

Workshop für ICT-Verantwortliche der kantonalen Schulen



Wolfgang Sidler

Master of Advanced Studies in
Information Security

Mitarbeiter des
Datenschutzbeauftragten des
Kantons Luzern

3. Juli 2009

Ziele des Workshops

- Datenschutz in Schulumgebungen kennen und anwenden können
- Die Kernelemente der IT-Sicherheit und der Informationssicherheit kennen
- Sensibilisierung im Umgang mit den neuen Kommunikations-Plattformen und das Verhalten der neuen Benutzer-Generation kennen

Agenda

- Einführung zum Datenschutz
- Der Generationenkonflikt – die Generation „Y“
- Die DSB-Merkblätter zum Thema Schule
- IT-Sicherheit und Informationssicherheit
- Ausblick - Trends
- Diskussion

Einführung zum Datenschutz

Gesetzliche Verankerung des Datenschutzes

Bundesverfassung (BV)

Art. 10 Persönliche Freiheit
Art. 13 Schutz der Privatsphäre

Bundesrecht (DSG)

Bundesgesetz über den Datenschutz vom 19.06.1992 (235.1)
Verordnung vom 14.06.1992 (235.11) – Revision: 2007 – seit dem 1.1.2008 gilt das revidierte DSG.

Kantonales Recht (Kt. DSG)

Gesetz über Schutz von Personendaten vom 02.07.1990 (SRL 38)
Verordnung vom 26.02.1991 – Revision 2007

BV & DSG Teil 1

Art. 10 Recht auf Leben und auf persönliche Freiheit

- ¹ Jeder Mensch hat das Recht auf Leben. Die Todesstrafe ist verboten.
- ² Jeder Mensch hat das Recht auf persönliche Freiheit, insbesondere auf körperliche und geistige Unversehrtheit und auf Bewegungsfreiheit.
- ³ Folter und jede andere Art grausamer, unmenschlicher oder erniedrigender Behandlung oder Bestrafung sind verboten.

BV & DSG Teil 2

Art. 13 Schutz der Privatsphäre

- ¹ Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.
- ² Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

Rolle des Datenschutzgesetzes?

Anwendungsbereich

Bund

- Bundesbehörde (Art. 16 ff DSG)
- Private (Art. 12 ff DSG)

Kanton

- kantonale- und Gemeindebehörden (§ 3 Kt. DSG)

Unter Vorbehalt von Gerichtsverfahren, Grundbuch und Zivilstand
(eigene Regelungen)!

Die Grundsätze des Datenschutzes

Personendaten (Art. 3 DSG; § 2 Kt. DSG)

- **Personendaten**
¹sind *Angaben über* bestimmte oder bestimmbare natürliche oder juristische Personen oder eine Personengesellschaft des Handelsrechts.

- **besonders schützenswerte Personendaten**
besondere Gefahr der Persönlichkeitsverletzung
Angaben über
 - religiöse, weltanschauliche oder politische Haltung
 - Intimsphäre, Gesundheit, ethnische Zugehörigkeit
 - Massnahmen der Sozialhilfe
 - administrative und strafrechtliche Massnahmen und Sanktionen

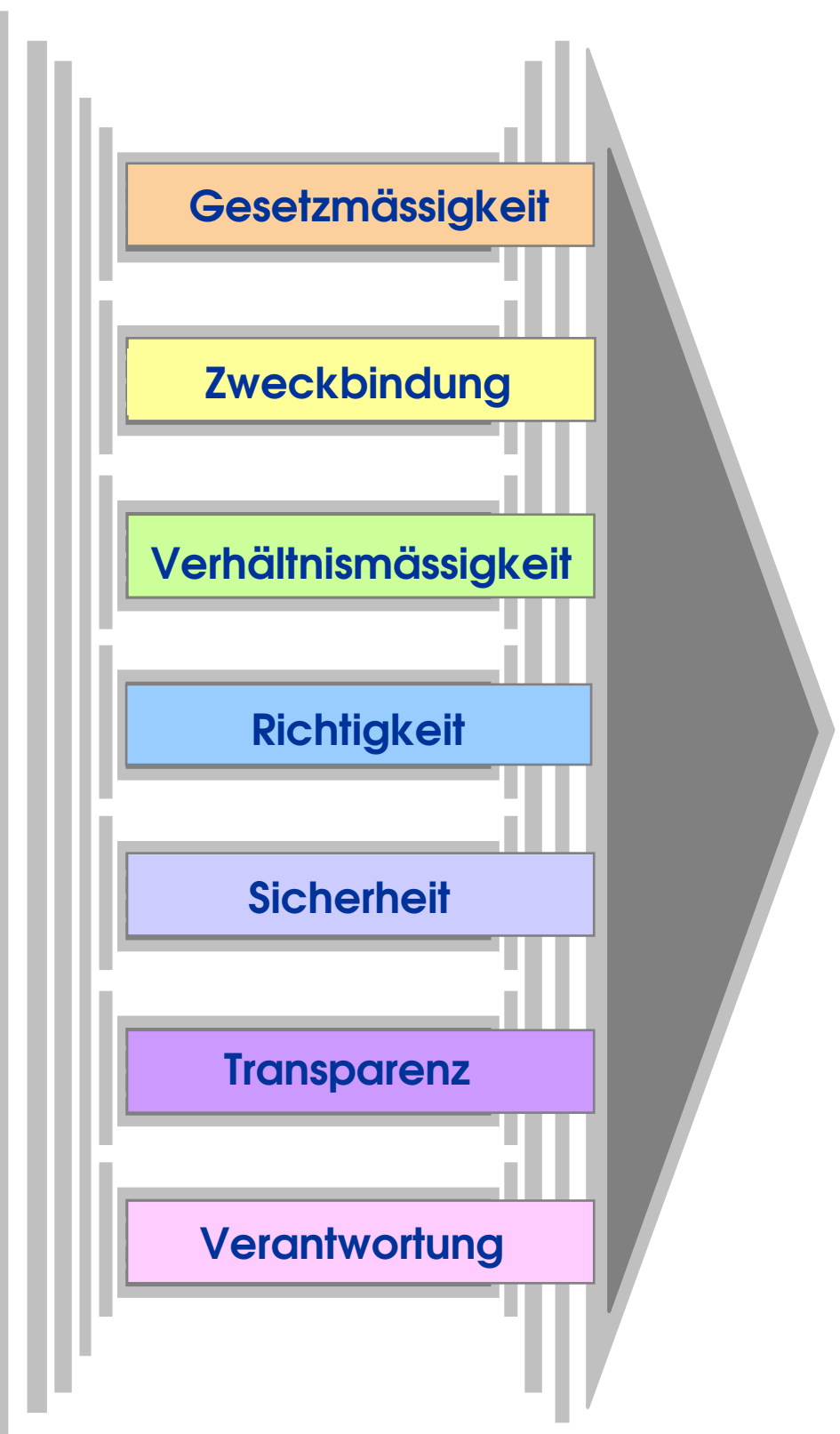
- **Persönlichkeitsprofile**
Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der natürlichen Person erlaubt.

Bearbeiten von Personendaten (Art. 3 DSG; § 2 Kt. DSG)

= jeder Umgang mit Personendaten

- unabhängig von den angewendeten Mitteln und Verfahren
- Erheben, Beschaffen, Aufzeichnen, Sammeln, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Vernichten usw.

Grundprinzipien des Datenschutzes



Prinzip der Gesetzmässigkeit (Art. 4 DSG; § 4 Kt. DSG)

- Personendaten dürfen zur Erfüllung von Aufgaben bearbeitet werden, für die eine Rechtsgrundlage besteht
- besonders schützenswerte Personendaten sowie Persönlichkeitsprofile bedürfen einer Rechtsgrundlage im Sinne eines formellen Gesetzes

Beispiel: Für polizeilich notwendige Datensammlungen liefert § 4 des Gesetzes über die Kantonspolizei die rechtliche Grundlage.

Prinzip der Zweckgebundenheit (Art. 4 DSG; § 4 Kt. DSG)

- Verwendung der Daten nur zum vorgegebenen Zweck
- keine Datensammlungen auf Vorrat

Prinzip der Verhältnismässigkeit (Art. 4 DSG; § 4 Kt. DSG)

- Bearbeitung nur soweit wie für Aufgabenerfüllung notwendig und geeignet
- Beschränkung auf das Notwendige und tatsächlich Erforderliche

Beispiel: falls Protokoll im Gemeinderat zirkuliert,
Personendaten anonymisieren!

Prinzip der Integrität (Art. 5 DSG; § 4 Kt. DSG)

- Daten müssen richtig (und vollständig) sein
- dem Verwendungszweck entsprechend
genügend genau, vollständig und nachgeführt

Kontrollrechte der Betroffenen

- Auskunftsrecht
- Berichtigungsrecht
- Beseitigungsanspruch

sind zu gewährleisten

Auskunftsrecht (Art. 15 - 20 DSG-LU)

gesuchstellende Person

- Mündliche oder schriftliche Anfrage
- Identitäts-Nachweis

Inhaber Datensammlung

- Mündliche oder Schriftliche Auskunft
- In der Regel kostenlos

Bekanntgabe von Personendaten an Private

§ 10 *Bekanntgeben an Private*

1 Unter Vorbehalt besonderer Geheimhaltungspflichten darf ein Organ privaten Personen und Organisationen Personendaten bekanntgeben, wenn

- a. ein **Rechtssatz** dazu verpflichtet oder ermächtigt oder
- b. die betroffene Person eingewilligt hat oder ihre **Einwilligung** nach den Umständen vorausgesetzt werden kann.

2 Personendaten aus allgemein zugänglichen amtlichen Veröffentlichungen darf ein Organ auf Anfrage in dem Umfang und in gleicher Weise bekanntgeben, wie sie veröffentlicht worden sind.

(...)

Der Generationenkonflikt – Die Generation „Y“

Ein kurzer Video-Film über die Generation „Y“



Motivation



The screenshot shows a Mozilla Firefox browser window displaying the website 20minuten.ch. The page features a navigation menu on the left with categories like Front, Nachrichten, Wirtschaft & Börse, Sport, Digital, Unterhaltung, Beauty & Fashion, Community, Gesundheit, Auto & Motorrad, Life & Lifestyle, Kochen, Service, Winterspecial, Weiterbildung, Ausgehen, Shop, and AutoImmoJob. The main content area is titled 'SOZIALE NETZWERKE' and contains an article with the headline 'Bund attestiert: Facebook nicht unsicher'. The article includes a photograph of a person's hands typing on a laptop keyboard, with the laptop screen displaying a Facebook profile. Below the photo, the text states: 'Bundesbeamte dürften auch weiterhin Facebook besuchen. Die Experten des Bundes sehen keine Sicherheitsgründe, die gegen die Benutzung des sozialen Netzwerks sprechen. Zu einer Sperrung könnte es trotzdem kommen. Von Lukas Mäder Mehr... 16 Kommentare'. At the bottom, a context box reads: 'Kontext: Facebook-Verbote sind unbegründet Schweizer sorgen sich um Daten im Internet'.

Aktuelles aus Luzern

INTERNET 08.06.2009 05:00

Facebook: Heikler Kampf gegen Surfer



🔍 Surfen in die weite Welt?
(Symbolbild Peter Appius/Neue LZ)

Der Bund droht seinen Beamten mit einem Facebook-Verbot. Auch die Stadt Luzern untersucht das Verhalten der Mitarbeiter im Internet.

Verstopfte Leitungen in der Bundesverwaltung: Bis zu 25 Prozent aller heruntergeladenen Daten stammen von der Internetplattform Facebook. Damit ist das soziale Netzwerk die zweithäufigst aufgerufene Seite.

Wie nutzen Angestellte der Stadt Luzern das Internet und welche Seiten rufen sie auf? Diese Daten werden zurzeit anonym bei 1400 Mitarbeitern erhoben. Ähnliche Untersuchungen des Bundes brachten Erstaunliches zu Tage: Die Seite, die in Bern am zweithäufigsten angeklickt wurde, war die Internetplattform Facebook.

Sollte die Luzerner Untersuchung zeigen, dass Mitarbeiter – entgegen einer Vereinbarung, die alle unterschreiben müssen – das Internet unerlaubt für private Zwecke nutzen, werde man alle ermahnen, sagt Personalchef Beat Däppeler. Verschiedene Luzerner Firmen haben längst damit begonnen, gewisse Seiten für ihre Angestellten zu sperren.

Gibt es einen Generationenkonflikt im Internet?

Das Unbekannte verunsichert und verängstigt

- Was ist die “nächste Generation”?

Warum?

- Sprache
- Kultur
- Forderungen und Erwartungen
- Lerngeschwindigkeit und -verhalten
- Nutzungsmuster

Was ist die Generation ‘Y’?

- **Generation Y** bezeichnet die Bevölkerungsgruppe, die zwischen 1978 (oder 1982*) und 1994 geboren wurde (also zwischen 15 und 27 Jahren)
- Es wird impliziert, dass die Mehrheit dieser Generation in ihrer Freizeit einen “online lifestyle” praktiziert

Diese 15- bis 27jährigen prägen nicht nur die virtuellen Computer- und realen Konsumentenwelten, sie treten jetzt auch ins Berufsleben ein.

Generation Y: einige wesentliche Statistiken

Ergebnis einer Befragung von College Studenten in den USA durch Junco und Mastrodicasa (2007):

- 97% besitzen einen Computer
- 94% besitzen ein Mobiltelefon
- 76% benutzen Instant Messaging (15% sind 24/7 online)
- 34% benutzen Webseiten als primäre Informationsquelle
- 28% schreiben einen Blog und 44% lesen Blogs
- 49% laden/tauschen Musik über peer-to-peer file sharing Netzwerke
- 75% haben einen Facebook-Account
- 60% besitzen einen portablen Musik/Video-Player (iPod usw.)

Warum macht uns das Sorgen?

Einige Beispiele ...

- ICT Werkzeuge zur Kommunikation / Kollaboration:

- Blogs

- Wikis

- Soziale Netzwerke (Xing, LinkedIn, ...)

- Instant Messenger

- Facebook

- Bebo

- Twitter

- Peer-to-Peer Netzwerke



Typische Gen-Y Web 2.0 Applikation

Das Schweizer Unternehmen, mit dem typischer Web 2.0 StartUp Namen **kooba** hat vor kurzem eine **Bilderkennungs-Suchmaschine** zusammen mit der ETH Zürich für das iPhone entwickelt.

- Kino-Filme
- Musik-Interpreten
- Sehenswürdigkeiten



www.kooba.com



Offene Fragen

- Soll der Zugang zu diesen Plattformen verboten, eingeschränkt oder zugelassen werden?
- Wie sollen Verbote und Einschränkungen umgesetzt werden?
- Wie bleibe ich attraktiv als Schule, wenn der Zugang nicht möglich oder eingeschränkt ist?
- Gelten solche Verbote oder Beschränkungen auch für die Freizeit der Mitarbeitenden?

Was ist mit uns? Sind wir Heuchler?

Wir:

- Informieren uns in Facebook, Xing usw. über Bewerber (meist im Sinne einer Negativ-Auslese, Kunden, Geschäftspartner usw.)
- Schalten Werbung in den virtuellen Umgebungen um unsere Produkte und Dienstleistungen der jungen Generation zu verkaufen (Second Life)
- Benutzen Informationen aus virtuellen Umgebungen, um Nutzungs-Profile zu erstellen, Trends zu erkennen und daraus Schlüsse für die Produktentwicklung und das Marketing zu ziehen.

Was bedeutet das für uns?

- Wir sind kaum agil genug, um “mitzuhalten”
- Wir sind fokussiert auf die Bedrohungen, nicht auf die Chancen
- Die Auflösung der Grenzen zwischen Privat und Schule (Geschäftsleben) ist nicht aufzuhalten, wir stemmen uns gegen die Flut.
- Externe und interne Applikationen und Systeme konvergieren (wer hat noch zwei Handys, 2 Agenden usw.?)
- Der Kontrollverlust über Daten ist erheblich!
- Das Bedrohungspotential für die Akteure (physisch und logisch) steigt

Verschwimmende Grenzen

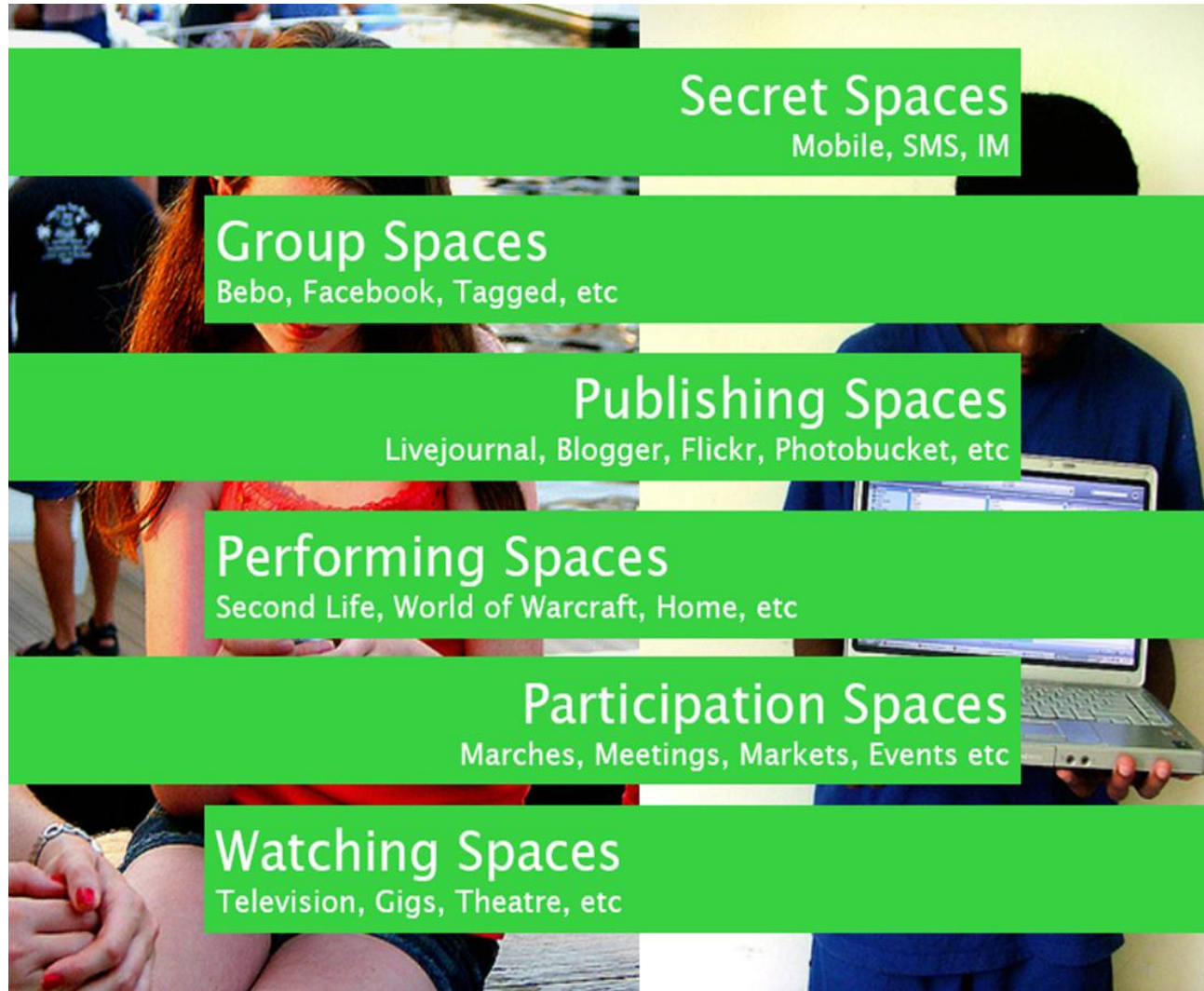
Öffentlich

Privat

Persönlich

**Politisch/
Professionell**

Wo die Generation „Y“ lebt ...



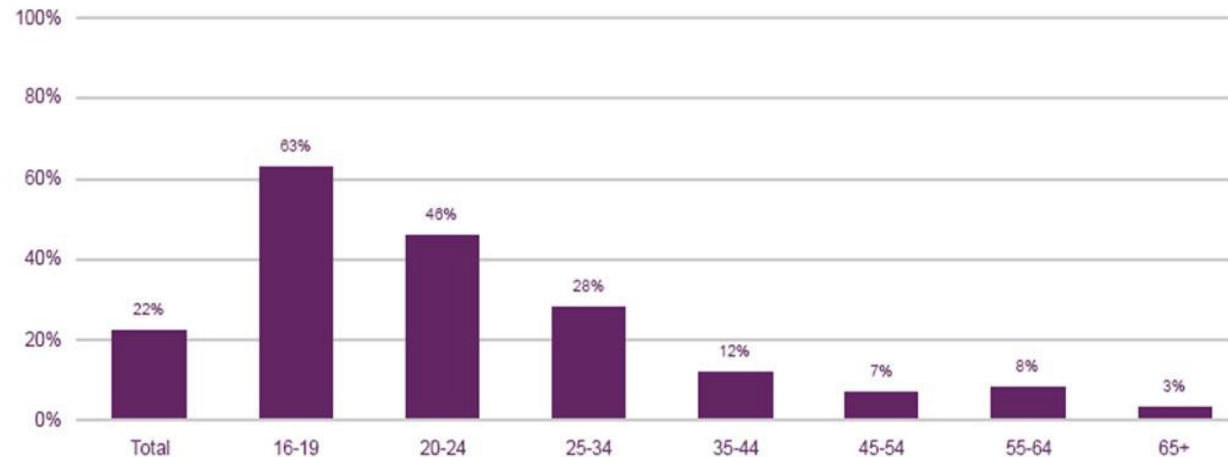
Ewan McIntosh
(<http://edu.blogs.com/>)

Generation „Y“ ist die „erste ihrer Art“



Nearly two in three 16-19 year old internet users have a profile on a social networking site

Age profile of adults who have set up a profile on a social networking site



IN28A – I'd like to read out a number of things people might do using the types of technologies we've been talking about. For each one, could you please tell me if you've done it, or you'd be interested in doing it, or you're not interested in doing it?
Base: All who use the internet at home or elsewhere (1723)
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in October to December 2007

Schlussfolgerungen

- Wir müssen wesentlich agiler sein und differenzierter mit dem Problem umgehen – Verbote nützen nichts
- Gegenseitige Erziehung (setzt gegenseitige Bereitschaft zum Lernen und Zuhören voraus)
- Wir müssen die Bedürfnisse der Generation Y aktiv unterstützen. Der Zugewinn an Innovationskraft hat einen hohen Marktwert (pädagogischer Wert?!)
- Es ist eine Herausforderung, aber keine Bedrohung

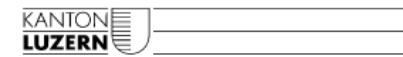
Die Merkblätter des Datenschutzbeauftragten des Kantons Luzern im Bereich der Schulen

Merkblätter des DSBs

Die 4 Merkblätter zum Thema Schule vom Luzerner Datenschutzbeauftragten

- Merkblatt **Schulen ans Internet**
- Merkblatt **Internet-Auftritt einer Schule**
- Merkblatt **Publikationen von Schulen**
- Merkblatt **Datenschutz in der Schule**

<http://www.datenschutz.lu.ch>



Datenschutzbeauftragter
des Kantons Luzern
Bahnhofstrasse 15
6002 Luzern
Telefon 041 228 66 06
dsb@lu.ch
www.datenschutz.lu.ch

Merkblatt Schulen ans Internet

1. Zweck des Merkblattes

An immer mehr Schulen nutzen Lehrer und Schüler das Internet vielfältig und werden je länger je mehr effektiv genutzt. Dabei werden Gefahren durch die vermehrte Nutzung des Internets wie ihnen entgegengetreten werden kann.

2. Datenschutz im Internet

Bei jeder Aktivität im Internet, ob beim Schreiben eines eMails oder beim Ausfüllen eines Online-Formulars oder beim Eintrag in



Merkblatt Schule ans Internet - Gefahren

- Spuren im Internet (online-Formulare, Newsgroups, Gästebücher, Facebook, Netlog etc.) -> Persönlichkeitsprofil
- Viren, Trojaner, Würmer (drive-by-Infection)
- eMails (unsichere Kommunikation)
- Mögliche Rufschädigung, welches durch das Surfverhalten der Benutzer entstehen könnte
- SPAM! Sobald Sie Ihre eMail Adresse auf verschiedenen Webseiten Preis geben, ist die Wahrscheinlichkeit sehr hoch, dass Sie immer mehr SPAM erhalten.

Merkblatt Schule ans Internet – **technische Massnahmen**

- Aktualisieren Sie Ihre Software regelmässig (Betriebssystem, Browser, etc.)
- Schützen Sie Ihren Internet-Zugang mit einer Firewall.
- Halten Sie Ihren Virenschutz aktuell! (update täglich)
- Sichern Sie Ihre Daten regelmässig.
- Setzen Sie einen SPAM-Filter ein.
- Verwenden Sie einen URL-Filter.
- Trennen Sie das Schulverwaltungs-Netzwerk vom Schüler-Netzwerk.

Merkblatt Schule ans Internet – **organisatorische Massnahmen**

- Zugriffsschutz auf Computern. Jeder Benutzer benutzt seine persönliche Benutzer-ID und Passwort und verrät das Passwort nicht. (Identitätsdiebstahl)
- Verwenden Sie starke Passwörter (Sommer = So\$Mmer04)
- Senden Sie keine sensiblen (vertrauliche) Daten unverschlüsselt via eMail über das Internet.
- Erstellen Sie ein Pflichtenheft für die ICT-Verantwortlichen.
- Machen Sie die IT-Benutzer-Richtlinien (Netiquette, Internet-Weisung, eMail-Weisung etc.) bekannt.
- Schulen Sie die Benutzer. Machen Sie die Benutzer auf die Gefahren und Risiken aufmerksam. Appellieren Sie an die Eigenverantwortung der Benutzer.
- Schützen Sie den Zutritt zu Ihrer IT-Infrastruktur vor unbefugten Personen.

Merkblatt Internet-Auftritt einer Schule - **Gefahren**

- Personendaten und Fotos werden ohne Einwilligung der Betroffenen veröffentlicht.
- Links auf andere Webseiten sind mit Sorgfalt einzusetzen. Sie sind nicht verantwortlich für deren Inhalt, jedoch für den Zugriff.
- Video- und Web-Kameras können falsch eingesetzt werden.

Merkblatt Internet-Auftritt einer Schule - Massnahmen

- Holen Sie sich die Einwilligung der Betroffenen, wenn Sie persönliche Daten und Fotos veröffentlichen wollen.
- Vermerken Sie auf Ihrer Webseite, dass die für die Nutzung und Inhalte der Links keine Verantwortung übernehmen können.
- Setzen Sie wo möglich keine Video- und Web-Kameras ein. Ansonsten nur, wenn alle Vorkehrungen getroffen werden das DSB nicht zu verletzen.
- Stellen Sie nur PDF-Dokumente und keine Word- und Excel-Dokumente zum Download zur Verfügung.
- Schützen Sie Ihren Web-Server (Hardening, Monitoring, Updates, Einsatz sicherer Web-Applikationen etc.)

Fazit - Empfehlung:

Verzichten Sie wenn möglich auf die Veröffentlichung von personenbezogenen Daten und Fotos.

Merkblatt Publikationen von Schulen - **Massnahmen**

- Holen Sie sich die Einwilligung der Betroffenen, wenn Sie persönliche Daten und Fotos in einer Publikation (Schulbroschüre, Jahressbücher etc.) veröffentlichen wollen.

Merkblatt Datenschutz in der Schule - **Gefahren**

- Personendaten werden ohne Grund gesammelt.
- Personendaten werden zu schnell an Dritte bekannt gegeben.
- Schulzimmer und Schränke sind nicht abgeschlossen – Ordner und Blätter liegen einsehbar im Lehrzimmer.
- Computer sind nicht gebührend gegen unbefugten Zugriff geschützt.

Merkblatt Datenschutz in der Schule - **Massnahmen**

- Halten Sie Personendaten unter Verschluss.
- Sichern Sie Ihren Computer mit einem starken Passwort.
- Versenden Sie keine vertraulichen Informationen oder Personendaten per eMail, ausser die Übermittlung erfolgt verschlüsselt.
- Erzählen Sie keine vertraulichen Informationen weiter.
- Notieren Sie keine persönlichen Daten der Schülerinnen und Schüler in der Schulchronik und anderen Publikationen.

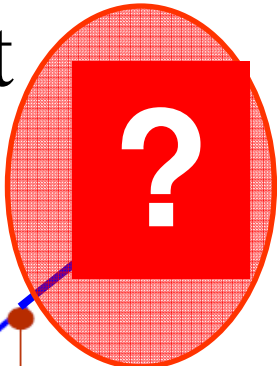
IT-Sicherheit und Informationssicherheit

Ziele der Informationssicherheit

Was wollen wir damit erreichen?

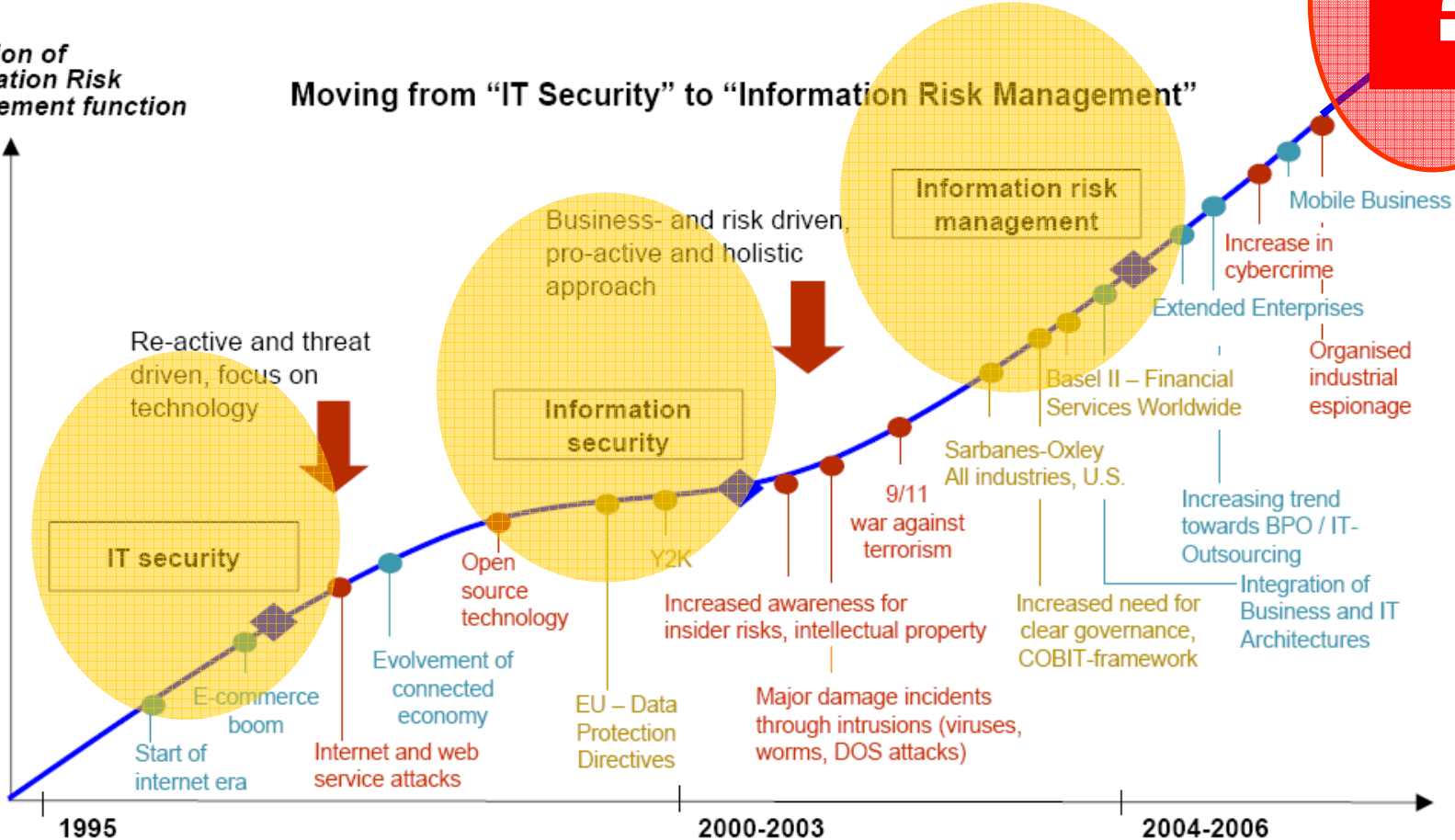
- Einhaltung der Gesetze und Verordnungen (DSG, GebüV, etc.)
- Sichert die Erreichung der Unternehmensziele (Schulziele)
- Die Schule und deren Schulleitung (Management) vor Haftungsklagen schützen
- Daten-Missbrauch und –Diebstahl erkennen und verhindern
- Alle Mitarbeitenden inkl. Schüler und Lehrpersonen in Bezug auf Sicherheit sensibilisieren
- Die Rest-Risiken kennen und akzeptieren. Es gibt keine 100% Sicherheit!

Die Entwicklung der Informationssicherheit



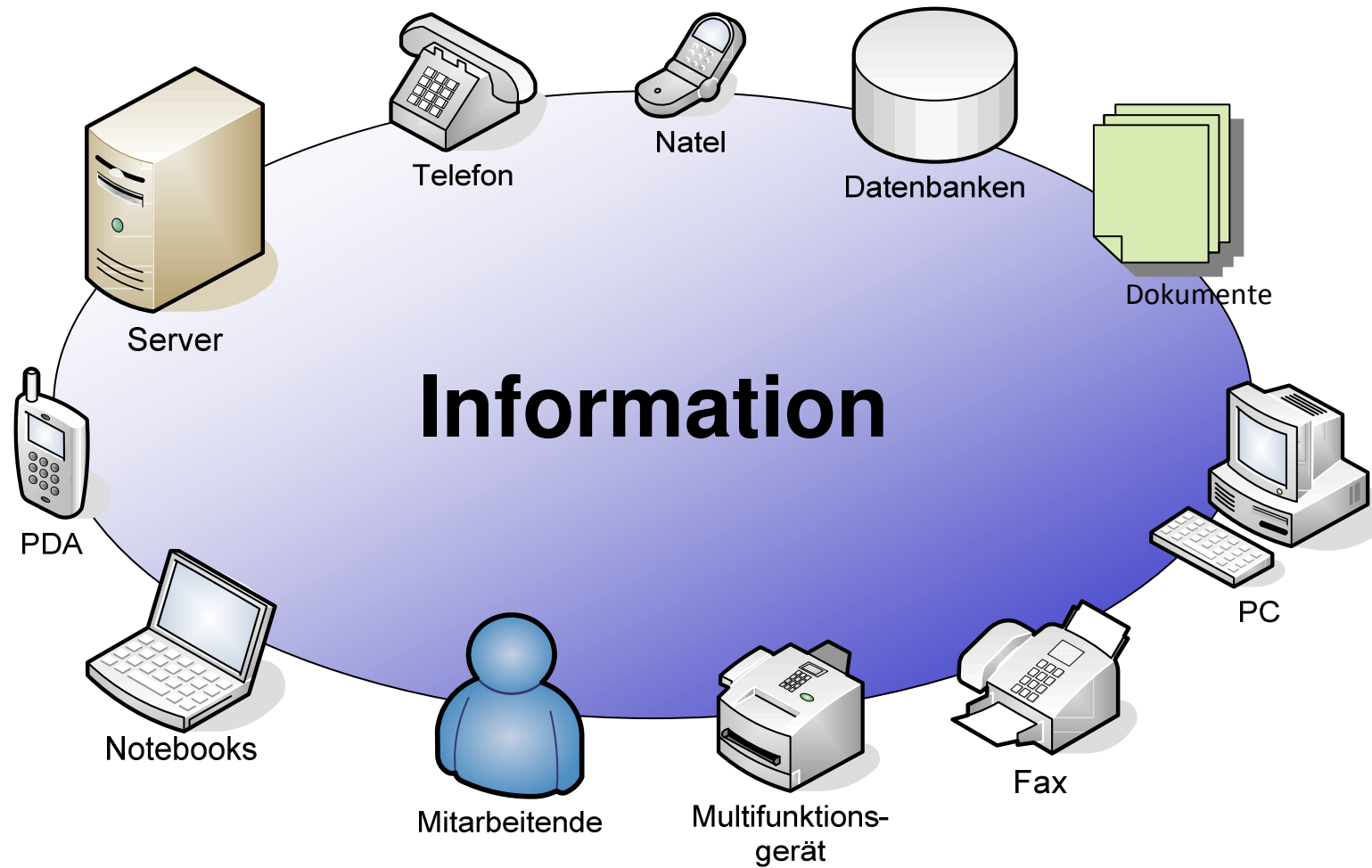
Evolution of Information Risk Management function

Moving from "IT Security" to "Information Risk Management"



Emerging threats, evolving business models and increasing regulatory requirements

Informationen sind überall



IT-Sicherheit und Informationssicherheit



Was ist IT-Sicherheit?

Bedrohung



Schwachstelle



Gefahr



Risiko

Vorsätzliche Handlungen



- Höhere Gewalt
- Technisches Versagen



- Organisatorische Mängel
- Menschliche Fehlhandlungen



Schwachstellen



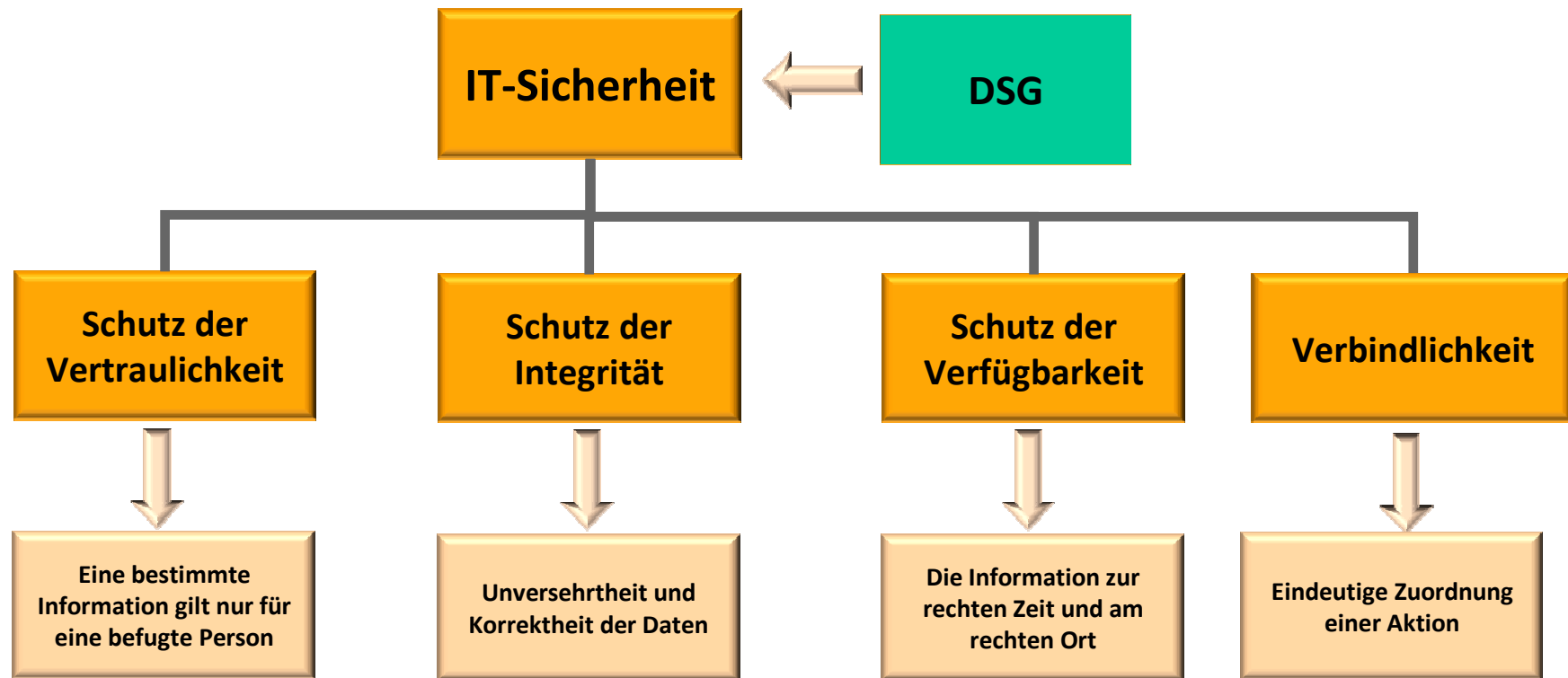
Schutzmassnahmen

$R = \text{Wahrscheinlichkeit (Häufigkeit)} * \text{Ausmass des Schadenereignisses}$

Wer sind die Täter?

- Geheimdienste (Echelon, NSA, MI5, ...)
- Industriespionage (organisierte Kriminalität)
- Hacker (Geltungsbedürfnis)
- Cracker (Finanzelle Interessen)
- Softwareentwickler (Back Doors)
- Fremdpersonal (externe Mitarbeitende, Temp-Mitarbeitende)
- Administratoren
- Schüler und Lehrpersonen (Mitarbeitende)
- Mitbewerber/Konkurrenten

Die 3 Pfeiler der IT-Sicherheit „Datensicherheit“



Vertraulichkeit

- Vertraulichkeit ist gegeben, wenn sichergestellt werden kann, dass Informationen nicht durch unautorisierte Personen, Instanzen oder Prozesse eingesehen werden können.
- Vertraulich: Nicht für die Öffentlichkeit bestimmt, mit Diskretion behandeln, geheim
(Quelle Duden)

Integrität

- Integrität ist gewährleistet, wenn Daten oder Systeme nicht unautorisiert manipuliert werden und dadurch ihre Verfügbarkeit nicht beeinflusst wurde.
- Makellosigkeit, Unbescholtenheit, Unbestechlichkeit

(Quelle Duden)

Verfügbarkeit

- Verfügbarkeit ist gewährleistet, wenn die Funktionalität von Software, Hardware und Services nicht unbefugterweise beeinträchtigt wurde.
- Verfügbar: (augenblicklich) zur Verfügung stehend, für den sofortigen Gebrauch, vorhanden

(Quelle Duden)

Verbindlichkeit

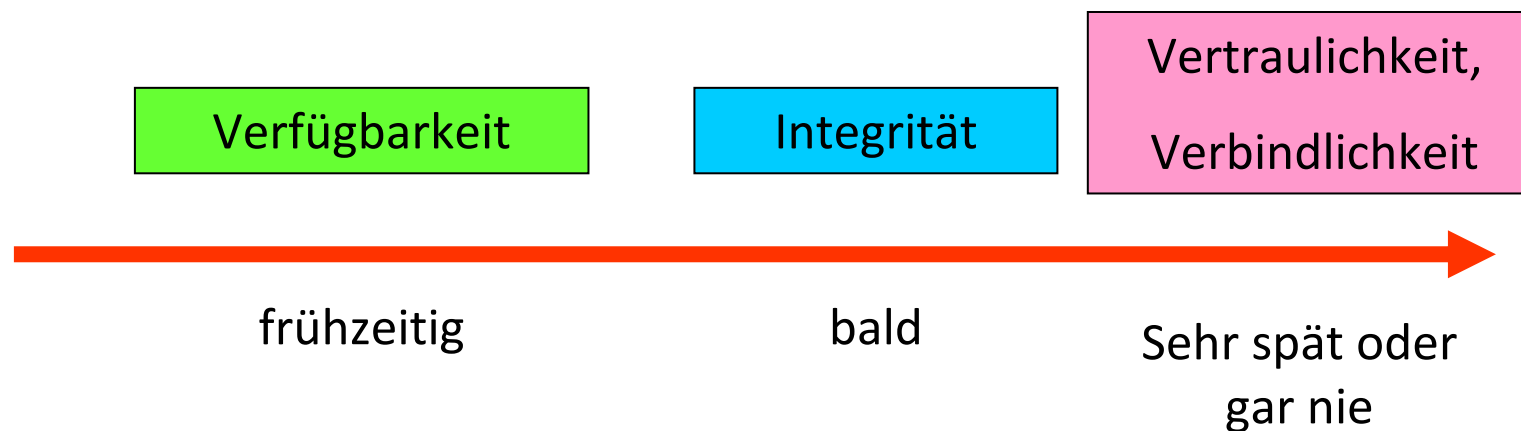
- Verbindlichkeit herrscht vor, wenn alle Aktionen einer Instanz eindeutig zugeordnet und nicht geleugnet werden können.
- Verbindlichkeit, Recht: Verpflichtung des Schuldners zu seiner Leistung, sie entspricht der Forderung auf der Gläubigerseite

(Quelle Duden)

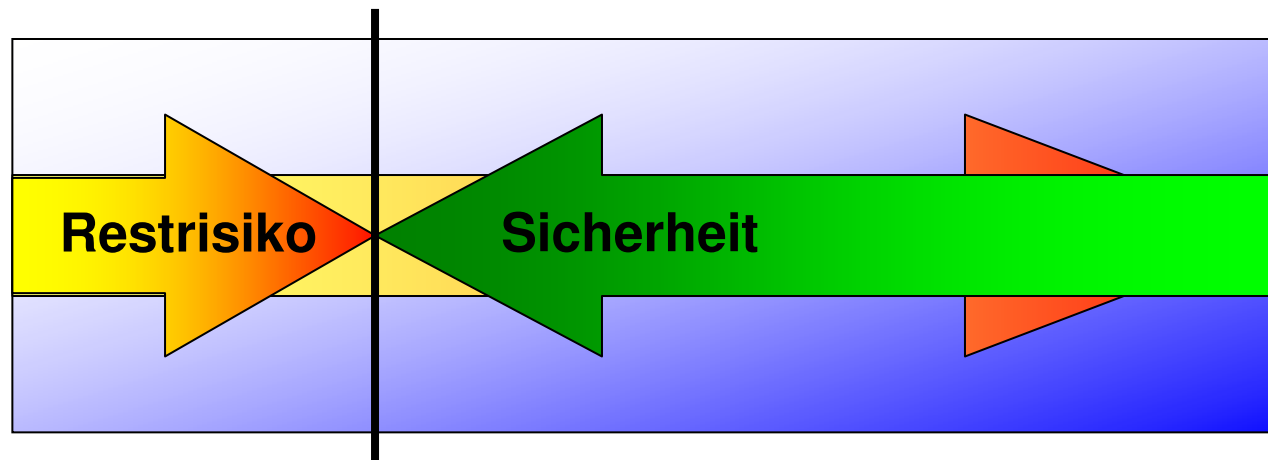
Grundziele

- Verfügbarkeit
- Vertraulichkeit
- Integrität
- Verbindlichkeit

Zeitpunkt der Entdeckung eines Grundzielverlustes



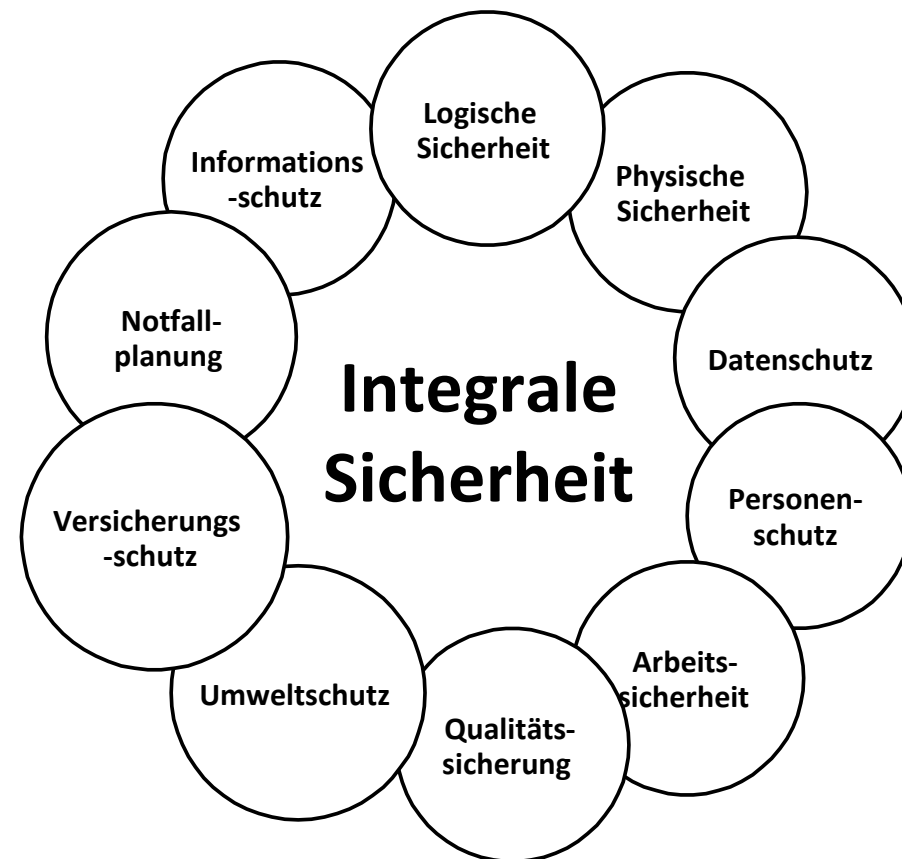
Sicherheit ist ... keine
unvertretbaren Risiken mehr
haben!



und nicht: es kann nichts mehr passieren

Integrale Sicherheit

- Umfassende Betrachtung aller Sicherheitsaspekte einer Organisation
- Sicherheit in der Verarbeitung von Information, nicht beschränkt auf die elektronische Verarbeitung

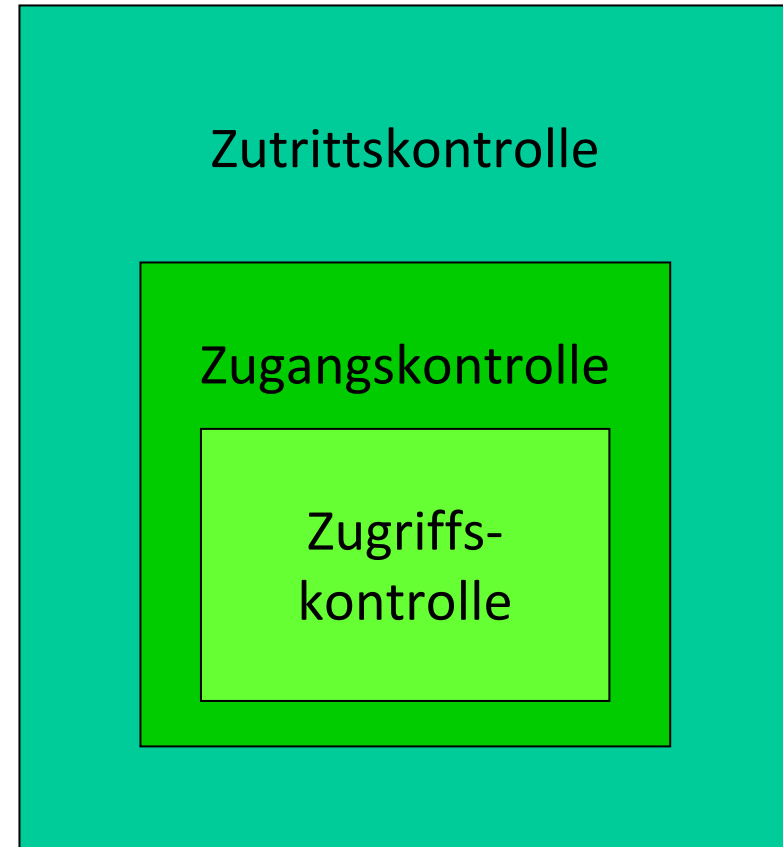


Die 4 Layer des Sicherheits- Managements Verteidigungsstrategie

Layer 1	Technologie (20%) Firewall, Virenschutz, IDPS, NAC, DMZ
Layer 2	Management (20%) Netzwerk-Management, Vulnerability Management, Audit, Pentest
Layer 3	Organisation (20%) Weisungen, Prozesse (ITIL), Kontrolle, BCM/DR
Layer 4	Mensch (40%) Ausbildung, Sensibilisierung

Zutritts-, Zugangs-, Zugriffskontrolle

- Zutrittskontrolle
 - gerätebezogen
 - Schutz des physischen Systems
- Zugangskontrolle
 - personenbezogen
 - Schutz des logischen Systems
- Zugriffskontrolle
 - „Daten“-bezogen
 - Schutz der Operationen



Wie sieht es bei Ihnen aus?



- Sensitive Informationen werden ungeschützt verschickt oder auf externen Speichermedien abgelegt
- Notebooks, PDAs, USB-Sticks etc. gehen verloren
- Zutritt zu Gebäuden ist kaum gesichert und fremde Personen können sich unbehelligt bewegen
- Mitarbeitende sind hilfsbereit und geben bereitwillig Auskunft
- Vertrauliche Dokumente liegen auf dem Pult, Drucker, Fax, Kopierer
- Whiteboard im Sitzungszimmer, public Transfer-Verzeichnis
- Bürotüren und Aktenschränke werden nicht abgeschlossen
- Sensitive Angelegenheiten werden fast überall am Telefon besprochen
- Datenträger und Akten werden nicht korrekt vernichtet
- Verlassen des Arbeitsplatzes ohne die Bildschirmsperre zu aktivieren

Ihr Nutzen

- Geringere Verwundbarkeit
- Keine falsche Sicherheit
- Bewusster Umgang mit Informationen
- Gefahren kennen, Restrisiko ist bekannt
- Sorgfaltspflicht erfüllt
- Einhalten aller Gesetze (Datenschutz, GebüV, etc.)
- Standortvorteil (Wettbewerbsvorteil) -> Sicherheit = Vertrauen
- Fördert das „Sicherheitsbewusstsein“ der Mitarbeiter (Sicherheitskultur)
- Steigert die Möglichkeit neue ICT-Projekte (z.B. LernJobs) sicher und schneller anzugehen



Ausblick / Trends

- Weiter wachsende Mobilität / “Intelligente” Geräte / Spontane Netzwerke (GPS, RFID, DNA, Genforschung, Nanotechnik etc.)
- Virtualisierung & Miniaturisierung der Hardware, Cloud-Computing
- Kommunikations-Tools (Skype, Teamviewer etc.)
- Erhöhte Abhängigkeit von komplexer Technologie
- Erhöhte rechtliche / regulatorische Anforderungen
- Die Trojaner werden raffinierter und tarnen sich als Microsoft oder Java Update
- Open-Source Angebote werden missbraucht (Abofallen)
- Die Fälle des Identitäts-Diebstahls werden zunehmen
- Kosten- / Nutzen-Betrachtungen / Sourcing / Fusionen / Übernahmen
(CH-Unternehmen wird durch ein Unternehmen in den USA oder China übernommen)

Noch Fragen ???

