Ist die NSA schon in der Schule?

Thilo Weichert, Leiter des ULD
Landesbeauftragter für Datenschutz Schleswig-Holstein
Medienkompetenztag
Christian-Albrechts-Universität zu Kiel
30. September 2014

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Chancen und Risiken
- Staatliche Hilfen ?
- Erziehung zu digitalen Grundrechten
- Spezielle Fragen
- Ansätze zum Selbstschutz

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

- Kontrollbehörde auch gegenüber Bildungseinrichtungen und Schulen, Entgegennahme und Bearbeitung von Beschwerden
- Beratung aller Beteiligten: Ministerium, Schulträger, Schulleitungen, Schulverwaltung, Lehrkräfte, Eltern, SchülerInnen
- Fort-und Ausbildung: DATENSCHUTZAKADEMIE Sch.Holst.
- Medienkompetenzvermittlung u.a. an Schulen
- Erforschung von datenschutzfreundlichen Lösungen (z. B. ID-Management an schwedischer Schule)
- Zertifizierung und Auditierung von Ausbildungs- und Schul-IT

Internet – Quell vieler Möglichkeiten

Information und Kommunikation

- Verwaltung und Bereitstellung eigener Daten, Bilder, Texte
- E-Mail, Teilnahme an Foren, Austausch mit Behörden und Unternehmen, berufliches Engagement im Netz
- eCommerce, Webshops
- Wikipedia, Blogs
- Demokratischer Austausch, Online-Petitionen
- Soziale Netzwerke
- Informationsportale, Selbstdarstellungen, Veröffentlichungen zu Wissenschaft, Literatur, Kunst ..., örtl. Orientierungshilfen
- Newsportale (Schrift, Ton und Bild)
- Suchmaschinen
- Unterhaltung und Spiele

… und mancher Risiken

- Ausforschung, Ausspionieren der Privat- und Sozialsphäre
- Anprangerung, Diskreditierung, Rufmord
- Manipulation und Falschinformation
- Belästigung durch Werbung, Spam
- Identitätsdiebstahl
- Internetbetrug
- Abzocke
- Internetabhängigkeit, Netz als Droge, Vereinzelung (Sex, Glücksspiele, Gewalt)

> Nutzen, aber mit Vorsicht

Chancen und Risiken für die Schule

(+)

- Online-Vermittlung von Inhalten
- Vermittlung von Medien- und Sprachkompetenz
- Innerschulische Kommunikation
- Internet/Smartphone/WLAN als schulisches Hilfsmittel

(-)

- Ausspionieren von Schulangehörigen (z. B. Noten), von Prüfungsaufgaben und interner Kommunikation
- eMobbing und eStalking
- Individualisierung und Entsolidarisierung
- Gewöhnung an Überwachung … nicht nur durch die NSA?

Was interessiert die NSA eine deutsche Schule?

NSA/GCHQ interessieren sich für alle und alles – also auch für die Schule, z. B.

- SchülerInnen als potenzielle TerroristInnen
- Lehrkräfte und SchülerInnen mit US-Kontakten
- Kompromittierendes Material bzgl. Perspektivzielen (Forschende, SportlerInnen, religiöse od. politische Aktivitäten an der Schule)
- Obrigkeitshörigkeit (technik-, konsum- und) überwachungsaffine Erziehung, nicht nur in den USA, sondern auch in Deutschland …
- Technische Innovationen in Bezug auf Überwachung und Datenschutz findet auch in Schulen statt

Enthüllungen Snowden

Anfang Juni 2013: Enthüllungen durch Edward Snowden

Rechtfertigung: Terrorismusbekämpfung

- National Security Agency (NSA - USA): Prism u. a.
- Government Communications Headquarters (GCHQ – GB): Tempora u. a.
- Direction Générale de la Securité Extérieure (DGSE – F)
- Bundesnachrichtendienst (BND – D): Strateg. TKÜ u. a.
- Weitere Five Eyes (Kanada, Australien, Neuseeland)
- Spionage aus China, Russland…

> Politische Spionage, Wirtschaftsspionage, allgem. Netzüberwachung

Angriffsarten

- Abgreifen von Internetdienstleistern, z. B. Soziale Netzwerke od. Clouds (in den USA, zwangsweise od. freiwillig)
- Verdeckter Zugang zu einem Netzbetreiber (BelgaCom, Telekom)
- Brechen von Kryptografie
- Verdeckter Zugang zu Internetdiensten (über Backdoors) zur Beschaffung von Meta- und Inhaltsdaten (z. B. Adressbücher)
- Abhören von Internetkabeln oder von Internetknoten
- Beschaffung von (evtl. zulässig erlangten Daten von) „befreundeten" Diensten (z. B. strategische BND-TKÜ)
- Kapern von Rechnern und Rechnernetzen (unterschiedliche Methoden, z. B. Online-Durchsuchung)
- Verdeckte technische und personale Ermittlungen
- Sammeln und Auswerten „öffentlicher Quellen" (im Netz)

Risiken und behördliche Helfer

Nicht nur staatliche Überwachung:

- Unternehmens-Wirtschaftsspionage
- Kriminelle Hacker – Abzocke, Sabotage
- Innentäter

- Spionageabwehr: Aufgabe der Ämter für Verfassungsschutz

- Informationssicherheit: Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Cyber-Strafverfolgung, Gefahrenabwehr: Bundeskriminal-amt, LKÄ, Europol, Staatsanwaltschaften

- Datenschutz: Aufsichtsbehörden, z. B. ULD (Kunden, Beschäftigte)

Schwarz-roter Koalitionsvertrag 2013

- Bündelung der IT-Netze in einer einheitliche Plattform
- Verstärke Standardisierungsarbeit
- Zertifizierung von Cloud-Infrastrukturen
- Ausbau Kryptografie
- Ende-zu-Ende-Verschlüsselung bei De-Mail
- Integration „Stiftung Datenschutz" in „Stiftung Warentest"
- Privacy by Design, Privacy by Default
- EU-Datenschutzgrundverordnung
- Datenschutzabkommen mit den USA
- Neuverhandlung von Safe Harbor, SWIFT, PNR-Abkommen

Digitale Agenda August 2014

Inhalte u.a. Schaffung digitaler Infrastrukturen, Innovationsförderung, Vermittlung von Medienkompetenz und Wissenschaftsförderung

Kapitel VI Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft

- Förderung einfacher Sicherheitstechniken
- Weiterentwicklung und Angebot vertrauenswürdiger Hard- und Software
- Schaffung sicherer IT-Infrastrukturen (nPA, De-Mail, „Verschlüsselungsstandort Nr. 1 auf der Welt"
- Förderung von datenschutzfreundlichen Geschäftsmodellen
- Moderner Datenschutz in Europa und „führende Rolle bei der Entwicklung internationaler Datenschutzprinzipien"
- „einer der sichersten digitalen Standorte weltweit"
- IT-Sicherheitsgesetz

Erziehung zu digitalen Grundrechten I

- Art. 12 Allgemeine Menschenrechtserklärung 1948: Privatleben, Familie, Wohnung, Schriftverkehr, Ehre, Ruf
- Art. 19 Allg.ErklMenschR: „Jeder Mensch hat das Recht auf freie Meinungsäußerung; dieses Recht umfasst die Freiheit, Meinungen unangefochten anzuhängen und Informationen und Ideen mit allen Verständigungsmitteln ohne Rücksicht auf Grenzen zu suchen, zu empfangen und zu verbreiten."
- BVerfG (VZU 1983): „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Gesellschaftsordnung nicht vereinbar, in der Bürger nicht mehr wissen, wer was wann bei welcher Gelegenheit über sie weiß."

Erziehung zu digitalen Grundrechten II

- BVerfG (Online-Durchs.-Urteil 2008): „Das allgemeine Persönlichkeitsrecht umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. …
  Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen."

> Grundrecht auf digitale Privatsphäre (Computergrundrecht)

Erziehung zu digitalen Grundrechten III

- Art. 8 Europäische Grundrechte-Charta:

(1)Jeder Mensch hat das Recht auf Schutz der ihn betreffenden personenbezogenen Daten.

(2)Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jeder Mensch hat das Recht, Auskunft über die ihn betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3)Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Erziehung zu digitalen Grundrechten IV

- Recht auf informationelle Selbstbestimmung (Datenschutz)
- Telekommunikationsgeheimnis
- digitale Privatsphäre (Computergrundrecht)
- Presse- und Meinungsfreiheit im Netz
- Informationsfreiheit über das Netz
- Transparenz und Öffentlichkeit (Open Data)
- Demokratische Versammlung im Netz
- Berufliche und wirtschaftliche Freiheit im Netz
- Netzneutralität (Diskriminierungsverbot im Netz)
- digitale Religionsfreiheit u. Ä.

Kommt nach der Allgemeine Erklärung der (analogen) Menschenrechte (1948) die der digitale Menschenrechte ?

Erziehung konkret

Entwicklung schuleigener attraktiver u. datenschutzkonformer Kommunikationsplattformen

Reflektierter Verzicht auf Facebook, WhatsApp, Google & Co.

Professionalisierung und Standardisierung der Schul-IT (weg von der Turnschuh-(Schüler-)Administration)

Integration v. Medien/Inhalten/Curicula I

In allen Schulfächern

- Mathe – Informatik
- Englisch – Privacy Policies/Terms of Use z. B. von Alibaba
- Gesellschaftskunde – digitale Grundrechte, z. B. Projekt Betroffenenrechte
- Geografie – Medieneinsatz (TV-Länderberichte, Internet)
- Literatur/Deutsch – Orwell, Huxley, Eggers, Elsberg
- Biologie/Chemie – Genetik
- Kunst – Gestaltung von eigenen Websites
- Sport – Wearables

Integration v. Medien/Inhalten/Curicula II

mit gesellschaftlichen Playern:

- Medienanstalt
- Offener Kanal
- Datenschutzbehörde
- Polizei (Cyberkriminalität)
- Frauenhäuser (digitale Gewalt)
- Unternehmen (Wirtschaftsspionage)

unter aktiver Einbeziehung der SchülerInnen und deren Schülermitverantwortung

Bspl. Alibaba (Fach Englisch)

- Weltweit größter Online-Anbieter
- Sitz in China/Hongkong/Singapur
- Privacy Policy: „Your **privacy is important** to us and we have taken steps to ensure that we do not collect more information from you than is necessary for us to provide you with our services and to protect your account. … If you provide any Personal Data to us, you are deemed to have authorised us to collect, retain and use that Personal Data for the following purposes: … 6. performing research on statistical analysis in order to improve the content and layout of the Sites, to improve our product offerings and services and for **marketing and promotional services**."

Betroffenenrechte (Gesellschaftskunde)

- Informationen (Impressum, Ausland, Art der Verarbeitung, Profilbildung, Übermittlungen, Rechte) (Art. 10 f. EU-DSRL)
- Auskunft (Art. 12 f. EU-DSRL)
- Datenkorrektur (Art. 6, 14 EU-DSRL), Löschung, Sperrung, Berichtigung, Anlass z. B.: Kündigung, Tod, Zeitablauf
- Kontoübertragung (Art. 18 EU-DSGVO-E)
- Widerspruchsrechte (Art. 14 EU-DSRL)
- Anonyme od. pseudonyme Nutzung (ergibt sich aus Grundrechten)

Sicherungsmaßnahmen (Fach Informatik)

- Aktuelle Browser, Antivirensoftware, Firewall
- Vermeiden von US-Anbietern (z. B. WhatsApp, Facebook od. Google+)
- Nutzen anonymer Suchmaschinen (z. B. Ixquick)
- Nutzung von Anonymisierungsdiensten (Tor, JonDos)
- Eigene IT oder Trusted Cloud (Schengen-Anbieter, Zertifizierung), Kontrolle Auftragsdatenverarbeiter
- Nutzung sichere Infrastrukturen (nPA, De-Mail)
- Nutzung starker Verschlüsselung (PGP, GnuPG)
- Klare Trennung beruflich-privat (z. B. bei BYOD)
- Datensparsamkeit !!!

Interessen

- UserInnen: Unterhaltung, Information, Kommunikation, Arbeit – preisgünstig und einfach
- Öffentliche Stellen (Polizei, Schulen, Staatskanzlei usw.): Kommunikationskanal zu jungen/für junge Menschen
- Unternehmen: Kundenansprache, Verkauf, Kundenbindung, Kundenkommunikation (Rückkanal), Kundenanalyse
- Schule: Erlernen eines solidarischen, verantwortungs-bewussten, freiheitlichen u. demokratischen Umgangs mit Informationstechnik

Relevante Aspekte

Recht
Technik
Ökonomie
Politik
Kultur
Erziehung
Psychologie
= eine große pädagogische Herausforderung

Ist die NSA schon in der Schule?
Ja, aber wir schmeißen sie wieder raus!

Dr. Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Independent Center for Privacy Protection Schleswig-Holstein (ICPP)
Holstenstr. 98, D- 24103 Kiel
mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de