.at Information an die Mitglieder des Datenschutzrates, http://www.bka.gv.at/DocView.axd?CobId=45271, aufgerufen am 15.10.2013)
.

5.4.6 Cyber-Übungen

Wie bereits im Kapitel 1.2 erwähnt, ist das Bedrohungsfeld im Cyber Space breit und die Risiken vielfältig. Um diesen Bedrohungen und Risiken auch im Anlassfall entgegentreten zu können, müssen die aufgebauten Fähigkeiten, System und Prozesse regelmäßig in Cyber-Planspielen geübt werden.

Dabei steht sowohl das Testen der organisationsinternen Abläufe, aber auch das Zusammenspiel der einzelnen nationalen und internationalen Akteure im Vordergrund. Bereits seit 2010 hat GovCERT.at in diesem Bereich daher ein umfassendes und detailliertes Wissen im Bereich der Cyber- Übungen aufgebaut.

Seit 2010 hat das GovCERT.at bereits an folgenden Übungen teilgenommen:

- US Cyberstorm III[30]
- Cyber Europe 2010[31]
- EU-US Exercise - Cyber Atlantic 2011
- EuroCybex 2011
- Lükex 2011
- Cyber Europe 2012

US Cyberstorm III

Die US Cyberstorm III im Jahr 2010 war die erste internationale Übung an der ein Vertreter des österreichischen GovCERT.at als Beobachter teilnahm. Cyberstorm III war bereits die dritte Cyber-Übung der Vereinigten Staaten von Amerika. Ziel dieser Übung war die Überprüfung der operativen Zusammenarbeit der einzelnen nationalen Organisationen zum Schutz des Cyber Space. Ein Angriffsvektor war dabei die Störung des Vertrauens der Benutzer in das Internet. Die Hauptangriffsszenarien waren dabei die Kompromittierung des Domain Name Systems und der Zertifikatsinfrastruktur.

[30] Vgl. http://www.dhs.gov/files/training/gc_1204738275985.shtm
[31] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010/ce2010report/

Abgesehen von den Bundesbehörden nahmen 12 internationale Partner und 60 private Unternehmen an dieser US-nationalen Cyber-Übung teil (vgl. http://www.dhs.gov/cyber-storm-securing-cyber-space, aufgerufen am 15.10.2013).

Cyber Europe 2010

Die Cyber Europe 2010 war die erste Pan-Europäische Cyber-Übung in Europa. Ziel dieser Übung war das Testen der länderübergreifenden Krisenkommunikation im Anlassfall. Für das österreichische GovCERT.at war die Teilnahme die erste aktive Beteiligung an einer Cyber-Übung (vgl. ENISA, CYBER EUROPE 2010 – EVALUATION REPORT, 2011).

Abbildung 11 skizziert das angenommen Szenario, die fiktive Annahme der internationalen Vernetzung und der Ausfall der internationalen Leitungen. Hierbei war es die Aufgabe der CERTs, die entsprechenden nationalen und internationalen Partner ausfindig zu machen und gemeinsame Ausfallswege zu definieren.

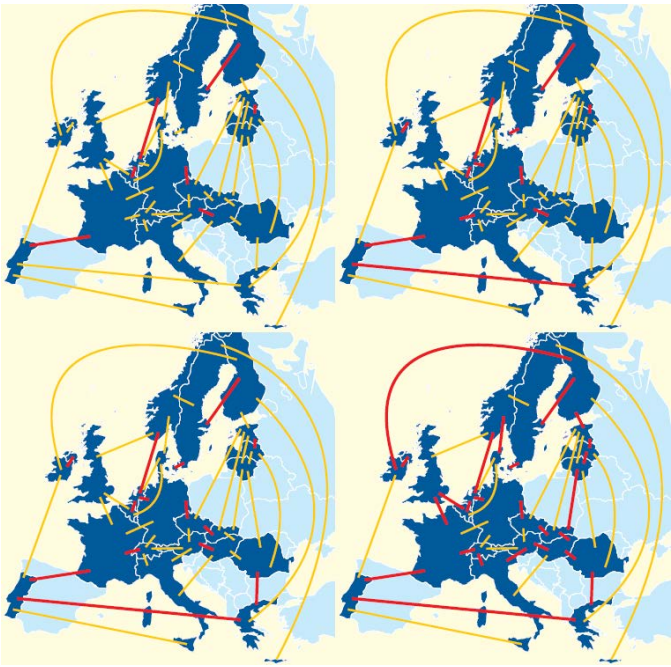

Abbildung 9: Übungsannahme Cyber Europe 2010

Cyber Europe 2012

2012 wurde auf Basis der gewonnenen Erkenntnisse der Cyber Europe 2010 erneut eine pan-europäische Übung ausgerichtet. Im Unterschied zur vergangenen Übung lag der Schwerpunkt der Cyber Europe 2012 folgenden drei Zielerreichungen (vgl. ENISA, Cyber Europe 2012
Wichtigste Erkenntnisse und Empfehlungen, 2012, S. 4):

1. Testen der Wirksamkeit und Skalierbarkeit von Mechanismen, Anweisungen und Informationswegen für die Zusammenarbeit öffentlicher Behörden in Europa
2. Untersuchen der Zusammenarbeit zwischen öffentlichen und privaten Interessengruppen in Europa
3. Ermitteln von Lücken und Herausforderungen in Bezug auf den wirksameren Umgang mit Netzstörungen großen Ausmaßes in Europa. Einbindung der privaten Unternehmen in die nationalen Krisenkommunikationsabläufe

Auch die österreichische Beteiligung an der Übungsplanung intensiviert. So war Österreich nicht nur im Planungsgremium der Übungsvorbereitung vertreten, sondern gestaltete einen eigenen nationalen Übungsteil in Abstimmung mit den nationalen Szenario. Erstmalig für die österreichischen Übungsteilnehmer war auch, dass nicht nur das koordinative Element in der Übung bespielt wurde, sondern auch die technische und mediale Ebene eingebunden wurde (vgl. http://www.ots.at/presseaussendung/OTS_20121004_OTS0118/nationale-cyber-exercise-ceat-2012-und-pan-europaeische-exercise-cyber-europe-2012, aufgerufen am 15.10.2013)

Weitere Cyber-Übungen

Ebenso war das GovCERT.at bei der ersten transatlantischen Cyber-Übung, der Cyber Atlantic 2011 als aktiver Teilnehmer vertreten. Weiters war das GovCERT.at 2011 bei der Übung EuroCybex als aktiver Spieler vertreten und nahm am Beobachterprogramm der deutschen Cyber-Krisenübung Lükex teil.

6 Auswertung der Experteninterviews

In dem vorliegenden Kapitel werden die durch die Experteninterviews gewonnenen Daten dargestellt. Zu Beginn des Kapitels werden die im Rahmen der Aufarbeitung der Experteninterviews erarbeiteten Kategorien dargestellt und erörtert. Weiters folgt eine Darstellung der gewonnenen Erkenntnisse in den einzelnen Kategorien und Unterkategorien.

Im Zeitraum Jänner bis Februar 2014 wurden durch den Autor sechs Experteninterviews durchgeführt. Die Interviews wurden für die weitere Verarbeitung anonymisiert. Im Rahmen der Bearbeitung der Einzelinterviews nach Mayring, siehe Kapitel 3 Methoden, haben sich folgende Hauptkategorien herausgebildet:

- Verarbeitung von sensiblen Daten an Schulen
- IT-Sicherheitsrisiken an Schulen
- Schutzmaßnahmen und Kontrolle
- Potentiale und Handlungsempfehlungen für ein Schul-CERT

Im Zuge der Verdichtung der aus den Experteninterviews gewonnenen Informationen hat es sich als sinnvoll herausgestellt, die Hauptkategorien noch in Unterkategorien zu gliedern um eine klarere Struktur für die Verschriftlichung sowie eine bessere Lesbarkeit der Inhalte zu gewährleisten.

6.1 Verarbeitung von sensiblen Daten an Schulen

Die Kategorie Datenverarbeitung an Schulen beinhaltet alle Aussagen der Interviewpartner im Zusammenhang mit der Speicherung, dem Zugriff und der Verarbeitung von schulspezifischen Daten sowie über geltende rechtliche Regelungen im Umgang mit diesen Daten.

Die Kategorie untergliedert sich in drei Teilkategorien:

- Daten im Verwaltungsbereich
- Daten im pädagogischen Bereich
- Gesetze und Richtlinien

6.1.1 Daten im Verwaltungsbereich

Die Unterkategorie Daten im Verwaltungsbereich befasst sich mit den Ausführungen der Fachexperten über die administrative Verarbeitung von Schuldaten. Im Folgenden wird ein Überblick über die unterschiedlichen sensiblen Verwaltungsdaten gegeben und die Frage der automatisierten Verarbeitung beantwortet.

Unter dem Verwaltungsbereich verstehen die Fachexperten jenen, in der Regel gut abgeschotteten, Bereich der Schulverwaltung, in dem die administrative Verarbeitung der Schuldaten automatisiert verarbeitet werden. Es sind sich die Experten einig, dass im Verwaltungsbereich die sensibelsten Daten der Schule zu finden sind.

Zu den Verwaltungsdaten zählen Abrechnungsdaten der Lehrer, welche sowohl personenbezogene Daten enthalten als auch die aktuellen Lohnverrechnungsdaten. Ein Großteil der Interviewpartner sieht diese Daten als sensibel an.

Weiters zählen zu den Verwaltungsdaten die Stammdaten der Schüler, welche eine Reihe von sensiblen personenbezogenen Informationen (unter anderem Adressen, Geburtsdaten, und so weiter) beinhalten. Eine Besonderheit bei den Stammdaten der Schüler ist, dass zu den personenbezogenen Schülerdaten auch sensible Informationen über Dritte verarbeitet werden. Dabei kann es sich um sensible Daten der Eltern beziehungsweise der Erziehungsberechtigten handeln, wie zum Beispiel Informationen über die aktuelle Familiensituation (zum Beispiel Scheidung, und Information über mögliche Vormundschaften).

Eine zentrale Applikation für den Schulalltag ist den Expertenaussagen nach das elektronische Klassenbuch. Obwohl es keine verpflichtende Auflage gibt, dass ein Klassebuch online verfügbar sein muss, bieten immer mehr Schulen dieses Service für Eltern, Lehrer und Schüler an. Im elektronischen Klassenbuch werden Informationen zum Stundenplan, Vertretungsplan und

Absenzen von Schülern gespeichert und bietet so den Erziehungsberechtigten die Möglichkeit sich online über den Schulalltag des Schülers zu informieren.

Die Verarbeitung der Daten im Verwaltungsbereich erfolgt entweder mittels dezentralen Services, welches in der Schule oder bei einem externen Dienstleister betrieben wird, oder über ein zentral bereitgestelltes Service.

Ein Beispiel für ein dezentrales Service ist das elektronische Klassenbuch. In der Regel wird das elektronische Klassenbuch als Internet-Service mit Benutzerauthentifizierung angeboten, um einen möglichst einfachen Einstieg zu ermöglichen. Laut Expertenaussagen wird es oft selber durch den EDV-Kustos der Schule betrieben und gewartet.

Als zentrales Service bietet das Fachministerium, das Bundesministerium für Bildung und Frauen, die Verwaltung der Lehrerdaten über SAP an. Zentrale Services werden in der Regel durch einen Dienstleister gehostet und betrieben. Laut Expertenaussagen ist der Trend zu beobachten, dass auch die Stammdaten der Schüler zentral verwaltet werden sollen.

6.1.2 Daten im pädagogischen Bereich

Die Unterkategorie Daten im pädagogischen Bereich beschreibt die Verwendung von Daten im Unterricht und in unterrichtsnahen Bereichen.

Im Gegensatz zum sensiblen Verwaltungsbereich werden pädagogische Daten in einem technisch nicht stark abgesicherten und regulierten Bereich verarbeitet. Die in diesem Bereich zu verarbeitenden Daten werden als Informations- und Wissensmanagement-Service betrieben und dienen der Wissensvermittlung. Es ist daher notwendig, dass dem Benutzer ein flexibler Zugang zu den Inhalten gewährleistet wird, und auch Raum für die Erprobung von neuen pädagogischen Zugangsmöglichkeiten gelassen wird.

Für die Wissensvermittlung werden klassische Lernplattformen eingesetzt, wie zum Beispiel Moodle, welche als Kollaborationswerkzeuge zwischen Lehrer und Schüler sowie zwischen Schüler und Schüler eingesetzt werden. Sie bieten die

Möglichkeit, Lerninhalte abzuspeichern, Einzel- und Gruppenarbeiten durchzuführen und auch Tests zu absolvieren.

Laut Expertenaussagen ist auch ein Trend zur Nutzung von öffentlichen Cloud-Services zu sehen. Aufgrund der hohen Convenience- und Usability-Faktoren greifen sowohl Schüler, als auch Lehrer immer öfter zu Cloud-Lösungen wie Dropbox, Google und ähnlichem um Unterrichtsmaterialien auszutauschen. Auch der Wissenstransfer erfolgt oft digital über soziale Medien. So organisieren sich Lerngruppen über Facebook und Whatsapp um sich rasch und bequem über Lösungswege zu den gestellten schulischen Aufgaben auszutauschen.

6.1.3 Gesetze und Richtlinien

Unterkategorie Gesetze und Richtlinien umfasst alle Aussagen der Experten zu den geltenden gesetzlichen Rahmenbedingungen zur Speicherung, Verarbeitung und Weitergabe von sensiblen Daten an österreichischen Schulen.

Die Befragung der Experten zeigt, dass ein Gutteil der als sensibel einzustufenden Daten unter das Datenschutzgesetz fallen. Das Datenschutzgesetz, siehe http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597 (letzter Aufruf am 04.03.2014), regelt den Umgang mit personenbezogenen Daten für Dienstleister, Auftraggeber und Betroffene. Alle Expertenmeinungen weisen darauf hin, dass das Datenschutzgesetz das wichtigste Materiengesetz in diesem Zusammenhang ist. Im Anwendungsfall Schule ist als Auftraggeber der Schulerhalter, vertreten durch den Direktor, als Dienstleister die Schule oder der IT-Partner der Schule und als Betroffene die Lehrer, Schüler und gegebenenfalls deren Angehörige zu verstehen.

Einzelne Expertenmeinungen verweisen auch auf das Beamtendienstrecht § 46 (1), welches speziell für alle Bediensteten der öffentlichen Verwaltung die Amtsverschwiegenheit regelt, siehe http://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR12102777/NOR12102

777.html (letzter Aufruf am 04.03.2014). Die Amtsverschwiegenheit besagt, dass ein öffentlich Bediensteter zur Verschwiegenheit über jegliche Information verpflichtet ist, die er im Rahmen seiner beruflichen Tätigkeiten erfährt, sofern ein berechtigtes Interesse daran besteht.

Als ein weiterer regulatorischer Rahmen wird der Digitale Schulerlass „Digitale Kompetenz an Österreichs Schulen“ aus dem Jahr 2010 seitens einiger Experten angeführt. Dieser Erlass enthält Empfehlungen seitens des Fachministeriums, das Bundesministerium für Bildung und Frauen, für die Bildung von digitaler Kompetenz an den österreichischen Schulen und gibt Handlungsanweisungen für eine sichere Nutzung von neuen Medien in der Verwaltung und im pädagogischen Bereich. Es wurde von wenigen Experten festgehalten, dass die Empfehlungen zu wenig Bezug zu den tatsächlichen Schulbedingungen haben, und die Umsetzung daher in der Realität zumeist schwer möglich ist.

Es waren sich alle Experten einig, dass die Umsetzung von Handlungsempfehlungen und die Einhaltung der rechtlichen Rahmenbedingungen immer sehr stark von der Führungskraft der Schule abhängig ist. Die Gewährleistung der Datensicherheit an den österreichischen Schulen ist eine Führungsaufgabe. Die Verantwortung für die Umsetzung von Sicherheitsmaßnahmen, der Einhaltung der gesetzlichen Verpflichtungen und der Kontrolle hat der Schuldirektor/die Schuldirektorin.

6.2 IT-Sicherheitsrisiken an Schulen

Die Kategorie IT-Sicherheitsrisiken an Schulen umfasst alle grundlegenden Aussagen der Experten im Hinblick auf mögliche Sicherheitsrisiken auf Österreichs Schulen im Verwaltungs- und Pädagogik-Bereich.

Die Kategorie ist in folgende drei Unterkategorien gegliedert:

- Risiken an Schulen
- Angreifer und deren Motivation
- Computerklassen und Bring Your Own Device

6.2.1 Risiken an Schulen

Die Unterkategorie Risiken an Schulen beschreibt die wesentlichsten IT-Sicherheitsrisiken, welche auf die IT-Infrastruktur einer Schule wirken. Sie umfasst sowohl technische, als auch organisatorische Risiken, welche die Experten im Rahmen der Interviews angeführt haben.

Alle Experten weisen darauf hin, dass der Umgang mit pädagogischen und Verwaltungsdaten an österreichischen Schulen unkritisch gesehen wird. Das lässt darauf schließen, dass ein Großteil der Lehrer und Schüler keine Awareness hinsichtlich der Schutzwürdigkeit der Daten haben. Einige Experten meinen, dass dies auf den Umstand zurückzuführen ist, dass sicherheitstechnische Maßnahmen, wie zum Beispiel ein regelmäßiger Passwortwechsel, nicht den Usability-Anforderungen der Benutzer entsprechen.

Weiters gehen die Experten davon aus, dass es aktuell zu einer Verschiebung des Begriffes „sensible Daten“ im allgemeinen Sprachgebraucht kommt. Sensible Daten im Sinne des Datenschutzgesetzes werden von dem Schüler nicht als schutzwürdig angesehen und werden im alltäglichen Gebrauch der neuen Medien mitgeteilt und ausgetauscht. So gibt der Lehrer auch schulsensible Daten, wie zum Beispiel Beurteilungsnoten, über soziale Medien seinen Schülern bekannt. Die Experten weisen darauf hin, dass das fehlende Bewusstsein über die Sensibilität dieser Daten auch das Profiling von schulnahen Personen wie Lehrern und Schülern vereinfacht. Einige Experten sind der Meinung, dass schulspezifische Daten eine gute Datenbasis für ein Personen-Profiling darstellen.

Als ein weiteres Risiko sehen die Experten den Bereich des Identitätsdiebstahls. Der Zugriff auf IT-Services an Österreichs Schulen erfolgt in der Regel mittels personengebundenen Benutzernamen und Passwort. Der Benutzername und das Passwort sind zumeist für alle IT-Services gleich. Auch wenn das pädagogische Netz und das Verwaltungsnetzwerk physikalisch getrennt sind, werden aufgrund einer gewünschten einfachen Bedienung durch

die Benutzer die gleichen Passwörter verwendet. Ein weiterer Faktor ist, dass gerade im Schulbereich wenige Geräte durch eine große Anzahl von Benutzern verwendet werden. Das bedeutet, dass es oft zu Benutzerwechseln kommt, was die Gefahr eines Identitätsdiebstahls erhöht. So ist die Wahrscheinlichkeit groß, dass ein Benutzer sich nicht ordnungsgemäß vom System abgemeldet hat, und fremde Personen auf das Benutzerprofil Zugriff erlangen. Laut Aussagen der Experten ist es auch möglich, dass ein Benutzer beim Anmeldevorgang beobachtet wird, und so der Benutzername und das Passwort bekannt werden.

Gerade im pädagogischen Netzwerk sehen Experten ein großes Risikopotential. Es besteht die Gefahr, dass das Schulnetzwerk für illegale Zwecke missbraucht wird. So kann der Internetzugang der Schule dazu verwendet werden, um illegale Inhalte wie beispielsweise Filme herunterzuladen. Hier orten einige Experten fehlendes Problembewusstsein bei Schülern hinsichtlich der Verletzung des geltenden Urheberrechtes.

Im Unterricht haben Schüler oftmals Zugriff auf das verwendete Unterrichtsmaterial. Laut Experten kann das zu Risiken in der Durchführung des Unterrichts führen. Schüler können das Unterrichtsmaterial verändern und somit die Integrität der Daten verletzen.

Auch in der Unterrichtsgestaltung orten einige Experten Risiken. Während des Unterrichts werden Smartphones und Tablets oft verwendet, um parallel zum Vortrag der Lehrkraft die Inhalte des Unterrichts zu überprüfen. Das führt oft zu einer Ablenkung der Schüler und zu unerwünschten Störungen in der Durchführung des Unterrichts. Ein generelles Risiko sehen einige wenige Experten darin, dass vor der Nutzung neuer Technologien im Unterricht keine Überlegungen hinsichtlich der formalen Rahmenbedingungen, wie ein neues Medium sinnstiftend eingesetzt werden kann, erfolgt.

Von den Experten wird auch das Risiko durch den Einsatz von neuen Medien als alternative Schummelmethode unterstrichen. So können zum Beispiel Aufgabenergebnisse und Lösungswege während eines Tests durch moderne

Messenger-Programme ausgetauscht werden. Durch die fast unüberschaubare Anzahl von Möglichkeiten, sich digital zu vernetzen, hat die Lehrkraft fast keine Chance dem Schummeln Einhalt zu gebieten, außer, dass in der Prüfungsphase digitale Medien verboten sind.

Die Verfügbarkeit von Verwaltungsdaten, zum Beispiel das digitale Klassenbuch, wird von vielen Experten kritisch gesehen. Die dezentrale Bereitstellung über das Internet wird als ein Risiko wahrgenommen. Das Kompromittieren von Internet-Services erfordert laut Expertenaussagen kein Spezialwissen mehr. Viele frei verfügbare Programme ermöglichen eine automatisierte Kompromittierung, ohne dass ein Angreifer tiefergehende Kenntnisse über das angegriffene IT-System oder im Bereich des Hackings haben muss. In ähnlicher Weise sieht ein geringer Anteil der Experten dieses Risiko auch im abgeschotteten Verwaltungsbereich. Schüler können sich beispielsweise durch die Manipulation von Schulnoten einen Vorteil beschaffen.

Als generelles Risiko bewerten die Experten die große Asymmetrie des Wissensstandes im Bereich IT zwischen Schülern und Lehrern. Laut Expertenaussagen verfügen Schüler über ein weitaus größeres Know-How im Umgang mit IT und neuen Medien als der Lehrkörper und sind diesem auf diesem Feld voraus. Auch innerhalb der Lehrerschaft gibt es ein großes Wissensgefälle zwischen technikaffinen Lehrern und Lehrern mit wenig bis gar keinem Bezug zu neuen Technologien.

Ein Experte sieht speziell das Risiko, dass an Österreichs Schulen oft Eigenentwicklungen zur IT-Systemverwaltung verwendet werden, welche aktuellen Sicherheitsstandards nicht genügen beziehungsweise nicht gewartet werden. Der Experte sieht hier noch großes Entwicklungspotential im Bereich Awarenessbildung, dass auch Schulerhalter den Wert von IT-Infrastruktur und IT-Services erkennen und entsprechende Investitionen in professionelle Unterstützungsleistung tätigen müssen.

Auch ausgelagerte IT-Serviceleistungen werden von den Experten kritisch gesehen. So werden beispielsweise die Schülerbewertungen an Verlage

ausgelagert, welche die Schülerdaten verarbeiten. Bei der ausgelagerten Speicherung und Verarbeitung von schulspezifischen Daten sehen die Experten eine Vielzahl von möglichen Angriffsvektoren.

Schlussendlich ist die Mehrheit der Experten überzeugt, dass die IT-Sicherheit an Österreichs Schulen abhängig von der Awareness und Motivation des EDV-Kustos ist. Es existiert ein großer Niveauunterschied in Bezug auf IT-Sicherheit zwischen Schulen. Ein engagierter und möglichst für diese Tätigkeit freigestellter EDV-Kustos kann im Schulalltag den Unterschied zwischen einem hohen und niedrigen Niveau ausmachen.

6.2.2 Angreifer und deren Motivation

In der Unterkategorie Angreifer und deren Motivation finden sich alle Expertenaussagen dazu, in welchem Umfeld mögliche Angreifer auf ein IT-System einer Schule zu finden sind und welche Motivation möglicherweise hinter einem Angriff steckt.

Generell sehen die Experten bei möglichen Angreifern auf ein IT-System einer österreichischen Schule kein finanzielles Interesse an den Daten. Das liegt daran, dass Schulen keine wirtschaftlich interessanten Daten in großen Mengen verarbeiten. Darin unterscheiden sich Schulen zu anderen Organisationen, die wirtschaftskriminell interessante Daten wie zum Beispiel Kreditkartendaten verarbeiten. Das Interesse der Angreifer an den Daten ist daher eher persönlicher Natur.

Die Experten sehen daher die Angreifer eher aus dem näheren Schulumfeld kommen. Als mögliche Motivationsfaktoren sehen einige wenige Experten Hacktivism an, sowie die Schadensfreude an der Verunglimpfung von Websites oder am entstandenen Imageschaden.

Ehrgeiz, Kreativität und Spieltrieb sehen alle Experten als Antrieb für Angreifer von IT-Systemen an Schulen. Der Drang, neue Technologien auszuprobieren und vorhandene Sperren zu umgehen, treibt Schüler auch in schulischen

Umgebungen an, auf verbotene Dateien zuzugreifen. Dabei geht es gar nicht so sehr um die Verwertung der gewonnenen Informationen aus den Daten, sondern nur um das Beweisen, dass man einen Weg gefunden hat, die technischen Sicherheitsmaßnahmen zu umgehen.

6.2.3 Computerklassen und Bring Your Own Device

Die Unterkategorie Computerklassen und Bring Your Own Device fasst die Expertenaussagen zum Thema Verwendung von Computern im Unterricht zusammen und geht dabei im Speziellen auf die Verwendung von privaten Endgeräten ein.

Die Experten stellten einhellig fest, dass der Einsatz von Computern im Unterricht diesen bereichern kann, aber auch neue didaktische und vor allem technische Anforderungen an den Lehrerkörper stellt. So sehen Experten das Thema Verfügbarkeit von IT-Komponenten als sehr wichtig an. Sollten Computer vor oder während des Unterrichts kaputt gehen, muss der Lehrer entweder in der Lage sein, das Gerät technisch zu reparieren oder sich um ein Ersatzgerät bemühen, damit dem Schüler eine entsprechende Lernumgebung bereitsteht. Die Verfügbarkeit hat auch unmittelbare Auswirkung auf die Sicherheit der Endgeräte. Sollte ein Endgerät sicherheitstechnisch kompromittiert sein, so ist laut Aussage der Experten die Fortführung des Unterrichts wichtiger als die akute Bereinigung des Systems.

Viele Experten haben die Erfahrung gemacht, dass Österreichs Schulen IT-infrastrukturtechnisch nicht gut ausgestattet sind. Um dem entgegenzuwirken, verwenden sowohl Lehrer als auch Schüler komfortable Cloud-Services für den E-Mailverkehr, für das Abspeichern und zur Verfügung stellen von Daten im Internet und so weiter. In den Hintergrund gerät dabei das Bewusstsein, dass so auch sensible Daten über schlecht abgesicherte öffentliche Systeme ausgetauscht werden, deren Datenschutzbestimmungen nicht kompatibel mit der österreichischen Gesetzeslage ist. Weiters sehen die Experten in der unzureichenden IT-Ausstattung auch den Grund für eine notwendige Integration von Bring Your Own Device-Komponenten. Die Schüler sind dazu angehalten

ihre eigenen, privaten Endgeräte im Unterricht zu verwenden, um auf eine aktuelle Hard- und Software zurückgreifen zu können.

Ein Großteil der Experten ist davon überzeugt, dass die Verwendung von privaten Endgeräten im Unterricht eine Menge von Komplikationen für Schüler, Lehrer und IT-Administration mit sich bringt. Die Netzwerkinfrastruktur und die Internet-Anbindung sind kapazitätenmäßig nicht dafür ausgelegt eine unkontrollierbare Anzahl von Endgeräten mit Bandbreite und Rechenleistung zu versorgen. Oft wird das Netzwerk auch außerhalb des IT-geleiteten Unterrichts genutzt, um im Internet zu surfen. Um die Verfügbarkeit der Internetbandbreite für den Unterricht zu gewährleisten, sind daher spezielle Schutzmaßnahmen notwendig.

Private Endgeräte können durch den EDV-Kustos einer Schule nicht zentral administriert werden und liegen in der Systemverantwortung des Besitzers. Dem EDV-Kustos ist es daher nicht möglich, ein Mindestmaß an Sicherheit für das in Verwendung stehende Gerät zu gewährleisten. Ebenso ist es auch nicht möglich eine Kompromittierung automatisch zu erkennen und gegebenenfalls zu beheben. Die Einführung einer Bring Your Own Device-Strategie erhöht dadurch die Anzahl potentiell gefährdeter Endgeräte in der IT-Landschaft der Schule.

Verstärkte Herausforderungen sehen alle Experten in der größeren Komplexität in der Betriebsführung durch den Einsatz von Bring Your Own Device. Die Zugriffe auf die zentralen Lernplattformen müssen von allen Gerätetypen aus gewährleistet werden. Die Experten rechnen mit einem vermehrten Aufwand in der Administration der zentralen Services und der Hilfestellung bei Problemen mit privaten Endgeräten.

Konträr zu den obigen Beiträgen sieht ein Experte aber keinen Unterschied in der sicherheitstechnischen Absicherung der IT-Systeme an Österreichs Schulen. Ob nun schuleigene Endgeräte im Unterricht verwendet werden oder Bring Your Own Device Komponenten, macht laut Aussage des Experten keinen Unterschied in der Risikobetrachtung.

6.3 Schutzmaßnahmen und Kontrollen an Schulen

Die Kategorie Schutzmaßnahmen und Kontrollen beinhaltet alle Aussagen der Experten in Bezug auf die getroffenen sicherheitstechnischen Maßnahmen und die Einhaltung dieser.

Die Kategorie ist in folgende drei Unterkategorien gegliedert:

- Getroffene Schutzmaßnahmen
- Verantwortung
- Potentiale

6.3.1 Getroffene Schutzmaßnahmen

Die Unterkategorie Getroffene Schutzmaßnahmen beschreibt jene Expertenaussagen, welche sich auf den aktuell implementierten Schutz der IT-Infrastruktur an österreichischen Schulen beziehen. Dazu unterscheiden die Experten zwischen proaktiven und reaktiven Maßnahmen, sowie zwischen technischen und organisatorischen Maßnahmen.

Als eine der wesentlichsten präventiven Maßnahmen sehen alle Experten die Durchführung einer Risikoanalyse vor dem Einsatz neuer Technologien und IT-Systemen. Dabei sollen einerseits technische Sicherheitsrisiken berücksichtigt werden, andererseits auch auf die speziellen Gegebenheiten einer Schule eingegangen werden. Dazu zählen die Experten unter anderem den offenen Internet-Zugang für Schüler und die notwendige Flexibilität in der IT-gestützten Unterrichtsgestaltung.

Laut Aussage eines Experten werden an Österreichs Schulen im IT-Sicherheitsbereich sehr viele kommerzielle Produkte implementiert. Diese haben gegenüber Open-Source und Community-Produkten den Vorteil, dass Sie mehr Komfort in der Betriebsführung und mehr Unterstützung im Fehlerfall anbieten. Unterstrichen wird diese Aussage durch die Bemühungen des Fachministeriums, für die österreichischen Bundesschulen kostenlose Microsoft-Lizenzen zur Verfügung zu stellen. Gesteuert durch die IT-

Gesamtstrategie eFit21, siehe http://www.bmukk.gv.at/schulen/efit21/index.xml (zuletzt aufgerufen am 06.03.2014), koordiniert das Bundesministerium für Bildung und Frauen die Bereitstellung von Microsoft Generallizenzen über das Microsoft Austrian College und High School Agreement, siehe http://www.bmukk.gv.at/schulen/it/it_angebote/microsoft.xml (zuletzt aufgerufen am 06.03.2014).

Bei der Verwendung von privaten Endgeräten im Unterricht können diese Lizenzen jedoch nicht verwendet werden. Ebenso ist auch nicht jedes Endgerät Microsoft-kompatibel. Für diesen Einsatz kommen laut Aussage von Experten Community-Produkte zum Einsatz. Oft sehen diese Lösungen vor, dass für den Unterricht ein Live-System vom USB-Stick geladen wird, welches eine vollständige Arbeitsumgebung für den Schüler bietet. Nachdem für jeden Unterricht dieses System neu initialisiert wird, kann der Lehrer davon ausgehen, dass sich die Schüler mit einem nicht kompromittierten System im Schulnetzwerk einloggen.

Als weitere Sicherheitsmaßnahme sehen einige Experten das Sperren von infizierten Websites über einen WebProxy-Filter. Durch das Filtern von Websites soll verhindert werden, dass Schüler und Lehrer Websites ansurfen oder unbemerkt auf diese weitergeleitet werden, welche Schadsoftware verbreiten und die Endgeräte infizieren. Die entsprechenden Filterlisten werden zumeist über kommerzielle Anbieter bereitgestellt.

Ebenso wichtig ist es den Expertenaussagen nach, alle IT-Systeme einer Schule auf einen aktuellen Softwarestand mit allen relevanten Sicherheitsupdates zu bringen. Dazu ist es wichtig, dass der EDV-Kustos eine Gesamtübersicht über seine zu verwaltenden IT-Systeme hat und sich informiert, wann auf welchen Systemen Updates eingespielt werden müssen.

Die Experten sind sich einig, dass es unerlässlich ist, den Verwaltungsbereich vom pädagogischen Netz physikalisch zu trennen, um den Schülern keine Möglichkeit zu geben, auf die sensiblen Administrationsdaten zuzugreifen. Zur Sicherung der Qualität der IT-Services empfehlen einige Experten auch ein

eigenes Schüler-WLAN einzurichten, welches logisch von dem Lehrer-WLAN getrennt ist. Diese Maßnahme gewährleistet, dass die Schüler keinen Zugriff auf die nicht freigegebenen Unterrichtsdaten erhalten.

Für die technische Verarbeitung von besonders sensiblen Informationen werden laut Expertenaussagen zentrale Applikationen seitens des Fachministeriums angeboten. Diese IT-Services werden in besonders geschützten Umgebungen betrieben und durch professionelle Dienstleister gewartet. Einen weiteren Vorteil sieht ein Großteil der Experten in der Benutzerunterstützung, welche durch einen einzelnen EDV-Kustos an den Schulen nicht zeitnah gewährleistet ist.

Sollten die getroffenen Maßnahmen nicht ausreichen und das IT-System an der Schule kompromittiert werden, ist es möglich, dass der EDV-Kustos Unterstützung durch ein Kompetenzzentrum des österreichischen Schulnetzwerkes erhält. Sogenannte Clusterschulen werden durch das Fachministerium durch Förderungen im Bereich Infrastruktur und Wissenstransfer unterstützt. Diese Clusterschulen sind als themenspezifische Anlaufstellen für Schulen aufgebaut, um so einen Multiplikatoreffekt zu erzielen.

Als weitere wichtige Maßnahme sehen die Experten die aufbereiten Informationen zur Förderung der digitalen Kompetenz und Aufbau einer IT-Infrastruktur durch das Fachministerium in Form von Erlässen und Handreichungen. Insbesondere für die Verwendung von zentral betriebenen Plattformen, wie zum Beispiel der Gehaltsabrechnung des Lehrkörpers, werden seitens des Bundesministeriums für Bildung Informationsmaterial zielgruppengerecht aufgearbeitet und den Schulen zur Verteilung an die Lehrkräfte zur Verfügung gestellt.

Als eine der wichtigsten Maßnahmen sehen die Experten das Thema der Bewusstseinsbildung an. Sowohl für Schüler als auch für Lehrkräfte wird seitens der Initiative Safer Internet Informationsmaterial zielgruppengerecht aufbereitet und bei Bedarf auch von Fachexperten vor Ort geschult.

6.3.2 Verantwortung

In der Unterkategorie Verantwortung werden alle Expertenaussagen eingearbeitet, welche im Zusammenhang mit der Übertragung und Übernahme von Verantwortung in der Umsetzung von IT-Sicherheitsmaßnahmen an Österreichs Schulen stehen.

Hinsichtlich der zentralen Applikationen sind sich die Experten einig, dass die Verantwortung über die Datensicherheit bei dem zuständigen Fachministerium liegt. Dieses hat die entsprechende IT-Sicherheit zu gewährleisten und die Vertraulichkeit, Verfügbarkeit und Integrität der Datensätze sicherzustellen. Darunter fällt auch die Durchführung von regelmäßigen Risikoanalysen und die Umsetzung der daraus gewonnenen Sicherheitsmaßnahmen.

Durch das Fachministerium werden, wie bereits in der vorangegangen Unterkategorie dargestellt, Handreichungen für einen sicheren Betrieb von Applikationen und bewussten Umgang mit Schuldaten bereitgestellt. Die Experten weisen darauf hin, dass für die Bekanntmachung an der Schule und die Verteilung der Information an den Lehrkörper die Führungskraft zuständig ist. Auch die Verantwortung über die Sicherheit der Datensätze obliegt in letzter Konsequenz der Führungskraft an der Schule.

Eine wichtige Rolle kommt laut Expertenaussagen dem Schulerhalter zu. Der Schulerhalter hat dafür Sorge zu tragen, dass die seitens der Führungskraft geforderten Sicherheitsanforderungen budgetär gedeckt sind. Er ist für die Schaffung der entsprechenden formalen Rahmenbedingungen verantwortlich. Welche Sicherheitsmaßnahmen umgesetzt werden, und in welcher Art und Weise, obliegt jedoch der Führungskraft an der Schule.

Für die Einhaltung der Sicherheitsmaßnahmen im schulischen Alltag und speziell im IT-geleiteten Unterricht ist die Lehrkraft verantwortlich. Es ist die Aufgabe des Lehrkörpers, die geforderten Maßnahmen auch im Unterricht umzusetzen und auch die Einhaltung durch die Schüler zu gewährleisten. Ein

Großteil der Experten ist jedoch davon überzeugt, dass der Schwerpunkt eines Lehrers das Unterrichten ist und nicht die Administration von IT-Infrastruktur.

6.3.3 Potentiale

In die Unterkategorie Potentiale sind alle Darstellungen der Experten eingeflossen, welche Verbesserungsmaßnahmen im Bereich der Umsetzung von IT-Sicherheitsmaßnahmen darstellen, welche bis dato im schulischen Betrieb noch nicht umgesetzt wurden.

Die Experten sind sich einig, dass der Trend an Schulen zur zentralen Verwaltung von Schülerdaten geht. Es ist aus Ihrer Sicht nachvollziehbar, dass für komplexe IT-Systeme mit hohen Anforderungen hinsichtlich Integrität, Verfügbarkeit und Vertraulichkeit eine professionelle Betreuungsstruktur notwendig ist. Es ist nicht ausreichend, einmalig ein IT-Service aufzusetzen und es dann so gut wie möglich laufen zu lassen. Eine professionelle Betreuung setzt eine fortlaufende Weiterentwicklung der Systeme voraus. Veränderungen am System müssen immer hinsichtlich sicherheitstechnischer Auswirkungen auf den Gesamtbetrieb untersucht werden. Daher ist gerade bei extern betriebenen IT-Systemen ein besonderes Augenmerk auf die Gewährleistung von IT-Sicherheit zu legen.

An das Fachministerium als zentraler Ansprechpartner für den Bundesbereich richten sich die Experten mit dem Vorschlag, dass ein verstärkter Fokus auf die Konzeption von Schulungen und die Erarbeitung von technischen Handlungsempfehlungen gelegt werden soll. Weiters erachten die Experten es als wichtig, dass eine verpflichtende Lehrerfortbildung für den Einsatz von IT-Mitteln im Unterricht das technische Verständnis und das Bewusstsein für die Sensibilität der Datenverarbeitung stärkt.

Viele Experten sind der Meinung, dass die Schulen verpflichtet werden sollen im Falle einer erkannten sicherheitstechnischen Kompromittierung Säuberungsmaßnahmen einzuleiten und den Betroffenen Erste Hilfe-Maßnahmen anzubieten.

Einige Experten haben die Erfahrung gemacht, dass die Handreichungen des Fachministeriums zum Thema IT nicht der Realität an Österreichs Schulen entsprechen. Insofern ist es auch schwierig, die geforderten Maßnahmen in den schulischen Alltag zu integrieren und umzusetzen. Viele Informationen werden daher an den Schulen dem Lehrkörper kundgetan, werden dann aber aufgrund fehlender Durchführbarkeit rasch wieder vergessen. Einige Experten fordern daher, dass bei der Erarbeitung von fachlichen Handreichungen vermehrt auf die Expertise von schulnahem Fachpersonal zugegriffen wird. Auch bei technischen Fragestellungen sehen die Experten einen Aufholbedarf. Es soll eine zentrale Anlaufstelle für Schulen bereitstehen, welche bei technischen Fragen entsprechende Hilfestellungen gibt und Leitfäden erstellt.

Einige Experten kritisieren, dass die Einhaltung der geforderten Sicherheitsmaßnahmen seitens des Fachministeriums nicht kontrolliert wird. Eine regelmäßige Kontrolle wird als sinnvoll angesehen. Ein Experte sieht eine Möglichkeit zur Überprüfung in der Selbstevaluierung der Schulen im Sinne des Qualitätszyklus.

Nicht jeder Schüler hat die Möglichkeit privat kommerzielle Software zu nutzen. Um den Schülern auch das Lernen zuhause zu ermöglichen, fordern einige Experten daher, dass im Schulunterricht vermehrt auf Open-Source zurückgegriffen werden kann, welche den Schülern kostenlos zur Verfügung stehen soll. Sollte dies nicht möglich sein, müssen Schülerlizenzen bereitgestellt werden. Der Einsatz von legaler Software im Schulbetrieb und das regelmäßige Updaten von Software auch auf Bring Your Own Device Geräten erhöht die Sicherheit der gesamten IT-Infrastruktur.

Als einen wesentlichen Punkt sehen die Experten die Weiterentwicklung von zielgruppenspezifischen Awareness-Programmen für Führungskräfte an Schulen. Nur durch die Sensibilisierung der Entscheidungsträger wird es gelingen, das Thema IT und insbesondere das Thema IT-Sicherheit und Datenschutz in das Bewusstsein des Lehrkörpers, der Eltern und Schüler zu bringen. Es ist die Forderung der Experten, dass die Schule dem IT-Thema

gezielt mehr Aufmerksamkeit widmet sowie auch mehr Ressourcen für IT-Sicherheit zur Verfügung gestellt wird. Ein konkretes Potential orten die Experten bei der Lehrverpflichtung des EDV-Kustos. Um einen professionellen Betrieb eines Schulnetzwerkes zu gewährleisten ist es notwendig, dass zumindest ein EDV-Kustos Vollzeit für die Administration und den Betrieb der IT-Infrastruktur zuständig ist.

Für den pädagogischen Bereich wünschen sich die Experten allgemein mehr Flexibilität für das Lernumfeld, um den Schülern die Möglichkeit zu geben, vermehrt neue Dinge auszuprobieren und unterschiedliche Herangehensweisen an neue Technologien auszuprobieren.

Für den Einsatz von Bring Your Own Device Geräte sehen die Experten den Bedarf an einem durchdachten Backup-Konzept, um die Verfügbarkeit von Unterrichtsdaten sicherzustellen. Schüler, die wochenlang an Projektarbeiten geschrieben haben, sollen nicht durch den Ausfall einzelner IT-Komponenten die Arbeit von mehreren Tagen oder vielleicht sogar die komplette Arbeit verlieren. Durch die Etablierung eines Backup-Konzepts, welches auch die Arbeit an privaten Endgeräten berücksichtigt, kann diesem Szenario vorgebeugt werden.

6.4 Potential und Handlungsempfehlungen für ein Schul-CERT

Die Kategorie Potential und Handlungsempfehlungen für ein Schul-CERT befasst sich mit allen Aussagen der Experten zu möglichen proaktiven und reaktiven Aktivitäten und Aufgaben eines Schul-CERTs. Weiters werden Handlungsempfehlungen für die Institutionalisierung eines Schul-CERTs und Mitarbeiterprofile diskutiert.

Die Kategorie gliedert sich in folgende Unterkategorien:

- Angebote und Hilfestellungen im Anlassfall
- Aufgaben für ein Schul-CERT
- Institutionalisierung eines Schul-CERTs und Mitarbeiterprofil

6.4.1 Angebote und Hilfestellungen im Anlassfall

Die Unterkategorie Angebote und Hilfestellung im Anlassfall fokussiert sich auf alle Aussagen der Fachexperten hinsichtlich bereits verfügbarer Hilfsangebote und Anlaufstellen für Schulen im Falle einer Kompromittierung. Weiters wird darauf eingegangen, welche CERT-Strukturen in Österreich bekannt sind, und welche Aufgaben im schulischen Bereich bereits jetzt durch ein CERT wahrgenommen werden.

Im Falle einer Kompromittierung fungiert das Fachministerium als Meldestelle für Bundesschulen. Als IP-Adressenhalter für das Schulnetzwerk werden in der Regel alle Sicherheitsvorfälle an die Fachabteilung im Bundesministerium für Bildung gemeldet. Die Fachabteilung informiert die betroffene Schule über den möglichen Schaden und fungiert auch als Ansprechstelle für polizeiliche Ermittlungen. Laut Aussagen von Experten gibt es aber keine etablierte Kontaktbasis zwischen den EDV-Kustoden und dem Fachministerium. Weiters ist auch kein Incident Handling-Prozess etabliert. Weitere Unterstützungsleistungen erhalten betroffene Schulen über externe Dienstleister und die Partner des Bildungsnetzwerkes.

EDV-Kustoden tauschen sich in bundesländerspezifisch organisierten Facharbeitsgemeinschaften über das Thema IT aus. Laut Aussage der Experten beschäftigen sich diese sehr gut etablierten Plattformen intensiv mit betrieblichen und medienspezifischen Inhalten. Aufgrund der guten Vernetzung der EDV-Kustoden untereinander kann eine betroffene Schule davon ausgehen, dass sie im Anlassfall auch eine fachliche Unterstützung durch weitere EDV-Kustoden aus anderen Schulen erhält. Diese Kompetenzencluster sind jedoch von der Eigeninitiative der verantwortlichen Lehrer abhängig und erhalten keine Unterstützung aus dem Fachministerium.

Obwohl bis dato noch keine Schul-CERTs in Österreich etabliert sind und es auch keine CERT-ähnlichen Strukturen gibt, sind die Services eines CERTs im Schulbereich bekannt. Von EDV-Kustoden werden vereinzelt die Services des nationalen CERT.at genutzt. So stehen die öffentlichen Feeds und Mailinglisten

den EDV-Kustoden zur Verfügung, um sich über aktuelle Sicherheitsprobleme in Hard- und Software zu informieren oder um eine tagesaktuelle Zusammenfassung an relevanten Internetartikeln zum Thema IT-Sicherheit zu erhalten. Ein operativer direkter Kontakt zwischen Schulen und CERTs ist den Experten jedoch nicht bekannt.

6.4.2 Aufgaben für ein Schul-CERT

Die Unterkategorie Aufgaben für ein Schul-CERT fasst alle Aussagen der Fachexperten zu proaktiven und reaktiven Maßnahmen eines Schul-CERTs zusammen. Hierbei wird zwischen technischen und organisatorischen Hilfestellungen und Aufgaben unterschieden.

Für die Experten steht als primäres Aufgabengebiet eines Schul-CERTs die Etablierung von proaktiven Aufgaben im Vordergrund. Dazu wird vorgeschlagen, dass ein Schul-CERT die Konzeption der IT-Sicherheitsausbildung für EDV-Kustoden übernimmt. Diese Ausbildungen sollen durch Kurse oder Tagungen in regelmäßigen Abständen angeboten werden.

Einen großen Bedarf sehen die Experten bei der zielgerichteten Aufbereitung von Informationen zum Thema IT-Sicherheit an den Lehrkörper und an Führungskräfte. Vorstellbar ist hier die konzeptionelle Entwicklung von Know How-Transfers im Bereich Datenschutz für Lehrende, welche diese Informationen in den Unterricht einfließen lassen können.

Aus technischer Sicht sehen die Experten ein großes Potential für ein Schul-CERT im Bereich der Standardisierung und der Konzeption von technischen Lösungen. Es ist wünschenswert, dass eine zentrale Stelle Überlegungen zu Best Practice-Ansätzen zum Aufbau einer Client, Server-Strategie anstellt, welche alle aktuellen Anforderungen und Bedürfnisse an ein Schulnetz umfasst, und diese den Schulen zugänglich macht.

Ein weiteres Aufgabenfeld umfasst die technische Konzeption und Entwicklung von technischen Hilfsmitteln für die Administration eines Schulnetzes. Ein

Schul-CERT kann hierzu die Entwicklung von Arbeitsmitteln in Form von Skripten für die automatisierte Administration, Aufbereitung von Filterlisten für die Absicherung des Netzwerkverkehrs aufbereiten und den EDV-Kustoden zur Verfügung stehen.

Ein Schul-CERT soll laut Aussage der Experten die Funktion einer zentralen Melde- und Entdeckungsstelle haben. Im Falle einer Kompromittierung ist das Schul-CERT der zentrale Ansprechpartner für die Betroffenen und koordiniert die Vorfallsbehandlung mit allen Beteiligten. Dazu ist es notwendig, dass das Schul-CERT eine Kontaktdatenbank der EDV-Kustoden aufbaut und pflegt, um eine intensive Kommunikation mit ihnen zu betreiben.

Eine weitere Aufgabe eines Schul-CERTs kann der Aufbau einer bundesländerübergreifenden Erfahrungs- und Informationsaustauschplattform sein, wie sie bereits in vielen anderen CERT-Bereichen etabliert ist. Auf Basis dieser Plattform lädt das Schul-CERT zu regelmäßigen Sitzungen in den Bundesländern ein und fungiert als Multiplikator um die EDV-Kustoden besser untereinander zu vernetzen und so den Erfahrungs- und Informationsaustausch zu fördern.

Außerdem sehen die Experten bei der Unterstützung des Fachministeriums bei der Aufarbeitung von technischen Erlässen und Handreichungen für den Schulbereich einen großen Bedarf. Durch die Beiziehung von CERT-Mitarbeitern soll eine größere Realitätsnähe und eine qualitative Verbesserung der Aussendungen erreicht werden. Eine weitere Aufgabe im Bereich der Unterstützung des Fachministeriums ist die Begleitung in der Durchführung von Risikoanalysen für zentrale Applikationen als qualitätssichernde Maßnahme.

6.4.3 Institutionalisierung eines Schul-CERTs und Mitarbeiterprofil

Die Unterkategorie Institutionalisierung eines Schul-CERTs und Mitarbeiterprofil befasst sich mit den Aussagen der Experten zum strukturellen Organisationsaufbau eines Schul-CERTs und mit den wichtigsten Eigenschaften, die ein Mitarbeiter für diesen Bereich mitbringen muss.

Die Experten sind sich einig, dass es für einen effizienten und effektiven CERT-Betrieb notwendig ist, dass es eine zentrale Verantwortung im Fachministerium für ein Schul-CERT geben muss. Um von den Schulen als Ansprechpartner akzeptiert zu werden, muss die Leitung des Schul-CERT im Bundesministerium für Bildung institutionalisiert werden. Eine möglichst breite Wirkung über alle öffentlichen Schulen entfalten sich nur, wenn es einen konsensualen Entschluss zum Aufbau dieser Organisation zwischen Bund, Ländern und Gemeinden gibt.

Um den Schulbetreibern und Schulverantwortlichen ein starker Partner in der Lösung von sicherheitstechnischen Problemen zu sein, ist es notwendig, dass ein Schul-CERT weisungsfrei gegenüber den Schulpartner agieren kann. Im Falle einer Kompromittierung eines Schulnetzes muss ein Schul-CERT selbständig die notwendigen Gegenmaßnahmen einleiten können, um eine zeitnahe und effektive Hilfestellung zu gewährleisten.

Ein Schul-CERT liefert eine Dienstleistung für Österreichs Schulen, hat aber in der Regel keine Möglichkeit sich selbst zu finanzieren. Es ist daher wichtig, dass bereits vor einer Institutionalisierung die Finanzierung der gewünschten Services durch das Schul-CERT ausreichend budgetiert und für die kommenden Jahre festgelegt wird.

Ein Großteil der Experten ist der Meinung, dass die operativen Agenden eines Schul-CERTs in eine bereits etablierte österreichische CERT-Struktur integriert werden soll. Dies hat den Vorteil, dass man bereits auf eine bereits aufgebaute Infrastruktur für einen CERT-Betrieb zugreifen kann. Ebenso ist das technische Personal bereits auf einem technisch sehr hohen Niveau und bringt bereits große betriebliche Erfahrungswerte ein. Nicht zu unterschätzen ist auch das bereits existente persönliche Netzwerk der CERT-Mitarbeiter, was beim Aufbau der Schul-CERTs Services sehr hilfreich sein wird.

Im Gegensatz zur allgemeinen Meinung ist ein Experte davon überzeugt, dass ein zentraler Betrieb eines Schul-CERT keinen Sinn macht. Aufgrund des

föderalistischen Ansatzes des österreichischen Schulsystems sieht er die Notwendigkeit, dass die Aufgaben einen Schul-CERTs in den Bundesländern eigens betrieben werden. Die Schaffung eines zentralen Kompetenzzentrums, welches eine Unterstützung für die Bundesländer bereitstellt sieht er als guten Ansatz an.

Wichtig ist es laut Expertenmeinung, dass es in der Anfangsphase eines Schul-CERT ein kleines, aber qualitativ hochwertiges und ausdefiniertes Service-Portfolio gibt. Dieses Portfolio sollte mit dem Fachministerium und den Schulansprechpartner in den Bundesländern gemeinsam erarbeitet werden, um möglichst rasch die wichtigsten Bedürfnisse der Verantwortungsträger abzudecken. Ein wichtiger Faktor ist dabei die Erreichbarkeit der Services, um das Vertrauen in die Aktivitäten eine Schul-CERTs zu stärken. Die Services sollten über möglichst viele Kommunikationskanäle erreichbar sein.

Hinsichtlich der fachlichen Qualifikation eines Schul-CERT Mitarbeiters sind die Fachexperten überzeugt, dass man ein breitgefächertes Profil benötigt. Als besonders wichtig wird das Wissen um die unterschiedlichen Strukturen im Schulbereich angesehen. Die Mitarbeiter eines Schul-CERTs müssen wissen, wie der tägliche Betrieb einer Schule funktioniert und wo die Prioritäten im Alltag liegen.

Essentiell für einen effektiven Betrieb eines Schul-CERTs sind Kompetenzen im technischen, sozialen und kommunikatorischen Bereich. Wichtig ist hierbei die Vermittlungskompetenz von technischen Inhalten. Die Mitarbeiter müssen in der Lage sein, technische Informationen zu analysieren und zielgruppenspezifisch aufzuarbeiten und zu kommunizieren.

Eine der wichtigsten Aufgaben eines Schul-CERTs ist der Aufbau einer übergreifenden Plattform für den Erfahrungs- und Informationsaustausch. Daher ist es notwendig, dass die Mitarbeiter auch eine Erfahrung im Projektmanagement aufweisen.

Es ist zu erwarten, dass das Schul-CERT auch internationale Kontakte für den Informationsaustausch aufbaut und pflegt. Einige Experten sind daher der Meinung, dass die Mitarbeiter auch gute Englisch-Kenntnisse haben müssen, um diese Aufgabe wahrzunehmen.

Die Aufarbeitung und Erstellung von Best Practice-Vorschlägen für den Betrieb eines Schulnetzes wird als ein bedeutendes Arbeitsumfeld gesehen. Um diese Aufgabe qualitativ hochwertig zu erledigen und auch umsetzbar zu gestalten, sollen Mitarbeiter Erfahrungen aus dem Bereich von Standards, Normen und Policies aufweisen.

Im Bereich der operativen Tätigkeiten ist es für die Experten wichtig, dass Schul-CERT Mitarbeiter die Fähigkeit haben, Bedrohungssituationen und Verwundbarkeiten für den Schulbereich richtig einzuschätzen. Die Frage, ob eine Sicherheitsschwachstelle in einem kommerziellen Content Management System eine Vielzahl von Schulen betrifft oder nur einige wenige, sollte bereits durch ein Schul-CERT beantwortet werden können. Auf Basis dieser Erkenntnis können die weiteren Schritte für eine Verständigung der betroffenen Schulen oder die Entwicklung von schnellgreifenden Schutzmaßnahmen getroffen werden.

7 Resumee

In dem folgenden Kapitel zieht der Autor ein Resumee über die vorliegende Arbeit und geht dabei auf drei Themenschwerpunkte ein. Im ersten Schritt beantwortet er explizit die in Kapitel 1.4 vorgestellten Forschungsfragen auf Basis der durch die Literaturanalyse und die Experteninterviews gewonnen Erkenntnisse. Folgende Forschungsfragen werden dabei konkret beantwortet:

1. Welche sensiblen Daten werden im Schulbereich verarbeitet?
2. Welche Sicherheitsrisiken existieren?
    a. Gibt es spezifische Auswirkungen durch den Einsatz von Computerklassen und Bring Your Own Device-Endgeräten?
    b. Gibt es spezifische IT-Sicherheitsrisiken an Schulen?
3. Gibt es bereits genügende Maßnahmen Schutz der Schulen und wie wird die Einhaltung dieser eingefordert?
    a. Welche technischen, organisatorischen und rechtlichen Maßnahmen werden getroffen, um die Risiken zu senken?
4. Welche Rolle kommt den Computer Emergency Response Teams (CERTs) dabei zu?

Im zweiten Teil dieses Kapitels wird im Detail auf die Forschungslücke eingegangen. Er beschreibt die Ausgangslage zu Beginn der Forschung und erläutert die im Verlauf der Arbeit gewonnenen Forschungsergebnisse.

Im dritten Teil des Resumees beschreibt der Autor die nächsten konkreten Schritte, wie ein Schul-CERT konkret strukturell aufgesetzt werden kann und welche Hilfestellungen Österreichs Schulen damit angeboten werden können.

7.1 Beantwortungen der Forschungsfragen

1. Welche sensiblen Daten werden im Schulbereich verarbeitet?

An Österreichs Schulen werden tagtäglich Tausende Datensätze bearbeitet, abgespeichert und verteilt. Grundsätzlich unterscheidet man bei den zu verarbeitenden Daten pädagogische Daten und Verwaltungsdaten.

Unter pädagogische Daten versteht man jene Daten, welche durch die Lehrkraft verwendet werden, um den Unterricht zu gestalten. Diese Daten werden verwendet, um einen multimedialen Unterricht zu gestalten und den Schülern Computer, Tablet oder Smartphone als digitale Arbeitsmittel näherzubringen. Pädagogische Daten werden zur Wissensvermittlung eingesetzt und enthalten in der Regel keine bis wenig sensible Daten.

Die Verarbeitung von pädagogischen Daten erfolgt in einem eigenen, weniger streng regulierten Bereich des Schulnetzwerkes, um einen flexiblen Zugang zu den Daten zu garantieren. Auf diese Weise wird sowohl den Lehrenden als auch den Schülern die Möglichkeit gegeben, unterschiedliche Methoden zur Nutzung der neuen Medien auszuprobieren.

So ist ein Trend erkennbar, dass Schüler und Lehrer vermehrt auf die Nutzung von öffentlichen Cloud-Services und sozialen Medien zugreifen, um einen komfortablen Wissens- und Datenaustausch zu betreiben, sei es, dass Unterrichtsdaten über Google-Drive oder Microsoft OneCloud ausgetauscht werden oder sich Lerngruppen über Facebook und Whatsapp organisieren.

Verwaltungsdaten dienen primär zur Administration des Schulbetriebs. Sie umfassen die Stammdatenverwaltung sowohl von Schülern und als auch von Lehrern. Auch im digitalen Klassenbuch werden sensible personenbezogene Daten verarbeitet.

Als besonders sensible Daten haben sich personenbezogene Daten von Dritten herauskristallisiert. Darunter fallen beispielsweise Informationen über die Scheidung der Eltern und Vormundschaften von Erziehungsberechtigten. So werden an Schulen typischerweise nicht nur Daten von Lehrern und Schülern verarbeitet, sondern auch Daten von Erziehungsberechtigten.

Die Daten werden sowohl über zentral angebotene Applikationen des Bundesministeriums für Bildung verarbeitet, als auch dezentral an den Schulen. Als Beispiele hierfür dienen die Lehrerverwaltungssoftware als zentrale Applikation und die Schülerverwaltungssoftware als dezentrale Applikation.

2. Welche Sicherheitsrisiken existieren?
    a. Gibt es spezifische Auswirkungen durch den Einsatz von Computerklassen und Bring Your Own Device-Endgeräten?
    b. Gibt es spezifische IT-Sicherheitsrisiken an Schulen?

Im schulischen Bereich greift eine Vielzahl von Benutzern auf eine beschränkte Anzahl von Endgeräten zu. Praktisch nach jeder Unterrichtseinheit wird der Benutzer in den Computerklassen geändert, teilweise erfolgt dies auch im administrativen Bereich. Die Wahrscheinlichkeit, dass sich ein Benutzer nicht richtig vom System abmeldet oder bei der Passworteingabe beobachtet, wird ist daher sehr hoch. Auch werden Lehrkräfte oftmals durch Schüler beim Benutzen der Unterrichtsprogramme unterstützt. All diese Faktoren tragen dazu bei, dass an Österreichs Schulen ein hohes Risiko eines Identitätsdiebstahls besteht. Mögliche Angreifer erhalten dadurch Zugriff auf Schüler- und Lehrer-Benutzerdaten und können mit deren Berechtigungen Daten verändern, löschen oder neue Datensätze anlegen. Erschwerend kommt hinzu, dass oftmals die Passwörter sowohl für den pädagogischen Bereich als auch für den Verwaltungsbereich gleich sind. Durch den Diebstahl von digitalen Identitäten hat ein Angreifer die Möglichkeit, in allen verfügbaren Services Daten zu manipulieren oder einfach nur mitzulesen.

Im pädagogischen Bereich erhalten Schüler oftmals Rechte auf das verwendete Unterrichtsmaterial. Das ermöglicht eine Kompromittierung der Datenintegrität

und somit eine Veränderung der Inhalte. Es kann passieren, dass einerseits die Lehrkraft mit verändertem, eventuell auch falschem, Unterrichtsmaterial den Unterricht durchführt oder Schüler falsche Lernunterlagen erhalten.

In der Regel greifen die Schüler über ein ungeschütztes und weitestgehend nicht reglementiertes Netzwerk auf die Unterrichtsdaten und das offene Internet zu. Durch den unbeschränkten Zugang in das Internet wird dieser oftmals für illegale Aktivitäten wie beispielsweise den illegalen Austausch von Filmen und Musik genutzt. Abgesehen von den Rechtsverletzungen führt die unkontrollierte Nutzung auch dazu, dass die Zugangskapazität zum Internet ausgelastet wird und für den Unterricht wenig Bandbreite zur Verfügung steht.

Ein großes Risiko existiert durch das fehlende Bewusstsein bei Administration, Lehrkörper und Schülern über die Sensibilität der Schuldaten und die damit einhergehende Verletzung der bestehenden Rechtslage. Oftmals ist es den Betroffenen nicht bewusst, dass sie personenbezogene Daten verarbeiten, welche nach der österreichischen Rechtslage besonders schutzwürdig sind. Stattdessen wird ein offener Austausch dieser Informationen gepflegt und teilweise auch über soziale Medien und öffentliche Cloud-Services ausgetauscht.

Das Angreiferprofil unterscheidet sich von anderen Bereichen, in denen sensible Daten verarbeitet werden, stark. An Schulen werden in der Regel keine wirtschaftlich interessanten Daten in großen Mengen verarbeitet. Angreifer haben daher tendenziell eher ein persönliches Interesse an den Daten und sind im schulnahen Umfeld zu suchen.

Die Motivation möglicher Angreifer entspringt dem Reiz des Verbotenen, neue Dinge auszuprobieren und vorhandene Sicherheitsbarrieren durch Kreativität zu umgehen. In den seltensten Fällen handelt es sich bei den Angriffen auf Schulen um koordinierte Attacken aus den Bereichen Hacktivism oder Wirtschaftskriminalität.

Computerklassen und Bring Your Own Device-Komponenten im Besonderen stellen die EDV-Kustoden vor neue Herausforderungen. Durch den vermehrten Einsatz von digitalen Endgeräten im Unterricht steigen die Anforderungen an die Verfügbarkeit, Vertraulichkeit und Integrität der IT-Services an den Schulen. EDV-Kustoden und alle Lehrer sind gefordert, sich ein großes technisches Verständnis für den Einsatz neuer Technologien anzueignen und diese im Anlassfall auch zeitnah wieder instandsetzen zu können.

Private Endgeräte können durch den EDV-Kustos nicht administriert werden und liegen in der Systemverantwortung des Schülers oder des Lehrers. Es ist somit schwer möglich, eine Kompromittierung des Gerätes zu erkennen und eine Ausbreitung im Netzwerk zu verhindern. Die Verwendung von Bring Your Own Device-Komponenten erhöht potentiell das Risiko einer Infizierung der zentralen IT-Services.

Grundsätzlich ist festzuhalten, dass sich die IT-Risiken an Österreichs Schulen nicht von denen eines normalen IT-Betriebes unterscheiden. Sowohl der Einsatz von zentralen und dezentralen IT-Systemen als auch die Anzahl der Endgeräte ist mit anderen IT-Betrieben vergleichbar. Auch die möglichen Angriffsszenarien unterscheiden sich nicht von denen in anderen Bereichen. Als Unterschied zu anderen IT-Betrieben ist die unterschiedliche Motivation eines Angreifers herauszustreichen. Während bei Angriffen auf ein IT-System in der Regel wirtschaftliche Interessen im Vordergrund stehen, ist davon bei Angriffen auf ein IT-System einer Schule nicht davon auszugehen.

3. Gibt es bereits genügende Maßnahmen Schutz der Schulen und wie wird die Einhaltung dieser eingefordert?
    a. Welche technischen, organisatorischen und rechtlichen Maßnahmen werden getroffen um die Risiken zu senken?

An Österreichs Schulen wird eine große Bandbreite aus technischen, organisatorischen und rechtlichen Maßnahmen eingesetzt, welche die IT-Sicherheit an den Schulen sicherstellen sollen.

Im technischen Umfeld setzen Schulen meist auf kommerzielle Hard- und Software, um IT-Sicherheit umzusetzen. Das liegt darin begründet, dass kommerzielle Komponenten eine bessere Unterstützungsleistung im technischen Support und mehr Komfort in der Bedienung bieten. Das Bundesministerium für Bildung bietet in diesem Zusammenhang den Bundesschulen kostenlose Microsoft-Lizenzen an, um ein professionelles Arbeitsumfeld für Lehrer und Schüler zu gewährleisten. Durch den Einsatz von legaler Software wird auch das Update-Verhalten der Administratoren verbessert und führt so zu einer insgesamt sichereren Umgebung. Als zentrale Schutzmaßnahme werden Webfilter verwendet, welche den Zugriff auf potentiell gefährliche Websites unterbinden.

Für Bring Your Own Device-Geräte werden Community-Produkte angeboten, welche eine komplette Live-Betriebssystemumgebung anbieten und somit den Schulbetrieb von der privaten Nutzung abkapseln.

Die wohl wichtigste technische Maßnahme ist die physikalische Trennung des pädagogischen Netzwerkes vom Verwaltungsnetz. Somit wird gewährleistet, dass nur der Lehrkörper und die Direktion auf die administrativen Daten zugreifen können. Die Schüler haben keine Möglichkeit, Zugriff auf diese Daten zu erlangen. Weiters ist der Trend erkennbar, dass Applikationen zur Verarbeitung von sensiblen Daten zentral betrieben werden. Aus sicherheitstechnischer Sicht ist auch das ein Vorteil, da dadurch ein Mindestsicherheitsstandard für die Verarbeitung der Daten umgesetzt werden kann.

Abgesehen von den technischen Sicherheitsmaßnahmen sind auch bewusstseinsbildende Maßnahmen ein Schwerpunkt im schulischen Bereich. Initiativen wie SaferInternet.at bereiten für Schüler und Lehrer zielgruppenspezifisch Informationsmaterial zum Thema Datensicherheit auf und bieten diese über ein Webportal an. Zur Unterstützung vor Ort ist es auch möglich, Experten von SaferInternet.at für Fortbildungsveranstaltungen an der Schule zu buchen.

Für die Verarbeitung von sensiblen Daten an Österreichs Schulen gilt die Einhaltung von nationalen Gesetzen und Richtlinien. Das wohl wichtigste Gesetz in diesem Zusammenhang ist das österreichische Datenschutzgesetz, welches den Umgang mit personenbezogenen Daten regelt, im Speziellen die elektronische Verarbeitung.

Lehrkräfte sind dem Beamtendienstrecht beziehungsweise dem Vertragsbedienstetengesetz verpflichtet. Das Dienstrecht regelt sowohl für Beamte als auch für Vertragsbedienstete der öffentlichen Verwaltung die Amtsverschwiegenheit. Die Amtsverschwiegenheit verbietet eine Weitergabe von Informationen, welche der Bedienstete im Rahmen der beruflichen Tätigkeit erfährt, an Dritte.

Weiters werden seitens des Bundesministeriums für Bildung Schulerlässe veröffentlicht, deren Anwendung für Bundesschulen bindend ist. Als einer der wichtigsten Erlässe in diesem Zusammenhang ist der Digitale Schulerlass zu werten, welcher Empfehlungen für die Bildung von digitaler Kompetenz an Schulen ausspricht und Handlungsanweisungen für einen sichere Nutzung digitaler Medien in Unterricht und Verwaltung gibt.

Aus Expertensicht ist das österreichische Schulnetz bereits gut abgesichert, natürlich gibt es aber auch hier noch Potential für Verbesserungen. Als eine wichtige Verbesserungsmaßnahme gilt es, einen kontinuierlichen Verbesserungsprozess für die Qualität der Maßnahmen zu erarbeiten. Das könnte in Form einer Selbstevaluierung der Schulen umgesetzt werden oder durch regelmäßige Kontrolle durch einen Experten einer fachvorgesetzten Stelle.

Für die technische Ausstattung an Schulen ist es wünschenswert, dass nicht nur Schullizenzen für die zentrale IT-Ausstattung zur Verfügung stehen, sondern dass auch verstärkt Schülerlizenzen für kommerzielle Softwareprodukte angeboten werden. Sollte dies für nicht alle Bereich möglich sein, muss eine Möglichkeit geschaffen werden, damit Schüler einen leichten Zugang zu Open Source-Produkten erhalten. Durch diese Maßnahme soll

gewährleistet werden, dass Schüler mit aktuellen und sicheren Softwareversionen im Unterricht arbeiten und kein leichtes Ziel für mögliche Kompromittierungen darstellen.

Private Endgeräte stellen heute bereits einen beträchtlichen Teil der verwendeten Endgeräte im Unterricht dar. Zur besseren Absicherung der Schülerdaten wie Hausaufgaben und Projektarbeiten ist es wichtig, dass ein umfassendes Backup-Konzept entworfen wird, um diese vor Verlust zu schützen.

Ein weiteres Potential bieten Fortbildungsveranstaltungen für den Lehrkörper und die Führungskräfte an den österreichischen Schulen. Um dem Thema IT an den Schulen mehr Aufmerksamkeit zu widmen, ist es notwendig, dass die Entscheidungsträger entsprechend sensibilisiert werden. Dazu ist eine konsequente Weiterentwicklung von zielgruppenspezifischen Awareness-Programmen notwendig.

4. Welche Rolle kommt den Computer Emergency Response Teams (CERTs) dabei zu?

In Österreich wurde 2006 das erste Computer Emergency Response Team durch den Betreiber des österreichischen Wissenschaftsnetzes, ACOnet, gegründet. Seit 2006 wurde eine Vielzahl von weiteren CERTs in den unterschiedlichsten Sektoren gegründet, welche sich unter dem Dachverband des nationalen CERT-Verbundes organisieren.

Für den schulischen Bereich sind bis dato keine expliziten CERT- oder CERT-ähnlichen Strukturen bekannt, obwohl es durchaus einen Bedarf an spezifischen Services gibt. EDV-Kustoden verwenden vereinzelt bereits Informationen aus den öffentlichen Services des nationalen CERT.at, welches unter anderem öffentliche Feeds und Mailinglisten zu aktuellen IT-Sicherheitsproblemen betreibt. Es gibt jedoch keinen regelmäßigen direkten Kontakt zwischen den Betreibern von Schulnetzwerken und CERT.at.

Als ein Aufgabengebiet für ein Schul-CERT bietet sich der breite Bereich der proaktiven Services an. Schwerpunkte von der Ausbildungsplanung über die technische Konzeption von Sicherheitslösungen bis hin zur Expertenunterstützung für andere Fachstellen im Bildungsbereich stehen hierbei im Vordergrund.

Eine besonders wichtige Aufgabe in diesem Bereich ist die Konzeption von IT-Sicherheitsschulungen für EDV-Kustoden, welche in regelmäßigen Abständen angeboten werden könnten. Mögliche Themen für diese Schulungen sollten in Abstimmung mit den bereits existierenden Arbeitsgruppen der EDV-Kustoden und den Clusterschulen des Bundesministeriums für Bildung erörtert werden.

Ein großes Potential steckt in der Erarbeitung von IT-Sicherheitskonzepten für Schulen. Mit dem notwendigen Wissen um die schulischen Strukturen und der Expertise im Bereich IT-Sicherheit ist es möglich, dass Best Practice-Ansätze zum Aufbau der Client- und Server-Implementierung erarbeitet werden. Ebenso können technische Hilfsmittel für die Administration der IT-Infrastruktur entwickelt und bereitgestellt werden.

Einen großen Bedarf gibt es auch bei der fachlichen Unterstützung des Bundesministeriums für Bildung im Bereich IT-Sicherheit. Die Experten eines Schul-CERTs können die technische Expertise für Handreichungen und Erlässe für den Schulbereich beisteuern. Damit kann eine realitätsnahe und qualitativ hochwertige Erarbeitung der Schulerlässe gewährleistet werden.

Eine zentrale Aufgabe für ein Schul-CERT ist der Aufbau einer Meldestelle für IT-Sicherheitsvorfälle an Österreichs Schulen. Als Ansprechpartner für Betroffene und kann ein Schul-CERT Erste-Hilfe-Maßnahmen anbieten und Informationen für die Erkennung und Behebung aufarbeiten. Diese Informationen können auch anderen Schulen zur Verfügung gestellt werden.

Für den Aufbau einer Meldestelle ist es wesentlich, dass das Schul-CERT gute Kontakte zu den EDV-Kustoden an den österreichischen Schulen aufbaut. Eine

der ersten Aufgaben muss daher sein, dass eine bundesländerübergreifende Plattform für den Erfahrungs- und Informationsaustausch aufgebaut wird, um die Kommunikation mit und zwischen den EDV-Kustoden zu verbessern.

Um eine möglichst hohe Akzeptanz eines Schul-CERTs zu gewährleisten, ist es notwendig, dass die zentrale Verantwortung für diese Struktur im Bundesministerium für Bildung verankert wird. Für eine Breitenwirkung über alle Schultypen hinweg ist eine gemeinsame Entscheidung von Bund, Ländern und Gemeindevertretung notwendig.

7.2 Weiterentwicklung des Forschungsfeldes

Die umfassende Literaturanalyse ergab, dass bereits eine Vielzahl von wissenschaftlichen Arbeiten verfasst wurde, welche das Thema IKT-Sicherheit und Informationssicherheit an Österreichs Schulen adressieren. Schwerpunkte dieser Arbeiten waren primär die Herausarbeitung von sicherheitstechnischen Anforderungen an den Schulen, meist mit dem Fokus auf bewusstseinsbildende Maßnahmen. Auch das Thema Computer Emergency Response Team wurde bereits mehrfach behandelt. Die Schwerpunkte in diesem Bereich lagen vorzugsweise in der formalen Beschreibung von CERT-Organisationen, sowie der Ausarbeitung von Möglichkeiten zum Ausbau der technischen und koordinierenden Vernetzungsmöglichkeiten.

Bis dato gab es keine wissenschaftlichen Erkenntnisse über mögliche Aufgaben und Services eines Computer Emergency Response Teams an Österreichs Schulen. Die hier vorliegende wissenschaftliche Arbeit kombiniert die Themen IT-Sicherheit an Österreichs Schulen und Computer Emergency Response Teams und beantwortet die Frage, welche Potentiale ein Schul-CERT im österreichischen Schulsystem bieten kann.

7.3 Nächste Schritte

Im Zuge der Erarbeitung der hier vorliegenden wissenschaftlichen Arbeit wurden die Fragen geklärt, welche IT-Sicherheitsrisiken an Österreichs Schulen existieren, welche Maßnahmen dagegen ergriffen werden und welche Hilfestellungen ein Schul-CERT in diesem Bereich anbieten kann.

Für den Aufbau eines SchulCERTs ist es aus Sicht des Autors notwendig, dass ein klarer Auftrag seitens des Bundesministeriums für Bildung erteilt wird um dieses Vorhaben zu starten.

Gemeinsam mit allen Schulerhaltern, Bund, Ländern und Gemeindevertretung, muss festgelegt werden, welche Zielgruppe ein Schul-CERT bedienen soll. Dabei muss die Frage geklärt werden, ob alle öffentlichen Schulen in die Zielgruppe des Schul-CERTs fallen. Schlussendlich dient dieser Schritt der Klärung der Finanzierungsfrage. Ein Schul-CERT kann sich mittels seiner bereitgestellten Services finanziell nicht selbst erhalten und ist auf eine Fremdfinanzierung angewiesen.

Parallel zur Finanzierungsfrage kann bereits ein Service-Portfolio aufgesetzt werden, welches die grundlegenden Leistungen beschreibt, welche durch das Schul-CERT erbracht werden sollen. Es bietet sich an, auf die bereits existierenden informellen und formellen Plattformen im schulischen Bereich zuzugehen und ein konsensuales Service-Angebot zu definieren, welches die Bedürfnisse der Betroffenen fokussiert. Hierbei sollte darauf geachtet werden, dass anfangs ein kleines Leistungsspektrum definiert wird, welches kurzfristig in einer guten Qualität erbracht werden kann.

Als erste CERT-Services bieten sich Alarmierungs- und Warnungsmeldungen an, welche mittels Mailinglisten an die EDV-Kustoden zugestellt werden. Das hat den Vorteil, dass man durch die Registrierung der Teilnehmer bereits einen interessierten Kundenstock identifiziert, welcher für Feedback zu den bestehenden Services kontaktiert werden kann. Mittels des ersten Kundenstocks ist eine Kontaktbasis geschaffen, um eine Plattform zu

etablieren, welche die Kommunikation mit und zwischen den EDV-Kustoden stärkt.

Für das Aufsetzen des operativen Betriebs eines Schul-CERTs ist es ratsam, sich mit bereits existierenden CERTs und technischen Schulplattformen in Verbindung zu setzen, um mögliche technologische, personelle oder wirtschaftliche Synergien zu ziehen. Eine Möglichkeit, einen Multiplikatoreffekt zu schaffen, ist es, die operativen Tätigkeiten an ein bereits existierendes CERT auszulagern. Als beispielgebendes CERT verweist der Autor auf das österreichische GovCERT, welches eine Public-Private-Partnership mit der Firma NIC.at eingegangen ist, um gemeinsam die GovCERT-Aktivitäten umzusetzen. Eine ähnliche strategische Partnerschaft ist auch für den schulischen Bereich denkbar.

Eine Partnerschaft bietet in der Regel für alle Beteiligten Vorteile. So kann das bereits etablierte CERT eine bessere Auslastung der Technologie und der Mitarbeiter erwarten und sich eine zusätzliche Finanzierung sichern. Das Bundesministerium für Bildung als Auftraggeber kann im Gegenzug auf eine bereits gut etablierte technische Infrastruktur und auf ausgebildetes Personal zurückgreifen.

Die schulspezifische Fachexpertise muss durch den Bildungsbereich eingebracht werden. Hier ist es wichtig, Personal mit Wissen im Bereich der Schulstrukturen einzubringen. Weiters ist es notwendig, dass die Mitarbeiter eine Schul-CERT-Erfahrungen im Bereich Projektmanagement haben, um neue Services umfassend aufzubauen und betreuen zu können.

Als Melde- und Kontaktstelle für IT-Sicherheitsvorfälle müssen Schul-CERT-Mitarbeiter Kompetenzen im sozialen und kommunikatorischen Bereich haben, sowie die Fähigkeit, technische Inhalte vermitteln zu können. Auch Fremdsprachenkenntnisse, vor allem Englisch, sind notwendig, um auch mit anderen Schul-CERTs und Schul-CERT ähnlichen Strukturen im Ausland Kontakt aufzunehmen und einen Erfahrungs- und Informationsaustausch zu betreiben.

Um die Struktur und die Services eines Schul-CERTs auch nachhaltig abzusichern, muss der formale Rahmen abgeklärt werden. Hierzu benötigt ein Schul-CERT einen klaren Auftrag seitens des Bundesministeriums für Bildung und eine zugesicherte Finanzierung für die kommenden Jahre. Um als starker Partner für Österreichs Schulen reüssieren zu können, muss ein Schul-CERT weitestgehend weisungsfrei in seinem Handeln sein.

Anhang A Abbildungsverzeichnis

Anhang B Quellenverzeichnis

APA-OTS (2012): Am Weg zu einer nationalen Cyber-Strategie für Österreich; http://www.ots.at/presseaussendung/OTS_20120305_OTS0184/am-weg-zu-einer-nationalen-cyber-strategie-fuer-oesterreich; zuletzt abgerufen am 04.01.2013

APA-OTS (2012): Nationale Cyber Exercise CE.AT 2012 und pan-europäische Exercise Cyber Europe 2012; http://www.ots.at/presseaussendung/OTS_20121004_OTS0118/nationale-cyber-exercise-ceat-2012-und-pan-europaeische-exercise-cyber-europe-2012; zuletzt aufgerufen am 15.10.2013

APA-OTS (2012): Am Weg zu einer nationalen Cyber-Strategie für Österreich http://www.ots.at/presseaussendung/OTS_20120305_OTS0184/am-weg-zu-einer-nationalen-cyber-strategie-fuer-oesterreich; zuletzt abgerufen am 04.10.2013

ACOnet-CERT: Das ACOnet-CERT; https://www.aco.net/cert.html?&L=0, zuletzt aufgerufen am 15.10.2013;

ACOnet-Roadshow (2008): Beitrag Mischitz: GovCERT Sicherheit mit System; http://www.aco.net/roadshow_agenda.html?&no_cache=1&cid=2433&did=1535&sechash=563ea68c, zuletzt aufgerufen am 13.11.2013;

BMUKK (2008): Einfaches und sicheres Schulnetz - IT-Einsatz und Internet Policy an Österreichs Schulen, Wien

BMUKK (2010): Digitale Kompetenz - IT-Einsatz und Internet Policy an Österreichs Schulen, Wien

BROWN LEE A.; GUTTMAN F. (1998): Request for Comments: 2350, Expectations for Computer Security Incident Response, www.ietf.org/rfc/rfc2350.txt, abgefragt am 13.2.2014

BRUNNER M.; SUTER E. (2008): International CIIP Handbook 2008/2009 – An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies, Zürich

Bundesoberstufenrealgymnasium Wiener Neustadt (2010): Schulbeginn mit Neuerungen - Elektronisches Klassenbuch und Klassenvorstandsstunde prägen den Schulanfang http://www.borg2700.at/php/projekt.php?projekt=Schulbeginn&schuljahr_id=0910; zuletzt aufgerufen am 20.10.2013

Carnegie Mellon University CERT/CC (2002): CSIRT Services; www.cert.org/csirts/services.html, zuletzt abgefragt am 13.2.2014.

Department of Homeland Security (2010): Cyber Storm: Securing Cyber Space; http://www.dhs.gov/cyber-storm-securing-cyber-space, zuletzt aufgerufen am 15.10.2013

derstandard.at (2014): Bifie-Datenleck gestopft, Tests gestoppt http://derstandard.at/1392686483213/Bifie-Datenleck-gestopft-Tests-gestoppt; zuletzt aufgerufen am 19.3.2014

derstandard.at (2014): Datenaffäre: Ministerin sagt Bildungsstandard- und Pisatests ab; http://derstandard.at/1392687781758/Schuelerdaten-Heurige-Bildungsstandard-Testungen-abgesagt, zuletzt aufgerufen am 19.3.2014

ENISA (2006): A STEP-BY-STEP APPROACH ON HOW TO SET UP A CSIRT, Heraklion

ENISA (2009): Baseline capabilities for national / governmental CERTs, Heraklion

ENISA (2011): Cyber Europe 2010 – Evaluation Report; Heraklion

ENISA (2012): Cyber Europe 2012 - Wichtigste Erkenntnisse und Empfehlungen, Heraklion

ENISA (2013): Inventory of CERT activities in Europe, Heraklion

Europäische Kommission (2010): KOM(2010) 245 endgültig/2 - Eine Digitale Agenda für Europa, Brüssel

Europäische Kommission (2010): KOM(2010) 2020 - Eine Strategie für intelligentes, nachhaltiges und integratives Wachstum, Brüssel

Europäische Kommission (2010): Survey of Schools:ICT in Education, Brüssel

Flick U.; Kardorff E.; Steinke I. (2005): Qualitative Forschung: Ein Handbuch, Rowohlt Verlag, Stuttgart

Froschauer U.; Lueger M. (2003): Das qualitative Interview - Zur Praxis interpretativer Analyse sozialer Systeme, WUV-UTB Verlag, Wien

Gabler Wirtschaftslexikon: UMTS/3G http://wirtschaftslexikon.gabler.de/Archiv/569859/umts-3g-v2.html; zuletzt aufgerufen am 21.2.2014

GovCERT.gv.at (2008): GovCERT in Österreich; http://govcert.gv.at; zuletzt aufgerufen am 15.10.2013

GovCERT.gv.at (2010): Einführung eines Informationssicherheits-Managementsystems; http://www.ref.gv.at/uploads/media/TOP10_GovCERT__Einfuehrung_eines_Informationssicherheits-Managementsystems.pdf, zuletzt aufgerufen am 15.10.2013

GovCERT.gv.at (2010): GovCERT.at und CERT.at - Information an die Mitglieder des Datenschutzrates; http://www.bka.gv.at/DocView.axd?CobId=45271; zuletzt aufgerufen am 15.10.2013

GovCERT.at; CERT.at (2010): Bericht Internet-Sicherheit Österreich 2010, Wien

GovCERT.at; CERT.at (2012): Bericht Internet-Sicherheit Österreich 2012, Wien

International Telecommunication Union (2008): Resolution 58 - Encourage the creation of national Computer Incident Response Teams, particularly for developing countries; Johannesburg

International Telecommunication Union (2011): The world in 2011 – ICT facts and figures; http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf; zuletzt aufgerufen am 20.11.2013

Lamnek S. (1995): Qualitative Sozialforschung, Beltz-Verlag, Eichstätt

Mayer H. (2002): Einführung in die Pflegeforschung, UTB-Verlag, Wien

Mayring P. (1996): Einführung in die qualitative Sozialforschung: Eine Anleitung zu qualitativem Denken, Psychologie Verlags Union, Basel

Mockapetris (1987): Request For Comments 1035: Domain Names – Implementation and Specification; http://tools.ietf.org/html/rfc1035; zuletzt aufgerufen am 20.3.2014

Meuser M; Nagel U. (1997): Experteninterviews – vielfach erprobt, wenig bedacht: Ein Beitrag zur qualitativen Methodendiskussion. In: Bogner; Littig;

Menz (2002): Das Experteninterview: Theorie, Methode Anwendung, VS Verlag für Sozialwissenschaften , Opladen

National Institute of Standards and Technology (2013): NISTIR 7298 Revision 2 - Glossary of Key Information Security Terms, Gaithersburg

Röhrl M. (2006): Computer Emergency Response Team (CERT): Analyse, Konzept und Umsetzung , Hannover

Spiel et al (2003): Evaluierung des österreichweiten Modellversuchs „e-Learning und e-Teaching mit SchülerInnen-Notebooks“; Wien

Stigler H.; Felbinger G. (2005): Der Interviewleitfaden; In: Stigler; Reicher (2005): Praxisbuch Empirische Sozialforschung in den Erziehungs- und Bildungswissenschaften, Studienverlag, Innsbruck

Twitter (2011): #Google MiTM attack by #Iran #government, again?; https://twitter.com/hkashfi/status/107758824810758144; zuletzt aufgerufen am 23.2.2014

UNTIS (2012): Untis; http://www.grupet.at/de/produkte/untis/uebersicht_untis.php; zuletzt abgerufen am 20.10.2013

West-Brown M. et al (2003): Handbook for Computer Security Incident Response Teams (CSIRTs), Pittsburgh

Anhang C Interviewkategorien

Kategorie 1 = Verarbeitung von sensiblen Daten an Schulen

Kategorie 2 = IT-Sicherheitsrisiken an Schulen

Kategorie 3 = Schutzmaßnahmen und Kontrollen

Kategorie 4 = Potentiale und Handlungsempfehlungen für ein Schul-CERT

Nummer	Interview-Nr	Geschlecht	Paraphrase	Generalisierung	Kategorien
1.	1	M	Schüler und Lehrer haben zur vereinfachten Administration eigene E-Mail Adressen bei Google registriert	Die Schule benutzt öffentliche Services für die Schulverwaltung	1
2.	1	M	Schüler haben Zugriff auf das elektronische Klassenbuch und auf die Lernplattform	Schüler greifen auf das pädagogische Netzwerk zu	2
3.	1	M	Mediadaten werden im Netzwerk abgelegt Schüler haben keinen Zugriff darauf	Schüler haben keinen Zugriff auf Unterrichtsdaten	3
4.	1	M	Direktion und Administration haben die Möglichkeit von zu Hause zu arbeiten	Die Schule bietet Remote Access für Direktion und Administration	1
5.	1	M	Personenbezogene Daten, Abrechnungsdaten und Noten werden als schützenswert angesehen.	Personenbezogene Daten, Abrechnungsdaten und Noten sind Verwaltungsdaten	1
6.	1	M	Aus dem Schulnetzwerk hat der Lehrer keinen Zugriff auf die Schülerverwaltungssoftware	Das pädagogische Netz und das Verwaltungsnetz sind strikt getrennt.	3

7.	1	M	Im Unterricht werden die gleichen Lehrerpasswörter wie im Verwaltungsbereich verwendet	Sicherheit bedeutet Komplexität für Lehrer und Schüler	3
8.	1	M	Die Lehrer entscheiden selber wo sie welche Daten abspeichern.	Die Einhaltung von Sicherheitsmaßnahmen liegt in der Verantwortung der Lehrer	3
9.	1	M	Die Schülerverwaltung soll demnächst ausgelagert werden.	Der Trend an Schulen geht zur zentralen Verwaltung von Schülerdaten	3
10.	1	M	Das Klassenbuch wird als sensibles, öffentliches Service angesehen und wird auf dem sicheren Verwaltungsserver der Schule gehostet. Das wird aber bald zentral für alle Schulen gehostet werden.	Das Klassenbuch ist ein öffentliches Services mit sensiblen Daten	1
11.	1	M	Es existieren Erlässe des BMUKK die gewisse Sicherheitsstandards vorschreiben. ZB Trennung vom pädagogischen und administrativen Netz. Diese gelten als überholt	Zentral erlassene Vorschriften spiegeln nicht die Realität an Schulen wieder.	3
12.	1	M	Elektronische Klassenbuch ist nicht verpflichtend, bietet aber viele Vorteile.	Die Schule setzt digitale Medien für den pädagogischen und verwaltungstechnischen Bereich nach verfügbarem Budget ein.	3
13.	1	M	Es ist nicht die Aufgabe der Schule die Einhaltung von Sicherheitsmaßnahmen zu überprüfen	Bei zentrale Applikationen ist das Ministerium für die Gewährleistung der IT-Sicherheit zuständig	3
14.	1	M	Für Risikoanalysen fehlt die Zeit und Testequipement ist nicht vorhanden	Ressourcen für IT-Sicherheit stehen den Schulen nicht in	3

				ausreichenden Maßen zur Verfügung.	
15.	1	M	An Schulen werden PCs in kurzen Abständen von vielen Benutzern verwendet.	An Schulen verwenden viele Benutzer die gleichen Geräte	2
16.	1	M	Services wie E-Mail, Home-Ordner, etc. werden als öffentliches Service über das Internet angeboten	Pädagogische Daten sind über das Internet erreichbar.	2
17.	1	M	Vulnerability Handling ist in einer großen, heterogenen Umgebung wichtig	Vulnerability-Handling ist als Schutzmaßnahme wichtig.	3
18.	1	M	Bei einem Stromausfall fallen wichtige Services aus, mit denen die Unterrichte gestaltet werden	Nicht nur die Applikationssicherheit ist wichtig, auch die Betriebssicherheit	3
19.	1	M	Privatgeräte können nicht kontrolliert werden. Die Schule muss sich überlegen wie sie die internen Services vor Angriffen schützen kann.	BYOD-Geräte können nicht kontrolliert werden.	2
20.	1	M	Identity Theft wird als Problem angesehen	Identity Theft ist auf Schulen ein großes Problem	2
21.	1	M	Für das Hacken brauchen die Schüler kein Spezialwissen mehr – dafür gibt es fertige Tools	Hacken erfordert kein Spezialwissen mehr	2
22.	1	M	Durch die Bereitstellung von zentralen Services verlagern sich die Sicherheitsrisiken zum externen Dienstleister	IT-Sicherheit ist bei externen Dienstleistern einzufordern.	3
23.	1	M	Der Zugriff auf die Verwaltungsdaten (Schüler, Eltern, Lehrer) und das Kompromittieren von Schul-Websites wird als lohnendes Ziel für Angreifer angesehen.	Verwaltungsdaten und Internet-Auftritte sind lohnende Ziele für Angreifer	2

24.	1	M	Mögliche Angreifer kommen aus dem Schulumfeld	Mögliche Angreifer kommen eher aus dem Schulumfeld	2
25.	1	M	Der Zugriff auf Verwaltungsdaten kann auch für externe interessant sein	Verwaltungsdaten sind für externe Angreifer interessant	2
26.	1	M	Der pädagogische Bereich muss offener sein um den Schülern auch etwas zeigen zu können	Der pädagogische Bereich braucht mehr Flexibilität für das Lernumfeld	3
27.	1	M	Schüler sind experimentierfreudiger	Schüler sind experimentierfreudig.	2
28.	1	M	Schüler nutzen das Netzwerk um illegal Daten zu downloaden	Das Schulnetzwerk wird für illegale Zwecke missbraucht.	2
29.	1	M	Die Kompromittierung von Schüler-PCs führt zu Blacklisting auf öffentlichen Listen, z.B. E-Mail.	Sicherheitsvorfälle haben Auswirkungen auf die gesamte Bereitstellung der IT-Infrastruktur	2
30.	1	M	Bei Problemen mit der Aufmerksamkeit wird das Internet gesperrt	Als Maßnahme gegen Unaufmerksamkeit wird das Internet gesperrt.	3
31.	1	M	Für den Unterricht ist eine OS-on-a-Stick Variante im Einsatz	Es gibt Community-Betriebssysteme für den Einsatz von BYOD im Unterricht	3
32.	1	M	Es wird ein Passwort für alle Services verwendet. Das ist nicht optimal aber praktisch.	Auch wenn die Netze getrennt werden sind die Passwörter für alle Services gleich	2
33.	1	M	Der Patchlevel wird auf einem aktuellen Stand gehalten	Als wichtige Maßnahme wird das Patchen der Applikationen angesehen	3
34.	1	M	Kommerzielle Firewalls bieten automatische Updates im Gegensatz zu Open Source Firewalls	Kommerzielle Produkte bieten mehr Unterstützung und Komfort als Open Source und Community-Produkte	3

35.	1	M	Richtlinien und Erlässe zu Mindeststandards gibt es, sind aber nicht verinnerlicht.	Mindestsicherheitsstandards an Schulen gibt es, passen aber nicht in das Arbeitsumfeld der Schule	3
36.	1	M	Safer Internet ist bekannt und wird auch genutzt	Awareness-Initiativen sind bekannt und werden auch genutzt.	3
37.	1	M	Systemadministration hat keine Unterstützungsprogramme	Für die Systemadministration gibt es keine Hilfestellungen.	3
38.	1	M	Internetlisten zu Sicherheitsthemen werden genutzt	Fortbildung erfolgt in Eigenregie.	3
39.	1	M	Die Einhaltung der Maßnahmen wird nicht kontrolliert. Es werden aber Fragebögen verschickt.	Die Einhaltung von Sicherheitsmaßnahmen wird seitens BMUKK an Schulen nicht kontrolliert.	3
40.	1	M	Eine stärkere Trennung der unterschiedlichen Bereiche wird als erforderliche Sicherheitsmaßnahme gesehen	Eine Trennung von Verwaltungs- und pädagogischen Daten ist notwendig	3
41.	1	M	Das Registrieren von Schüler-Endgeräten wäre eine geforderte Sicherheitsmaßnahme	Schüler-Endgeräte sollen an Schulen explizit freigeschalten werden.	3
42.	1	M	Vertretbarer Zeitaufwand vs. was man gerne hätte	Es müssen mehr Ressourcen für IT-Sicherheit an Schulen zur Verfügung gestellt werden.	3
43.	1	M	Die Kustoden sind in Form von Arbeitsgemeinschaften vernetzt und betreiben einen Erfahrungs- und Informationsaustausch	Ein Erfahrungsaustausch zwischen EDV-Kustoden ist über eigens organisierte Arbeitsgemeinschaften koordiniert	4
44.	1	M	Seitens des BMUKK wird die Kooperation zwischen den Schulen	Das BMUKK betreibt keine aktive Förderung des	4

			nicht gefördert.	Erfahrungs- und Informationsaustausches	
45.	1	M	Eine Unterstützung aus dem BMUKK würde positiv gesehen werden.	Das BMUKK betreibt keine aktive Förderung des Erfahrungs- und Informationsaustausches	4
46.	1	M	Schulen haben eine heterogene IT-Umgebung	Schulen haben eine heterogene IT-Umgebung	4
47.	1	M	Der Begriff eines CERT ist bekannt	CERTs und CERT-Services sind im Schulbereich bekannt	4
48.	1	M	Der Kontakt mit dem CERT beschränkt sich auf Mailinglisten	Es existiert kein operativer Kontakt zwischen Schule und CERT	4
49.	1	M	Tipps für die Absicherung der Schulumgebung wäre positiv	Know-How Transfer und Empfehlungen als Aufgabe für ein Schul-CERT	4
50.	1	M	Proaktive Maßnahmen stehen im Vordergrund	Proaktive Maßnahmen stehen im Vordergrund	4
51.	1	M	Tipps zu Datensicherung und Ablaufplänen, etc.	Know-How Transfer und Empfehlungen als Aufgabe für ein Schul-CERT	4
52.	1	M	Ausbildung und regelmäßige Tagungen als qualitätssichernde Maßnahme	Qualitätssichernde CERT-Aufgaben wären Konzeption von Ausbildungen für EDV-Kustoden und regelmäßige Tagungen/Schulungen	4
53.	1	M	Fachvorträge für Lehrer im Rahmen der Unterrichtsgestaltung	Im Rahmen der Unterrichtsgestaltungen können CERTs Fachvorträge für Lehrende geben	4
54.	1	M	CERT muss gut online verfügbar sein	Ein CERT muss gut online vernetzt sein	4

55.	1	M	Handelnde Personen sollen den Schulbetrieb kennen	CERT-Mitarbeiter müssen den Schulbetrieb kennen	4
56.	1	M	Handelnde Personen sollen Experten aus der Privatwirtschaft sein	Die technische Expertise für ein CERT muss aus dem Privatsektor kommen	4
57.	1	M	Aufbereiten von Informationen für den schulrelevanten Bereich wird als wichtiges Profil gesehen	Zielgruppenorientierte Aufbereitung von Information als CERT-Aufgabe	4
58.	2	F	Schülerverwaltung, elektronische Klassenbuch, Lernplattformen sind bekannt	Schülerverwaltung, elektronisches Klassenbuch und Lernplattformen sind bekannte schulische IT-Services	1
59.	2	F	Sensible Daten werden oft unbewusst von den Lehrern gespeichert.	Lehrern fehlt eine Awareness sensiblen Daten gegenüber	2
60.	2	F	Verschiebung der Begrifflichkeit von sensiblen Daten im allgemeinen Gebrauch ist spürbar.	Verschiebung der Begrifflichkeit von sensiblen Daten im allgemeinen Gebrauch ist spürbar.	2
61.	2	F	Datenschutzkonforme Verwaltung ist umständlich und wird daher nicht oft betrieben	Sicherheit entspricht nicht den Usability-Anforderungen der Benutzer	2
62.	2	F	Als Kriterium für sensible Daten gilt das Datenschutzgesetz, das auch in Safer Internet Broschüren aufgearbeitet wird.	Zur Beurteilung von sensiblen Daten gilt das Datenschutzgesetz	1
63.	2	F	Schülerbewertungen werden an Verlage ausgelagert	Sensibel sind ausgelagerte Schülerbewertungen an Verlagen	2
64.	2	F	Der Digitale Schulerlass regelt den Umgang mit sensiblen Daten	Der Digitale Schulerlass ist als Handlungsempfehlung zur Handhabung von sensiblen Daten an Schulen bekannt.	1

65.	2	F	Bei zentralen Services ist die Sicherheit besser gegeben.	Eine zentrale Bereitstellung von IT-Systemen gewährleistet eine bessere IT-Sicherheit	3
66.	2	F	Lehrer haben einen hohen Grad an Selbstbestimmung und wollen generell keine Fremdbestimmung auch nicht im Softwarebereich	Eine Zentralisierung von IT-Services an Schulen führt zu einer geringeren Akzeptanz bei den Lehrenden aufgrund eines hohen Anspruchs auf Selbstbestimmung	2
67.	2	F	In der Risikoanalyse sind Technik und Mensch wichtig	In einer umfassenden Risikoanalyse ist der Fokus auf die Technik nicht ausreichend. Auch der Faktor Mensch muss berücksichtigt werden.	3
68.	2	F	Schüler helfen Lehrern mit der Technik	Es besteht ein Know-How Unterschied im IT-Bereich zwischen Schüler und Lehrer	2
69.	2	F	Schulungen und Vorgaben für Lehrende im Umgang mit IT sind wichtig.	Die Konzeption von Schulungen und die Erarbeitung von Handlungsempfehlungen für Lehrende ist wichtig	3
70.	2	F	Diskrepanz des Know-How zwischen Lehrern und Schüler	Es besteht ein Know-How Unterschied im IT-Bereich zwischen Schüler und Lehrer	2
71.	2	F	Schüler haben einen Ehrgeiz alles auszutricksen	Schüler entwickeln eine Eigenmotivation durch den Ehrgeiz sperren zu Umgehen und neue Dinge auszuprobieren	2

72.	2	F	Die Aufmerksamkeit der Schule in Bezug auf den Umgang mit IT an der Schule ist wichtig. Die Schuld liegt nicht immer beim Schüler oder den Eltern.	Die Schule muss den Themen IT und Umgang mit IT an den Schulen gezielt Aufmerksamkeit widmen	3
73.	2	F	Ändern von Powerpoint während des Vortrags	Schüler verändern Unterrichtsmaterialien	2
74.	2	F	Ausbessern des Lehrers durch Mitlesen auf Wikipedia	Nutzung des Internet-Angebots um den Lehrer auf seine Fehler aufmerksam zu machen	2
75.	2	F	Nutzung von Whats-App zum Schummeln	Einsatz digitaler Medien zum Schummeln	2
76.	2	F	Schülerdatenmanipulation im Verwaltungsbereich	Schülerdatenmanipulation im Verwaltungsbereich	2
77.	2	F	Die Internetleitung ist meist nicht ausgelegt für BYOD.	Internet-Kapazität an Schulen ist meist nicht ausgelegt für BYOD	2
78.	2	F	Eigene Lehrer-WLANs	Absicherung der Daten und Qualität der IT-Services zur Trennung von Schüler- und Lehrer-WLAN	3
79.	2	F	IT-Sicherheit ist eine Frage der Betriebsverfügbarkeit	Eine verwundbare IT-Komponente kann zum Stillstand des gesamten EDV-Systems an den Schulen führen	2
80.	2	F	Urheberrechtsverletzungen werden nicht als Sicherheitsproblem gesehen.	Fehlende Awareness bei Schülern und Lehrer hinsichtlich Verletzung von Urheberrechten	2
81.	2	F	Die Frage des Aufwands für IT-Sicherheit an Schulen ist abhängig von der Motivation des EDV-Kustos	Die IT-Sicherheit ist abhängig von der Awareness des EDV-Kustos	2

82.	2	F	Welche Maßnahmen umgesetzt werden entscheidet der Betreiber der IT an Schulen	Investitionen in IT-Sicherheit sind abhängig von der Entscheidung des Betreibers (Awareness).	3
83.	2	F	Auch innerhalb der Lehrer und der Schuladministration gibt es einen großen Know-How Unterschied	Auch innerhalb des Lehrkörpers gibt es einen großen Know-How Unterschied	2
84.	2	F	Erlässe werden nicht kontrolliert.	Erlässe werden nicht kontrolliert	3
85.	2	F	Die digitale Kompetenz wird evaluiert	Die Umsetzung des Erlasses zur Digitalen Kompetenz wird evaluiert	3
86.	2	F	Die Kernaufgabe eines Lehrers ist unterrichten.	Der Umgang mit neuen Medien im Unterricht erfordert neue Anforderungen an das Lehrpersonal	2
87.	2	F	Verpflichtende Fortbildungen im IT-Bereich für Lehrende wäre vertretbar und sinnvoll	Aus-, Fort- und Weiterbildung im Bereich IT für den Lehrkörper sollte verpflichtend gemacht werden.	3
88.	2	F	Im Falle einer Kompromittierung erhalten Schulen Unterstützung von anderen EDV-Kustoden, externen Dienstleistern und dem Bildungsnetzwerk	Im Falle einer Kompromittierung ist eine externe Unterstützung vorhanden (Dienstleister, Bildungsnetzwerk)	4
89.	2	F	Die EDV-Kustoden sind innerhalb eines Bundeslandes gut vernetzt und pflegen einen regen Austausch	EDV-Kustoden sind bereits in bundesländerspezifischen Organisationen vernetzt und betreiben eine regen Informations- und Erfahrungsaustausch	4

90.	2	F	Sicherheit ist eher kein Thema auf den Austauschplattformen	Auf den bereits existierenden Informations- und Erfahrungsaustausch-Plattformen ist kein Platz für das Thema IT-Sicherheit.	4
91.	2	F	Unterstützung der IT-Verantwortlichen und Führungskräfte (Direktoren)	Eine zielgruppengerechte Unterstützung im Bereich IT-Sicherheit für IT-Verantwortliche und Führungskräfte ist notwendig	4
92.	2	F	Kontinuierliche Awarenessbildung im Bereich Datenschutz	Die Entwicklung eines nachhaltigen, kontinuierlichen Programms zur Awarenessbildung im Bereich Datenschutz für IT-Verantwortliche und Führungskräfte ist notwendig	4
93.	2	F	Weiterbildung im Bereich der IT-Kustoden	Konzeption und Durchführung von zielgruppenspezifischen Weiterbildung im Bereich IT-Sicherheit für IT-Kustoden	4
94.	2	F	Schul-CERT müsste im BMUKK angesiedelt sein um Akzeptiert zu werden	Ein Schul-CERT muss im zuständigen Fachressort institutionalisiert sein um eine Akzeptanz an den Schulen zu haben	4
95.	2	F	Technische und Vermittlungskompetenz sind wichtig	Wichtige Eigenschaften von Schul-CERT Mitarbeitern ist eine technische Vermittlungskompetenz	4
96.	2	F	Unterstützung des BMUKK im Bereich der Richtlinien und Erlässe ist	Unterstützung des Fachressorts bei der	4

			notwendig um die Aktualität zu gewährleisten.	Aufarbeitung von Richtlinien und Erlässen im technischen Bereich	
97.	3	M	Es gibt die stark personenbezogenen Services der Verwaltung und die pädagogischen Services die eher auf Informationsgewinnung und Wissensmanagement ausgelegt sind.	Im schulischen Bereich werden Services zur Verwaltung, Informationsmanagement und Wissensmanagement betrieben	1
98.	3	M	Schüler und Lehrer organisieren sich über Google, Dropbox und dergleichen.	Im pädagogischen Bereich werden Cloud-Services wie Google und Dropbox verwendet	1
99.	3	M	Die Trennung der Daten verschwimmt sehr zwischen den Bereichen	Eine Trennung von Verwaltungs- und pädagogischen Daten ist nicht immer möglich	2
100.	3	M	Die Schulen sind nicht gut ausgestattet und daher nutzen die Schüler und Lehrer gerne komfortable aber ungesicherte Cloud-Services	Usability geht vor Security. Die Schulen sind infrastrukturtechnische nicht immer gut ausgestattet. Lehrer und Schüler bedienen sich daher komfortabler Cloud-Services	2
101.	3	M	Auch sensible Daten von Eltern werden verarbeitet, Bsp Scheidung, Vormundschaften etc.	Sensible Daten von Eltern werden verarbeitet	1
102.	3	M	Der Großteil der Daten wird als unkritisch angesehen, da es sich um Wissensvermittlung und Partizipation geht.	Ein Großteil der zu verarbeitenden an Schulen sind unkritisch.	2
103.	3	M	Daten an Schulen werden nach dem Need-to-Know Prinzip verarbeitet	Daten an Schulen werden nach dem Need-to-Know	2

				Prinzip verarbeitet	
104.	3	M	Amtsverschwiegenheit und Datenschutz sind relevante gesetzliche Regelungen	Die Amtsverschwiegenheit und die Einhaltung des DSG werden als relevante rechtliche Rahmenbedingungen angesehen	1
105.	3	M	Die Daten sind sensibler als sie auf den ersten Blick aussehen	Die Sensibilität der Daten an Schulen erschließt sich meist erst auf den zweiten Blick	2
106.	3	M	Eine falsche Beurteilung aufgrund einer Kompromittierung der Datenintegrität ist ein Risiko	Verlust von Datenintegrität bei Noten ist ein Risiko	2
107.	3	M	Risikoanalyse bei zentralen Applikationen ist notwendig.	Eine Risikoanalyse bei zentralen Applikationen ist wichtig	2
108.	3	M	Awareness bei den Verantwortungsträger ist wichtig	Awareness-Bildung bei Führungskräften ist wichtig	3
109.	3	M	Eine höhere Fluktuation der Schüler als von Mitarbeitern in normalen Betrieben	Die hohe Fluktuation von Schülern wird als Risiko gesehen	2
110.	3	M	Eine höhere Fluktuation der Schüler als von Mitarbeitern in normalen Betrieben	Die hohe Fluktuation von Schülern wird als Risiko gesehen	2
111.	3	M	Der Spaßfaktor bei Schülern ist ein Risiko	Schüler versuchen aus Spaß die Sicherheit von IT-Systemen zu umgehen	2
112.	3	M	Sicherheit ist abhängig vom Engagement des EDV-Kustos	Die Sicherheit des gesamten IT-Systems an Schulen ist abhängig von der Motivation des EDV-Kustos	2

113.	3	M	Der pädagogische Bereich muss offener sein um mit den Schülern zu arbeiten als der administrative Teil	Es existieren unterschiedliche Risikoprofile. Der pädagogische Bereich darf nicht so streng reglementiert sein um auch im Unterricht flexibel reagieren zu können	2
114.	3	M	Jedes neue Gerät ist potentielles Risiko	BYOD erhöht die Anzahl der potentiell infizierten Endgeräten an den Schulen	2
115.	3	M	Das Gerät muss im Unterricht verwendbar sein – ob infiziert oder nicht	Die Teilnahme am Unterricht geht vor der Sicherheit des Endgerätes	2
116.	3	M	Sicherheitslösungen werden vom Schulerhalter definiert und umgesetzt	Die Schaffung von Rahmenbedingungen für das Umsetzen von IT-Sicherheit obliegt dem Schulerhalter	3
117.	3	M	Safer Internet bietet viel im Bereich Awareness an	Safer Internet ist im Schulbereich bekannt	3
118.	3	M	Grundaufgabe des Lehrers ist unterrichten, nicht IT-Sicherheit	Schwerpunkt eines Lehrers ist das Unterrichten nicht IT	3
119.	3	M	Sicherheit hängt viel vom Engagement des EDV-Kustos ab	Die Sicherheit des gesamten IT-Systems an Schulen ist abhängig von der Motivation des EDV-Kustos	2
120.			Die hohe Grad des Benutzerwechsel am PC ist schulspezifisch	Hoher Grad an Benutzerwechseln erhöht das das Risiko	2
121.	3	M	Ja, es werden zentrale Aussendungen gemacht und auch in den Lehrerkonferenzen diskutiert	Seitens des Fachressorts werden zentrale Aussendungen vorbereitet. Die Bekanntmachung an den Schulen obliegt den	3

				Führungskräften	
122.	3	M	Eine Unterstützung für EDV-Kustoden gibt es nicht	Eine technische Unterstützung für EDV-Kustoden ist nicht bekannt	3
123.	3	M	Die Umsetzung von IT-Sicherheit liegt in der Verantwortung der Führungskraft.	Die Umsetzung von IT-Sicherheit liegt in der Verantwortung der Führungskraft.	3
124.	3	M	Eigene Kontrollmaßnahmen gibt es nicht	Kontrollmaßnahmen zur Einhaltung von Maßnahmen sind nicht bekannt	3
125.	3	M	Eine Selbstevaluierung im Sinne eine Qualitätszyklus ist sinnvoll	Eine sinnvolle Maßnahme wäre die Selbstevaluierung im Sinne es Qualitätszyklus	3
126.	3	M	Für zentrale Applikationen gibt es die Unterstützung des Dienstleisters	Zentrale Applikationen werden durch Dienstleister gewartet und bieten Benutzerunterstützung	3
127.	3	M	Für die offenen Strukturen ist keine Hilfestellung bekannt	Technische Unterstützung für den pädagogischen Bereich ist nicht bekannt	4
128.	3	M	Die Arbeitsgruppen der EDV-Kustoden sind bekannt.	EDV-Kustoden sind in bundesländerspezifischen Arbeitsgruppen organisiert	4
129.	3	M	Die Arbeitsgruppen beschäftigen sich eher mit betrieblichen, medienspezifischen Fragen – nicht mit Sicherheit	Die Arbeitsgruppe der EDV-Kustoden beschäftigt sich mit betrieblichen, medienspezifischen Inhalten	4
130.	3	M	Es gibt keine Schul-CERT Strukturen	Es sind keine Schul-CERT Strukturen bekannt	4
131.	3	M	Präventive Aufgaben stehen im Vordergrund	Präventive Aufgaben sollten im Fokus eines Schul-CERTs	4

				stehen	
132.	3	M	Qualitätssichernde Aktivitäten wie Policies, Handlungsempfehlungen wäre eine wichtige CERT-Aktivität	Qualitätssichernde Aktivitäten (Policies, Handlungsempfehlungen) wären wichtige Aufgaben für ein Schul-CERT	4
133.	3	M	Wenn möglich in eine vorhandene Struktur integrieren.	Ein Schul-CERT sollte in vorhandene Strukturen integriert werden	4
134.	3	M	Kooperation von Bund, Ländern und Gemeinden notwendig	Um ein allgemein akzeptiertes Schul-CERT zu etablieren sind gemeinsame Anstrengungen von Bund, Ländern und Gemeinden notwendig	4
135.	3	M	Wissen um den Schulbetrieb ist wichtig	Ein wichtiges Kriterium für Schul-CERT Mitarbeiter ist das Wissen um die unterschiedlichen Strukturen im Schulbereich und den täglichen Betrieb	4
136.	4	M	Personenbezogene Daten und Noten werden als sensibel angesehen	Personenbezogene Daten und Noten werden an Schulen als sensibel angesehen	1
137.	4	M	Sensible Daten sind Daten die in das Datenschutzgesetz fallen	Ein Großteil der sensiblen Daten fallen in den Wirkungsbereichs des Datenschutzgesetzes	1
138.	4	M	Alles was Geschäftsgeheimnissen, Urheberrechten oder NDAs unterliegt.		

139.	4	M	Hinsichtlich Verfügbarkeit wird E-Learning als sensibel angesehen.	Die Verfügbarkeit von E-Learning Systemen wird als sensibel für die Unterrichtsgestaltung gesehen	1
140.	4	M	Die Veröffentlichung von Klassenbuch-Informationen und Noten stellen eher ein Imageproblem dar.	Klassenbuch-Informationen und Noten werden als sensibel im Sinne von Imageschädigend angesehen	2
141.	4	M	Je höher der Abhängigkeitsgrad, desto mehr ist eine professionelle Struktur notwendig die das System betreibt und entwickelt	Für IT-Systeme mit hoher Komplexität ist eine professionelle Betreuungsstruktur notwendig	3
142.	4	M	Auch kleine Änderungen müssen sicherheitstechnisch überprüft werden	Veränderungen am IT-System müssen hinsichtlich der sicherheitstechnischen Auswirkungen untersucht werden	3
143.	4	M	Es existierte ein Niveauunterschied zwischen Lehrer und Schülern in IT-Themen	Es besteht ein Know-How Unterschied im IT-Bereich zwischen Schüler und Lehrer	
144.	4	M	Für den Schulbetrieb muss ein Mittelweg zwischen starker und schwacher Sicherheitskonzept gefunden werden	Verwaltungsdaten müssen strikt abgesichert werden und der pädagogische Bereich muss sich Flexibilität im Einsatz der IT-Infrastruktur bewahren	3
145.	4	M	Schüler haben nicht die Awareness	Fehlende Awareness bei Schülern	2
146.	4	M	Die Verwaltungsdaten stehen eher im Fokus von Hackern	Verwaltungsdaten sind sensibler als pädagogische Daten	2

147.	4	M	Die Unterrichtsdaten sind eher uninteressant	Verwaltungsdaten sind sensibler als pädagogische Daten	2
148.	4	M	Der Einsatz von Computern im Unterricht erfordert eine rasche Wiederherstellungszeit von kaputter Hard- und Software	Beim Einsatz von Computerklassen ist Verfügbarkeit ein wichtiges Thema	2
149.	4	M	Aus sicherheitstechnischer Sicht ist das Bereitstellen von Computern für den Unterricht und BYOD vergleichbar	Es existiert kein Unterschied hinsichtlich IT-Sicherheit zwischen dem Einsatz von Computerklassen und BYOD	2
150.	4	M	In Computerklassen und bei BYOD ist eine Backup-Strategie für Schüler wichtig.	Beim Einsatz von Computerklassen und BYOD stellt ein durchdachtes Backup-Konzept die Verfügbarkeit von Unterrichtsdaten sicher	3
151.	4	M	Das Schulnetzwerk ist in Form von Kompetenzzentren organisiert	EDV-Kustoden erhalten im Anlassfall Unterstützung durch die Kompetenzzentren des Schulnetzwerkes	3
152.	4	M	Die Kompetenzzentren müssen ressourcenmäßig besser ausgestattet werden.	Die Kompetenzzentren müssen ressourcenmäßig besser ausgestattet werden	3
153.	4	M	Eine Verpflichtung zur Behebung von sicherheitstechnischen Problemen ist wünschenswert.	Eine Verpflichtende Behebung von erkannten sicherheitstechnischen Problemen ist wünschenswert	3
154.	4	M	Ein Schul-CERT kann konzeptionelle und koordinierende Aufgaben im Schulbereich übernehmen.	Ein Schul-CERT kann konzeptionelle und koordinierende Aufgaben im Schulbereich übernehmen.	4

155.	4	M	Safer Internet als Initiative im Schulbereich ist bekannt.	Safer Internet als Initiative im Schulbereich ist bekannt und wird genutzt.	3
156.	4	M	GovCERT hat bereits einmal eine Unterstützungsleistung für Schulen geboten.	Das österreichische GovCERT bietet Schulen Unterstützungsleistung an	4
157.	4	M	Ein Schul-CERT kann als Melde- und Entdeckungsstelle funktionieren.	Ein Schul-CERT Funktion einer Melde- und Entdeckungsstelle haben	4
158.	4	M	Ein Schul-CERT kann eine Kontaktdatenbank für Schulen aufbauen	Ein Schul-CERT soll ein Point of Contact für alle Schulen sein und eine Kontaktdatenbank aufbauen	4
159.	4	M	Ein Schul-CERT könnte ein "Find-mir-das-Problem-im-Haus-Kastl - in a Box" konzipieren.	Ein Schul-CERT soll technisch konzipierend tätig sein um Schulen neue Arbeitsmittel in die Hand zu geben	4
160.	4	M	Ein Schul-CERT kann eine einheitliche Client- und Serverstrategie entwickeln – inklusive Sicherheitsstrategie	Eine zentrale Client/Serverstrategie kann durch ein Schul-CERT entwickelt werden	4
161.	4	M	Ein Schul-CERT kann eine Vernetzungsplattform für IT-Kustoden aufbauen	Der Aufbau einer Plattform für den Informations- und Erfahrungsaustausch ist eine Aufgabe für ein Schul-CERT	4
162.	4	M	Ein Schul-CERT kann zielgruppenspezifische Hilfestellungen aufbereiten.	Die zielgruppenspezifische Aufarbeitung von technischer Information ist eine Aufgabe für ein Schul-CERT	4
163.	4	M	Diese Aufgaben stellen eine hohen Anspruch in technischer, sozialer und kommunikatorischer Sicht	Mitarbeiter eines Schul-CERT müssen Kompetenzen im technischen, sozialen und	4

				kommikatorischen Bereich haben	
164.	4	M	Ein Schul-CERT kann im Aus-, Fort- und Weiterbildungsbereich die Konzeption für Ausbildungen durchführen.	Die Erarbeitung von Konzepten für Lehrerfortbildung im Bereich IT-Sicherheit ist eine Aufgabe eines Schul-CERTs	4
165.	4	M	Eine virtuelles Schul-CERT funktioniert nicht	Eine zentrale Verantwortung für ein Schul-CERT ist notwendig.	4
166.	4	M	In einem Schul-CERT darf es keine Nebenbeschäftigung geben.	In einem Schul-CERT darf es keine Nebenbeschäftigung geben.	4
167.	4	M	Ein Schul-CERT muss so institutionalisiert werden, dass es etwas bewegen kann – beim BMUKK oder GovCERT.	Ein Schul-CERT muss in bereits etablierten und akzeptierten Strukturen integriert werden.	4
168.	4	M	In einem Schul-CERT muss technisches Personal beschäftigt werden.	Mitarbeiter eines Schul-CERT müssen Kompetenzen im technischen, sozialen und kommikatorischen Bereich haben	
169.	4	M	In einem Schul-CERT müssen Kommunikationsexperten beschäftigt werden.	Mitarbeiter eines Schul-CERT müssen Kompetenzen im technischen, sozialen und kommikatorischen Bereich haben	
170.	4	M	In einem Schul-CERT muss rechtskundiges Personal beschäftigt werden.	Ein Schul-CERT muss ein rechtskundiges Profil aufweisen	4
171.	4	M	In einem Schul-CERT ist Projektmanagement-Erfahrung gefragt.	Ein Schul-CERT muss ein Projektmanagement-Profil aufweisen	4

172.	4	M	In einem Schul-CERT sind Personen mit Englisch-Kenntnissen gefragt	Mitarbeiter eines Schul-CERTs müssen gute Englisch-Kenntnisse aufweisen	4
173.	4	M	In einem Schul-CERT müssen Personen mit Kenntnissen im Bereich ISO-Standards und Policies beschäftigt werden.	Ein Schul-CERT muss Expertise im Bereich von Standards, Normen und Policies aufweisen	4
174.	5	M	Das elektronische Klassenbuch und die Notenverwaltung wird als sensibel angesehen	Im Schulbetrieb werden Klassenbuch-Daten und Daten der Notenverwaltung als sensibel angesehen	1
175.	5	M	Die Kommunikation zwischen Schüler und Lehrer über Facebook zu schulrelevanten Themen ist datenschutzrechtlich fragwürdig.	Schüler und Lehrer kommunizieren über schulsensible Inhalte über Soziale Medien	2
176.	5	M	Die Einhaltung des Datenschutzgesetzes ist wichtig.	Das Datenschutzgesetz ist für die Verwaltung von Daten im Schulbetrieb relevant	1
177.	5	M	Durch Schuldaten ist ein Profiling von Kindern und deren Eltern möglich	Mit Schuldaten kann ein Profiling von Schülern und Lehrern gemacht werden	2
178.	5	M	Die Technologie wird genutzt ohne die formalen Rahmenbedingungen zu klären	Die Technologie wird genutzt ohne die formalen Rahmenbedingungen zu klären	2
179.	5	M	Verfügbarkeit ist bei zentralen Plattformen, z.B. Zentralmatura, ein wichtiger Punkt.	Bei zentralen Applikationen steht die Verfügbarkeit des Service im Vordergrund	2
180.	5	M	Zentrale Plattformen die auch die Auswertung übernehmen stehen im Blickpunkt von Angreifern.	Angreifer sehen zentrale Plattformen von Schulen als lohnende Ziele an	2

181.	5	M	Bei Internet-Plattformen, welche personenbezogene Daten verarbeiten muss eine Risikoanalyse gemacht werden.	Es soll bei allen öffentlichen Plattformen, auf den personenbezogene Daten verarbeitet werden eine Risikoanalyse gemacht werden	2
182.	5	M	Schul-Applikationen werden oft von engagierten Lehrern und Schüler programmiert – die Sicherheitstechnik bleibt da oft außen vor.	Die Entwicklung von schuleigenen Applikationen wird nicht durch Professionisten durchgeführt.	2
183.	5	M	Der Schaden an Schulen ist zumeist ein Imageproblem	Bei Kompromittierung von Schuldaten entsteht ein Image-Problem	1
184.	5	M	Motivation mit Angreifer können Hacktivism und Schadensfreude sein.	Hacktivism und Schadensfreude sind mögliche Motivationsfaktoren für Angreifer	2
185.	5	M	Ein finanzielles Interesse ist seitens eines möglichen Angreifers nicht gegeben.	Angreifer eines Schul-Systems haben kein finanzielles Interesse an den Daten	2
186.	5	M	Schüler schleusen unwissentlich Viren ein.	Es fehlt die Awareness der Schüler	2
187.	5	M	Eine strikte Netzwerktrennung ist an Schulen notwendig.	Verwaltungsdaten und Unterrichtsdaten müssen strikt von einander getrennt werden	3
188.	5	M	Ein vernünftiges Patch-Management gehört zentralisiert.	Eine wichtige Maßnahme für die Sicherstellung IT-Sicherheit an Schulen ist ein zentrales Patch-Management	3
189.	5	M	Schüler müssen zum Einsatz von legaler Software und regelmäßigen	Der Einsatz legaler Software und das regelmäßige	3

			Updates animiert werden.	Updaten von Software erhöht das Sicherheitsrisiko an Schulen	
190.	5	M	Schulen sollen Schullizenzen hergeben und den Zugang zu Open Source erleichtern.	Schulen sollen den Zugang zu Open Source und Schülerlizenzen von kommerzieller Software erleichtern	3
191.	5	M	Safer Internet bietet eine Menge im Bereich Awareness.	Die Initiative Safer Internet ist an den Schulen bekannt und wird auch genutzt	3
192.	5	M	Der Einsatz von mobilen Endgeräten erschwert den Einsatz von Filtersoftware für Kinder.	Der Einsatz von mobilen Endgeräte erschwert die Endgerätkontrolle	2
193.	5	M	Technische Ratgeber an die Schulseite gibt es wenige.	Es gibt nicht ausreichend technische Ratgeber und Hilfestellungen für Schulen	3
194.	5	M	Es keine eine Asymmetrie des Wissensstandes zwischen Schüler und Lehrer	Es keine eine Asymmetrie des Wissensstandes zwischen Schüler und Lehrer	2
195.	5	M	Die Motivation alte Geräte von der Schule zu verwenden ist gering.	Schulen sind IT-technisch meist schlecht ausgestattet. Dadurch entsteht meist BYOD	2
196.	5	M	BYOD als sinnstiftender Einsatz im Unterricht ist ein Feature	BYOD kann im Unterricht positiv genutzt werden, da dadurch eine Vielzahl von meist aktueller Hard- und Software verfügbar ist	2
197.	5	M	Wie verhindere ich Schummeln durch den Einsatz von moderner Technologie.	Durch den Einsatz von neuen Technologien haben auch die Schummelmethoden sich weiterentwickelt.	2

198.	5	M	Betriebene IT-Infrastruktur muss auch professionell gewartet werden.	Bei professionellen Anforderungen an ein IT-System muss eine professionelle Betriebsführung sichergestellt sein	3
199.	5	M	Der Einsatz von „Nebenberufinformatiker“ skaliert nicht.	Die Tätigkeit eines EDV-Kustos muss einer vollen Lehrverpflichtung entsprechen	3
200.	5	M	Wenn der Serverraum während der Matura abstürzt ist die Priorität klar.	Die Tätigkeit eines EDV-Kustos muss einer vollen Lehrverpflichtung entsprechen	3
201.	5	M	Eine Schul-CERT Aufgabe ist die Awareness-Bildung bei IT-Kustoden.	Die Konzeption und Durchführung von Awareness-Aktivitäten für die Zielgruppe EDV-Kustoden ist eine Aufgabe eines Schul-CERTs	4
202.	5	M	Die schlechte IT-Ausstattung an den Schulen bewirkt den Einsatz von BYOD durch die Hintertür	Schulen sind IT-technisch meist schlecht ausgestattet. Dadurch entsteht meist BYOD	2
203.	5	M	Ein Schul-CERT kann Vorabsicherheitsüberprüfungen von gemeinsam genutzten Anwendungen durchführen.	Die Durchführung von umfassenden Risikoanalysen von zentralen Applikationen kann eine Aufgabe eines Schul-CERTs sein	4
204.	5	M	Zentrales IT-Know How wäre wichtig.	Der Aufbau und die Bereitstellung von Know-How im IT-Bereich durch ein Schul-CERT ist sinnvoll	4

205.	5	M	Eine schnelle Eingreiftruppe kann ein Schul-CERT nicht leisten.	Eine vor Ort-Unterstützung durch ein Schul-CERT ist nicht möglich	4
206.	5	M	Man verspricht eventuell zu viel als was man leisten kann.	Zur Erreichung der notwendigen Akzeptanz eines Schul-CERTs ist ein kleines, aber qualitativ hochwertiges Service-Portfolio wichtig	4
207.	5	M	Eine Definition der Kernleistung ist notwendig.	Eine Definition der Kernleistung ist notwendig.	4
208.	5	M	Mit einem geordneten und strukturierten Ausbildungskonzept und gezielten Awareness-Kampagnen kann man sehr viel erreichen.	Die Konzeption und Durchführung einer Ausbildung- und Awareness-Kampagne ist eine Aufgabe eines Schul-CERTs	4
209.	5	M	Es muss klar sein wer die Leistung zahlt.	Die Finanzierung eines Schul-CERTs muss im Vorfeld sichergestellt sein	4
210.	5	M	Es ist nicht sinnvoll alles zentral an einem Standort zu betreiben. Man braucht Leute in den Bundesländern die die Themen koordinieren.	Der zentrale Betrieb eines Schul-CERTs ist nicht sinnvoll, Die Aktivitäten an den Schulen in den Bundesländer müssen eigens koordiniert werden.	4
211.	5	M	Vielleicht ist der Ansatz eines gemeinsam betriebenen Kompetenzentrums richtiger als der eines CERTs.	Die Bildung eines Kompetenzzentrums mit zentraler Koordinationsfunktion ist ein besserer Ansatz als der eines Schul-CERTs	4
212.	5	M	Klassische CERT-Aktivitäten können durch bestehende CERTs erledigt	Klassische CERT-Aktivitäten können über die	4

			werden.	bestehenden CERTs abgehandelt werden	
213.	5	M	Die Spezialität einer Schule liegt im Kundenkreis und der Betreuungssituation.	Das Alleinstellungsmerkmal einer Schule im CERT-Kontext liegt im Kundenkreis und den unterschiedlichen Schulstrukturen	4
214.	5	M	Erfahrung im Umgang mit Service Anrufen ist notwendig.	Ein Schul-CERT Mitarbeiter muss Erfahrung im Bereich Call Center mitbringen	4
215.	5	M	Technisches Wissen in den Bereichen Client, Server, Netzwerk, Firewalling und Web-Technologien ist notwendig.	Ein Schul-CERT Mitarbeiter muss Wissen im Bereich Technik mitbringen	4
216.	5	M	Das Wissen ob eine Schwachstelle im CMS 3 oder 3000 Schulen betrifft ist wichtig.	Die Einschätzung einer Bedrohungssituation für den schulischen Bereich wird als wichtige Fähigkeit eines Schul-CERTs eingestuft	4
217.	5	M	Das Einschätzen von Verwundbarkeiten ist wichtig.	Das Einschätzen von Verwundbarkeiten wird als wichtige Fähigkeit eines Schul-CERTs eingeschätzt	4
218.	6	W	Den Bundesschulen wird über ein Microsoft School Agreement über das BMUKK Schullizenzen zur Verfügung gestellt.	Das Fachressort stellt Schulen Lizenzen zur Verfügung	3
219.	6	W	Jede Bundesschule muss gewissen Verwaltungsapplikationen nutzen z.B. SAP.	An den Schulen werden zentrale Applikationen zur Verwaltung genutzt	1
220.	6	W	Die Verwaltungsdaten, das elektronische Klassenbuch und Noten sind sensible Daten an Schulen.	Die Verwaltungsdaten, Daten aus dem elektronischen Klassenbuch und Notendaten werden als sensibel	1

				angesehen	
221.	6	W	Für zentrale Applikationen werden Erlässe herausgegeben z.B. Haushaltsführung.	Das Fachministerium stellt Erlässe und Handreichungen zur sicheren Nutzung der zentralen Applikationen zur Verfügung	3
222.	6	W	Der Direktor ist verantwortlich für die Datenhaltung.	Die Verantwortung der Datenhaltung obliegt dem Direktor einer Schule	1
223.	6	W	Für zentrale Applikationen veranlassen wir Risikoanalysen.	Das Fachministerium ist für die Durchführung von Risikoanalysen für zentral bereitgestellte Applikationen zuständig	3
224.	6	W	An den Schulen ist der Mensch ein Sicherheitsrisiko.	An der Schule ist der Mensch ein großes IT-Sicherheitsrisiko	2
225.	6	W	Der pädagogische Bereich und der Verwaltungsbereich sind oft strikt voneinander getrennt.	Verwaltungsdaten und Unterrichtsdaten werden strikt voneinander getrennt	3
226.	6	W	Wir versuchen über Handreichungen die Verwaltung der Daten zu steuern.	Das Fachministerium stellt Erlässe und Handreichungen zur sicheren Nutzung der zentralen Applikationen zur Verfügung	3
227.	6	W	Der Lehrer muss mit Computern zu Recht kommen.	Den Lehrern fehlt oft das notwendige Know-How um dem Einsatz von PCs im Unterricht gerecht zu werden	2
228.	6	W	Die schulische IT-Infrastruktur und BYOD muss zusammenpassen – das ist meist ein Problem.	Durch den Einsatz von BYOD entsteht eine große Heterogenität im schulischen	2

				Bereich, was die Komplexität der Betriebsführung erhöht	
229.	6	W	Computerklassen brauchen viel Zeit für die Administration der Geräte durch den Lehrer.	Die Administration der Computerklassen verbraucht viel Zeit in der Unterrichtsgestaltung	2
230.	6	W	Die Schule kann sich durch externe Unterstützung viel Aufwand und Zeit ersparen.	Der Schulerhalter bestimmt über die Bereitstellung von externer Unterstützungsleistung im IT-Bereich	3
231.	6	W	Das BMUKK unterstützt das Konzept mit Clusterschulen.	Das Fachressort unterstützt die Bildung von Clusterschulen als zentrale Anlaufstellen	3
232.	6	W	Die Steuerung der technischen Sicherheit ist von Lehrer zu Lehrer unterschiedlich.	Es herrscht ein großer Niveauunterschied im Bereich IT-Sicherheit von Schule zu Schule	2
233.	6	W	Meist ist der Sicherheitsschutz an Schulen sehr streng angelegt – z.B. durch das Filtern von Websites.	Das Filtern von Websites als Maßnahme zum Schutz der IT-Infrastruktur	3
234.	6	W	Die Mindeststandards ergeben sich durch die eingesetzte Software.	Die Mindeststandards ergeben sich durch die eingesetzte Software.	3
235.	6	W	Zentrale Applikationen verlangen Sicherheitsstandards an den Schulen.	Das Fachministerium veröffentlicht Erlässe für den Umgang mit zentralen Applikationen an den Schulen	3
236.	6	W	Das BMUKK informiert die Schulen über Sicherheitsvorfälle.	Das Fachministerium fungiert als Meldestelle für die Schulen im Falle einer	4

				Kompromittierung	
237.	6	W	Oft gibt es keine Rückmeldung zu gemeldeten Sicherheitsproblemen.	Für das übergreifende Incident Handling zwischen Fachministerium und Schule ist kein Prozess etabliert	4
238.	6	W	Es ist unklar ob die Information an den richtigen Empfänger gelangt (EDV-Kustos)	Es gibt keine etablierte Kontaktmöglichkeit für die Kommunikation zwischen Fachministerium und den EDV-Kustoden	4
239.	6	W	Das ACOnet-CERT informiert uns über Sicherheitsvorfälle an Schulen	Das Fachministerium fungiert als Meldestelle für die Schulen im Falle einer Kompromittierung	4
240.	6	W	Ein CERT muss vom BMUKK eingesetzt werden.	Zur Erreichung der notwendigen Akzeptanz muss ein Schul-CERT durch das zuständige Fachministerium eingesetzt werden	4
241.	6	W	Man müsste ein CERT an bestehende Strukturen dranhängen.	Für die Institutionalisierung eine Schul-CERTs sollen bereits bestehende Strukturen genutzt werden	4
242.	6	W	Ein CERT muss unabhängig von der Weisung eines Direktors sein.	Ein Schul-CERT muss weisungsunabhängig sein	4
243.	6	W	Die Kompetenzcluster haben keinen Auftrag vom Ministerium.	Die derzeitigen Kompetenzcluster haben keinen Auftrag vom Ministerium, sondern sind durch Eigeninitiativen von Privatpersonen entstanden	4

244.	6	W	Das Wissen um die unterschiedlichen Schulstrukturen ist sehr wichtig.	Ein Schul-CERT Mitarbeiter muss in den unterschiedlichen Schulstrukturen bewandert sein	4