



Datenschutzbeauftragter des Kantons Luzern



Datenschutz und Informationssicherheit


**Gemeindeschreiberverband Amt Willisau
Stamm – 11. Nov. 2009**

Wolfgang Sidler

12.11.2009 Seite 1

Datenschutzbeauftragter des Kantons Luzern

Zu meiner Person

Ausbildung	<ul style="list-style-type: none">▪ Master in Information Security FHZ▪ Wirtschaftsinformatiker
Engagement	<ul style="list-style-type: none">▪ Mitarbeiter des Datenschutzbeauftragten des Kantons Luzern (Teilzeitpensum)▪ Präsident des Vereins „InfoSurance“  InfoSurance und ihr Computer ist sicher.▪ Prüfungsexperte für Informatik-Lehrlinge im Kanton Luzern
Berufserfahrung	<ul style="list-style-type: none">▪ 23 Jahre Informatik-Erfahrung▪ Mitautor „IT-Sicherheitshandbuch für die Praxis“▪ 6 Jahre IT-Security Officer bei einer renommierten Schweizer Privat Bank▪ European Security Consultancy Manager bei einer weltweit führenden Schweizer Versicherungs-Gesellschaft▪ 3 Jahre Erfahrung im Ausland im Bereich IT, IT-Sicherheit und Projekt-Management (USA und Middle-East)
Kontakt	<p>E-mail: wolfgang.sidler@sidler-security.ch Webseite: www.sidler-security.ch</p>

12.11.2009 Seite 2

LUZERN

KANTON
LUZERN

Datenschutzbeauftragter des Kantons Luzern

Ziele des Vortrages

- Datenschutz kennen und anwenden können
- Die Kernelemente der IT-Sicherheit und der Informationssicherheit kennen

12.11.2009 Seite 3

LUZERN

KANTON
LUZERN

Datenschutzbeauftragter des Kantons Luzern

Agenda

- Einführung Datenschutz
- Der Datenschutzbeauftragte des Kantons Luzern
- IT-Sicherheit und Informationssicherheit
- Ausblick - Trends
- Fragen und Diskussion

12.11.2009 Seite 4

Datenschutzbeauftragter des Kantons Luzern

LUZERN

Einführung Datenschutz

Datenschutz schützt nicht Daten, sondern Personen vor Missbrauch Ihrer Daten. Dem Grundsatz nach soll eine Person selbst bestimmen, wer was über sie weiss (sog. informationelle Selbstbestimmung)

KANTON LUZERN

12.11.2009 Seite 5

Datenschutzbeauftragter des Kantons Luzern

LUZERN

Datenschutz-Pannen (1/3)

- **Patientendaten im Müll:**
12 kg Unterlagen der CSS auf der Strasse gefunden.
Ein Anwohner will einen fremden Kehrichtsack ordnungsgemäss in den Container werfen. Als der Sack dabei reisst, fallen gut 12 kg Krankenunterlagen der Krankenkasse CSS auf die Strasse, darunter Krankengeschichten, Versicherungsabschlüsse, Mandatserteilungen, usw.
- **Einsatzprotokoll im Internet**
Die Hessische Polizei stellt versehentlich ein 13 Seiten langes Einsatzprotokoll von Verkehrskontrollen ins Netz. Darin finden sich Namen, Geburtsdaten, aktuelle Adressen der Kontrollierten, „eventuelle Vorstrafen“, Automarke, Kennzeichen sowie Gesetzesverstösse. Die Daten standen ab Februar 2006 fast ein Jahr im Netz.
- **Amerikanische Zustände**
privacyrights.org schätzt, dass in den USA insgesamt 217,551,182 Personen vom Diebstahl oder Verlust ihrer besonders schützenswerten Personendaten betroffen sind.

KANTON LUZERN

12.11.2009 Seite 6

Datenschutzbeauftragter des Kantons Luzern

Datenschutz-Pannen (2/3)

Pannenland Grossbritannien

- **Januar 2008**
Dem britischen Verteidigungsministerium werden auf einem Notebook Informationen über rund 600'000 potenzielle Rekruten gestohlen.
- **Dezember 2007**
Daten von drei Millionen Führerscheinkandidaten und 7'500 Fahrzeugen werden versehentlich gelöscht.
- **November 2007**
Das Nationalen Gesundheitssystems (NHS) verliert vertraulichen Informationen von 160'000 kranken Kindern.
- **November 2007**
Die Steuerbehörden verlieren zwei CDs mit den persönlichen Daten von 25 Millionen Personen, bzw. 7.25 Millionen Familien, die Kindergeld beziehen.

12.11.2009

Seite 7

Datenschutzbeauftragter des Kantons Luzern

Datenschutz-Pannen (3/3)


- **Telefonauskunft**
Die Auskunft der Telekom schlampte 2002 und gab die Adresse des Frauenhauses Tübingen heraus. Daraufhin musste die ganze Einrichtung schliessen, weil die Sicherheit der Frauen nicht mehr gewährleistet war.
- **Brief von der Bank**
Eine englische Kundin der britischen Grossbank HBOS bekam 2007 nicht nur ihren eigenen Kontoauszug zugeschickt, sondern gleich fünf Briefe mit insgesamt rund 2.500 Seiten, die Angaben zu den Finanzverhältnissen von 75.000 Kunden enthielten.
- **Grösster Fall**
Die Kaufhauskette TJX Companies Inc. gibt 2007 öffentlich bekannt, dass sein Datenverarbeitungssystem für Kreditkartendaten gehackt wurde. Es wurden 45,7 Millionen Kreditkarten-Datensätze und über 455'000 Kundenunterlagen zur Warenrückgabe (samt Kundennamen und Führerscheindaten) gestohlen.

12.11.2009

Seite 8

Datenschutzbeauftragter des Kantons Luzern

Gesetzliche Verankerung des Datenschutzes

LUZERN 	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

12.11.2009 Seite 9

Datenschutzbeauftragter des Kantons Luzern

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.

12.11.2009 Seite 10

Datenschutzbeauftragter des Kantons Luzern

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?


- Das kantonale Datenschutzgesetz konkretisiert diese Bestimmung der Bundesverfassung.
- Es gilt für die gesamte kantonale Verwaltung (für Private und Bundesbehörden: eidgenössisches Datenschutzgesetz, EDÖB).
- Es ist ein Querschnittsgesetz, findet also auf alle Bereiche gleich Anwendung. Ein Gesetz für alle Bereiche ist effizient, hat aber einen Nachteil: keine spezifischen Regeln.
- Diese finden sich in Spezialgesetzen, z.B. Polizeigesetz, Gesundheitsgesetz, etc.

12.11.2009

Seite 11


Datenschutzbeauftragter des Kantons Luzern

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)!

12.11.2009

Seite 12

Datenschutzbeauftragter des Kantons Luzern




**Die Grundsätze des
Datenschutzes**

KANTON
LUZERN

12.11.2009 Seite 13

Datenschutzbeauftragter des Kantons Luzern



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.

12.11.2009 Seite 14

LUZERN

Datenschutzbeauftragter des Kantons Luzern

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.

12.11.2009 Seite 15

LUZERN


Datenschutzbeauftragter des Kantons Luzern

Grundprinzipien des Datenschutzes

The diagram illustrates the seven principles of data protection as the pillars of a classical building. The pillars are labeled from left to right: **Gesetzmässigkeit** (orange), **Zweckbindung** (yellow), **Verhältnismässigkeit** (green), **Richtigkeit** (blue), **Sicherheit** (purple), **Transparenz** (pink), and **Verantwortung** (light pink). A small arrow points to the 'Richtigkeit' pillar.

12.11.2009 Seite 16

Datenschutzbeauftragter des Kantons Luzern



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.

12.11.2009

Seite 17

Datenschutzbeauftragter des Kantons Luzern



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

- Verwendung der Daten nur zum vorgegebenen Zweck
 - Gesetzliche Grundlage ist vorhanden,
 - Zweck bei der Beschaffung wurde angegeben,
 - Zweck aus den Umständen ist ersichtlich.
- keine Datensammlungen auf Vorrat

12.11.2009

Seite 18

Datenschutzbeauftragter des Kantons Luzern

LUZERN


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 - Datensparsamkeit

Beispiel: falls Protokoll im Gemeinderat zirkuliert, Personendaten anonymisieren!

Seite 19

12.11.2009



Datenschutzbeauftragter des Kantons Luzern

LUZERN

Verhältnismässigkeit




Seite 20

12.11.2009



Datenschutzbeauftragter des Kantons Luzern




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

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

12.11.2009 Seite 21

Datenschutzbeauftragter des Kantons Luzern



Kontrollrechte der Betroffenen

- Auskunftsrecht
- Berichtigungsrecht
- Beseitigungsanspruch

sind zu gewährleisten

12.11.2009 Seite 22

Datenschutzbeauftragter des Kantons Luzern

Auskunftsrecht (Art. 15 - 20 DSG-LU)

- Identität von Anfragenden (Gesuchsteller)
 - Datenbekanntgaben per Telefon
 - Anfragen per E-Mail
 - Datenbekanntgabe per Fax
- Voraussetzungen von Datenbekanntgaben
 - Amtsgeheimnis gilt grundsätzlich auch zwischen den verschiedenen Stellen innerhalb der Verwaltung.
 - Personendaten dürfen anderen Stellen grundsätzlich nur dann bekanntgegeben werden, wenn eine entsprechende ausdrückliche gesetzliche Grundlage dies zulässt oder die betroffene Person der Datenbekanntgabe zugestimmt hat.
 - An Privatpersonen darf ausschliesslich Auskunft über ihre **eigenen** Daten gegeben werden.

Seite 23

Datenschutzbeauftragter des Kantons Luzern

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.

(...)

Seite 24

Datenschutzbeauftragter des Kantons Luzern

Bekanntgabe an Private durch die Einwohnerkontrolle

§ 11 Bekanntgeben an Private durch die Einwohnerkontrolle

- 1 Die Einwohnerkontrolle gibt auf Gesuch privaten Personen und Organisationen, die ein schutzwürdiges Interesse glaubhaft machen, Namen, Vornamen, Geschlecht, Geburtsdatum und Adresse bekannt.
- 2 Soweit diese Angaben zur Wahrung des schutzwürdigen Interesses nicht ausreichen, gibt sie auch Auskunft über Beruf und Titel von Einzelpersonen, Zivilstand, Heimatort, Staatsangehörigkeit und zivilrechtliche Handlungsfähigkeit sowie über Ort und Datum des Zu- und Wegzugs.
- 3 Die Einwohnergemeinde kann durch Reglement oder Gemeindeordnung bestimmen, dass auch ohne Glaubhaftmachung eines schutzwürdigen Interesses Personendaten gemäss Absatz 1 zu politischen, kulturellen, gesellschaftlichen, wohltätigen und **wissenschaftlichen Zwecken** veröffentlicht oder auf Anfrage hin bekanntgegeben werden.
- 4 Jede betroffene Person kann bei der Einwohnerkontrolle das Bekanntgeben ihrer Personendaten ohne Angabe von Gründen **sperr**en lassen; die Sperre ist indessen unwirksam, wenn die Einwohnerkontrolle durch Rechtssatz zum Bekanntgeben verpflichtet ist oder **der Gesuchsteller eine Behinderung in der Verfolgung schutzwürdiger Ansprüche gegenüber der betroffenen Person glaubhaft macht**.

Seite 25

Datenschutzbeauftragter des Kantons Luzern

Fazit


Jeder Mensch hat ein Recht darauf, dass er selber darüber bestimmen kann, welche Informationen über ihn wann, wo und wem bekannt gegeben werden. Dieses Recht kann jedoch anderen gewichtigen Sicherheitsaspekten entgegenstehen.

Zudem stellt sich auch die Frage, inwieweit der einzelne vor der sorglosen Bekanntgabe persönlicher Daten geschützt werden kann. Es muss stets von Fall zu Fall abgewogen werden, welches Interesse nun gewichtiger zu beurteilen ist.

Seite 26

Datenschutzbeauftragter des Kantons Luzern

Der Datenschutzbeauftragte des Kantons Luzern



The screenshot shows the homepage of the Data Protection Officer of the Canton of Lucerne. The page features a navigation menu on the left with links to 'Auftrag', 'Rechtsgrundlagen', 'Rechtsprechung', 'News', 'Themen', 'Publikationen', 'Register der Datensammlungen', 'Fragen an den DSB', and 'Sitemap'. The main content area includes a welcome message, a brief description of the DPO's role, and a list of publications. A search bar and a 'Schnell Gefunden' section are also visible.

12.11.2009 Seite 27

Datenschutzbeauftragter des Kantons Luzern

Organisation und Stellung


- **Organisation**
 - 90 Stellenprozente
 - Standort: Bahnhofstrasse 15, 6002 Luzern
 - administrativ der Staatskanzlei unterstellt
 - Webseite: www.datenschutz.lu.ch
- **Stellung**
 - Kantonales und kommunales Kontrollorgan im Sinne des Bundesgesetzes über den Datenschutz
 - Verwaltungsunabhängig
 - Untersteht dem Amtsgeheimnis

12.11.2009 Seite 28

Datenschutzbeauftragter des Kantons Luzern

Gesetzlicher Auftrag

- Überwachung der Anwendung der Vorschriften über den Datenschutz
- Führung des Registers der Datensammlungen
- Beratung der Behörden
- Mitwirkung bei der Gesetzgebung
- Vermittlung zwischen öffentlichen Organen und Privaten
- Information (Merkblätter etc.)




Seite 29

Datenschutzbeauftragter des Kantons Luzern

Unsere Arbeitsweise

- **Beratung und Unterstützung**
 - Direkter Zugang (Telefon, E-Mail, Kontaktformular)
 - Keine Formalismen
 - Beratung vor Ort
- **Aufsicht und Kontrolle**
 - Vorgängige Koordination
 - Vorbesprechungen
 - Gelegenheit zur Stellungnahme
 - Schlussbesprechung
 - Nachfassen/Feedback




Seite 30

Datenschutzbeauftragter des Kantons Luzern

Unsere Grundsätze

- ✓ **Unabhängig**
- ✓ **Partnerschaftlich**
- ✓ **Dienstleistungsorientiert**



Seite 31

12.11.2009

LUZERN
KANTON
LUZERN

Datenschutzbeauftragter des Kantons Luzern

Video

Wohin geht der Datenschutz?

Seite 32

12.11.2009

LUZERN
KANTON
LUZERN

Datenschutzbeauftragter des Kantons Luzern

LUZERN

Der sichere Umgang
mit Daten!

IT-Sicherheit und
Informationssicherheit

KANTON LUZERN

12.11.2009 Seite 33

Datenschutzbeauftragter des Kantons Luzern

LUZERN

Bekannte Gefahren und Risiken



Höhere Gewalt
Feuer, Blitz, Sturm, Überschwemmung, Stromausfall, Krankheit, ...

Menschliche Bedienung

Gesetzliche Nicht-Erfüllung

Technische Netzwerke

Organisatorische Mängel
Fehlende oder nicht angewendete Weisungen, unzureichende Zutrittskontrollen, falsche Zugriffsrechte, Abgang von Schlüsselpersonen (Know-how-Verlust), Versagen der Prozesse, ...

Vorsätzliche Handlungen
Manipulation, Diebstahl, Missbrauch, Sabotage, Spionage, Hacking, Erpressung, Viren, organisierte Kriminalität, ...

Konsequenzen:

- Unterbruch der Geschäftsprozesse
- Produktions-Ausfall, Auslieferungs-Verzug
- Projekt-Verzögerung
- Verlust von vertraulichen Daten oder Know-how
- Bussen (juristische Konsequenzen)
- Image Schaden
- Wiederherstellungskosten

KANTON LUZERN

12.11.2009 Seite 34

Datenschutzbeauftragter des Kantons Luzern

Gefahren und Risiken



Wireless LAN Attack



Commercial Spyware



USB Memory Stick Attack



Notebook Cracking Attack



KANTON LUZERN

12.11.2009 Seite 35

Datenschutzbeauftragter des Kantons Luzern

Gefahren und Risiken



Password Cracking



Phishing Attack



Social Engineering



Employees



KANTON LUZERN

12.11.2009 Seite 36

Datenschutzbeauftragter des Kantons Luzern

Gefahren und Risiken

LUZERN




Handy-Würmer



Keylogger



E-Mail & VOIP Sniffing



Mobile Device Attack



12.11.2009Seite 37

Datenschutzbeauftragter des Kantons Luzern

Gefahren und Risiken

LUZERN




Messenger Attack



Espionage



Adware/Spyware/Rootkit



Bot-Netze



12.11.2009Seite 38

Datenschutzbeauftragter des Kantons Luzern

Gefahren und Risiken



Cyber Erpressung



Browser Hijacking



Fiber Tapping

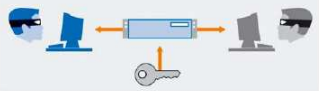


12.11.2009Seite 39

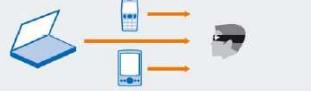
Datenschutzbeauftragter des Kantons Luzern


Zunahme von Datenverlust und -diebstahl

6. Diebstahl von Schlüsseln und Passwörtern

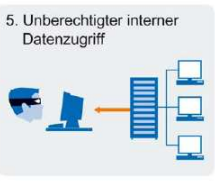


1. Verlust oder Diebstahl mobiler Endgeräte







5. Unberechtigter interner Datenzugriff




2. Ungeschütztes Outsourcing



4. Datendiebstahl von Wechselmedien



3. Abhören von E-Mails



12.11.2009Seite 40

Datenschutzbeauftragter des Kantons Luzern

Menschliche Fehlhandlungen

Innert **6 Monaten** verloren gegangene mobile Geräte in London:

2001	2004	2006
– 62'000 Handys (3 pro Taxi)	– 63'135 Handys	– 54'872 Handys
– 2'900 Notebooks	– 4'973 Notebooks	– 3'179 Notebooks
– 1'300 PDAs	– 5'838 PDAs	– 4'718 PDAs
		– 923 Memory Sticks

Quellen:
http://www.theregister.co.uk/2001/08/31/62_000_mobiles_lost/
http://www.theregister.co.uk/2005/01/25/taxi_survey/

KANTON LUZERN
12.11.2009
Seite 41

Datenschutzbeauftragter des Kantons Luzern

Sicherheitsvorfälle – Realität

Dieb klaute Bundesrätin Tasche
BLICK fand ihre Unterlagen ▶ 13

LEUTHARDS GEKLAUTE TASCHE
Bundesrats-Laptop weg!
▶ SEITEN 2/3

War die Festplatte verschlüsselt?

KANTON LUZERN
12.11.2009
Seite 42

Datenschutzbeauftragter des Kantons Luzern

Sicherheitsvorfälle

Festplattendiebstahl bei US-Regierung: 26,5 Millionen persönliche Data-Records verschwunden

Offizier verliert USB Memory Stick mit Details über Afghanistan Einsatz

Time Warner verliert personenbezogene Daten von 600.000 Angestellten

Automobilzulieferer Valeo werden durch Mitarbeiterin Vorserien-Konstruktionspläne entwendet

Ausrangierte Festplatte der Polizei Brandenburg mit internen Alarmplänen und geheimen Namenslisten im Internet ersteigert

KANTON LUZERN
12.11.2009
Seite 43

Datenschutzbeauftragter des Kantons Luzern

Sicherheitsvorfälle

Laptop mit persönlichen Daten von fast 200'00 Angestellten gestohlen: Diesmal war Hewlett-Packard (HP) an der Reihe

Freitag, 10. November 2006

Datenschutz

Pati

Handelsblätt, Montag, 25. September 2006, 16:55 Uhr

Vier Verz Strafanzeige eingereicht Krankenkassen Daten zu

VOM PETER

Der Vice Luzerner bei rung CSS + traalichen unggangene denfalls vie jetzt eine S größte Sc rung einget Genäss: chel ist 4 Amtesanbu gangen. Sie die Untru insbesondere Vertrauens ausgef. sechs Gene Mauerstein

«Nicht in Der Prozess laut der Zeit hätten nicht

KANTON LUZERN

Einige Mitarbeiter von Fidelity Investments benutzen diesen Laptop ausser Haus. Er enthielt die Daten von 196'000 ehemaligen und gegenwärtigen HP-Angestellten, Daten wie Namen, Adressen, Social Security-Nummern sowie weitere Informationen. Also alles, damit man sich in den USA eine neue Identität zulegen kann. Dies bringt nun das Total der letzten 13 Monate auf mehr als 53 Millionen personenbezogener Datensätze, welche in Dutzenden von Vorfällen abhanden gekommen sind.

USB-Dumper äußerst gefährlich

Hacker-Tool klaut Daten von USB-Sticks

Ein kleines Programm kopiert heimlich alle Daten eines USB-Sticks auf den PC. Dabei werden sogar gelöschte Dateien wieder sichtbar gemacht.

hiz DÜSSELDORF. Die Sicherheitsfirma Centennial Software warnt vor einem Hacking-Tool namens **USB-Dumper**. Dieser Schädling lädt völlig unbemerkt Daten von USB-Sticks, sobald diese an den einen Computer mit dem installierten Tool angeschlossen werden. Da in dem Programm ein so genanntes Recovery-Tool enthalten ist, werden sogar bereits gelöschte Daten entwendet.

„USB-Dumper ist durch den neuen Ansatz ein einzigartiges und äußerst gefährliches Programm“, warnt Matt Fisher, Vice President von Centennial Software. „Vorher wurden mobile Speichermedien benutzt, um Daten von einem PC herunter zu laden. USB-Dumper hingegen ist auf dem PC installiert und kopiert Daten von angeschlossenen USB-Sticks. Wer also Firmeninformationen auf USB-Speichermedien mitführt und sie auf einem fremden Computer nutzen möchte, sollte seine Daten auf dem Stick unbedingt vorher verschlüsseln.“

KANTON LUZERN
12.11.2009
Seite 44

Datenschutzbeauftragter des Kantons Luzern

Sicherheitsvorfälle

Millionen DSL -Router sind akut gefährdet 08.04.2009 | 08:08 Uhr

2008: Phisher überfallen Facebook-Anwender 30.04.2009 | 08:38 Uhr

Facebook-User sind das Opfer einer breit angelegten Phishing-Attacke

Im in a Beri Gigantisches Botnetz aufgeflon 23.04.2009 | 11:31 Uhr

(cw) Das neu entdeckte Riesen-Botnetz soll über 1,9 Millionen Zombie-Rechner verfügen und damit eines der grössten aktiven kriminellen Netze der Welt sein.

(cw)



Ein Grossteil der gekaperten Zombie-Rechner gehört Regierungsbehörden, die rund um den Erdball verstreut sind. Das behauptet Sicherheitsexperte Finjan. Nachforschungen hätten ergeben, dass das Botnetz seit Februar 2009 von einer Gruppe aus der Ukraine betrieben wird. Theoretisch könnten die Kriminellen mit den ferngesteuerten Rechnern alles anstellen, heisst es. Botnetze werden vor allem zum Versenden von Spam verwendet.

nicht unter falscher Identität in Facebook tummeln wollen. Vielmehr ist es ihr Ziel, durch die Facebook-Angaben in andere Systeme einzubrechen. Dabei machen sich die Phisher die Gewohnheit vieler Anwender zu Nutze, jeweils die selben User-ID und Passwörter für mehrere Dienste zu verwenden.

an Sich...

rizon
igen
ISS

12.11.2009 Seite 45

Datenschutzbeauftragter des Kantons Luzern

Sicherheitsvorfälle



So präsentierte sich Peter Jauchs Haus am Dienstag. «Das Schlimmste ist der Verlust des Büro's. Alle Kundendaten sind weg.»

„Das Schlimmste ist der Verlust des Büro's. Alle Kundendaten sind weg!“ Aug 2005

12.11.2009 Seite 46

LUZERN

Datenschutzbeauftragter des Kantons Luzern

Social Engineering


Unter Social Engineering verstehen wir das Planen und Durchführen von Angriffen auf Informationen und Systeme unter Ausnutzung der **«Schwachstelle Mensch»**.

Der Mensch ist generell hilfsbereit!


Vorgehen:

1. Infobeschaffung
2. Vertrauensaufbau
3. Gezielte Manipulation
4. Diebstahl der Informationen
5. Person zu einer Aktion bewegen

«Guten Tag, Herr Müller, hier ist Frau Meier von der IT. Wir haben gerade ein grosses Systemproblem und brauchen unbedingt Ihre Hilfe. Wie lautet Ihr Passwort?»




«Entschuldigen Sie, ich habe den Badge vergessen»



Eine typische Situation: Ein Social Engineer nutzt die Gruppenschleuse. Er hängt sich an einen ahnungslosen hilfsbereiten Mitarbeitenden (Piggy Backing).

«Habe meinen Koffer liegen gelassen und den Schlüssel im Auto.»



Eine typische Situation: Der Wirtschaftsspion gibt sich als «Chef» aus und gelangt so einfach in die für ihn fremde Räumlichkeit.

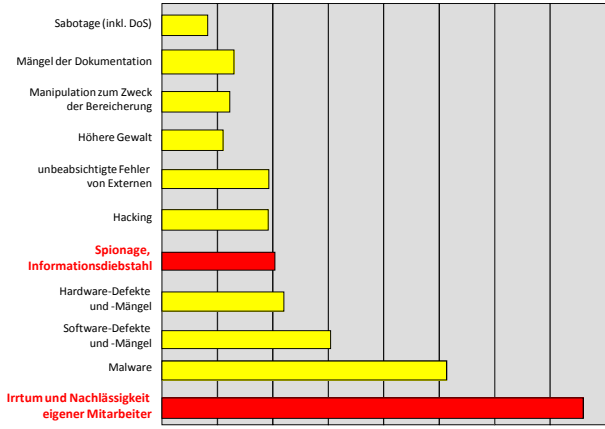
12.11.2009

Seite 47

LUZERN

Datenschutzbeauftragter des Kantons Luzern

Sicherheits-Statistik



Sicherheitsbedrohung	Häufigkeit (geschätzt)
Sabotage (inkl. DoS)	10%
Mängel der Dokumentation	15%
Manipulation zum Zweck der Bereicherung	12%
Höhere Gewalt	10%
unbeabsichtigte Fehler von Externen	18%
Hacking	15%
Spionage, Informationsdiebstahl	18%
Hardware-Defekte und -Mängel	20%
Software-Defekte und -Mängel	25%
Malware	30%
Irrtum und Nachlässigkeit eigener Mitarbeiter	45%

Quelle: KES 2006

12.11.2009

Seite 48

Datenschutzbeauftragter des Kantons Luzern

Informationen sind überall

Information

Mitarbeitende

Multifunktions-
gerät

Fax

PC

Dokumente

Datenbanken

Natel

Telefon

Server

PDA

Notebooks

KANTON LUZERN

12.11.2009 Seite 49

Datenschutzbeauftragter des Kantons Luzern

Ihre Werte und Ihr Know-how gilt es zu schützen!

Informationssicherheit

- Gesamtheitlicher Schutz der Information, die in einem Unternehmen vorhanden ist, unabhängig von deren Form.
- Nicht begrenzt auf Personen
- Durch Massnahmen
- Informations- und Datenschutzgesetze, die Anforderungen an den Datenschutz erfüllen sind.

Datenschutz

- DSGVO Art.1: „Dieses Gesetz bezieht sich auf die Verarbeitung von personenbezogenen Daten, über die eine Person identifiziert werden kann.“
- Gesetzliche Anforderungen an die Verarbeitung von Daten, die erfüllt sind.

IT-Sicherheit

- Schutz der technischen Mittel zur Bearbeitung von Informationen/Daten
- Schutz der Informatikmittel leitet sich ab von Sicherheitsanforderungen:
- der damit bearbeiteten Information (Vertraulichkeit, Datenschutz, Integrität)
- Der abgebildeten Geschäftsprozesse (Verfügbarkeit)

Vertraulichkeit
Verfügbarkeit
Integrität

KANTON LUZERN

12.11.2009 Seite 50

Datenschutzbeauftragter des Kantons Luzern

Was ist IT-Sicherheit?

Bedrohung

↓

Schwachstelle


↓

Gefahr


↓

Risiko


Vorsätzliche Handlungen




Höhere Gewalt
• Technisches Versagen



Organisatorische Mängel
• Menschliche Fehlhandlungen



Schwachstellen



Schutzmassnahmen

R = Wahrscheinlichkeit (Häufigkeit) * Ausmass des Schadenereignisses

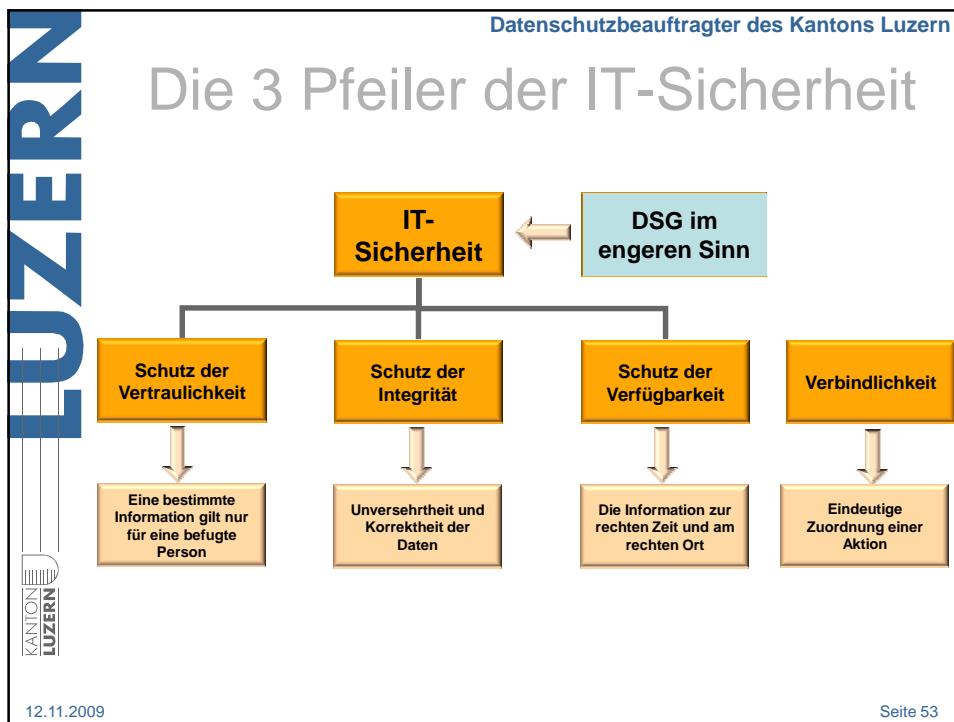
12.11.2009Seite 51

Datenschutzbeauftragter des Kantons Luzern

Wer sind die Täter?

- Geheimdienste (Echelon, Onyx, ...)
- Industriespionage
- Hacker (Geltungsbedürfnis)
- Cracker (Finanzelle Interessen)
- Softwareentwickler (Back Doors)
- Fremdpersonal
- Administratoren
- Mitarbeiter

12.11.2009Seite 52



Datenschutzbeauftragter des Kantons Luzern

Zweck der IT-Sicherheit

Die IT-Sicherheit (Datensicherheit) bezweckt den Schutz von Daten
Insbesondere gegen:

- a) zufällige Bekanntgabe, Vernichtung oder Verlust;
- b) technische Fehler;
- c) unbefugte Kenntnisnahme;
- d) unbefugte Bearbeitung;
- e) Fälschung, Entwendung oder widerrechtliche Verwendung.

KANTON LUZERN


12.11.2009 Seite 54

Datenschutzbeauftragter des Kantons Luzern

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)

Seite 55




12.11.2009

Datenschutzbeauftragter des Kantons Luzern

Integrität

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

Seite 56





12.11.2009

Datenschutzbeauftragter des Kantons Luzern

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)

Seite 57





Datenschutzbeauftragter des Kantons Luzern

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)

Seite 58



Datenschutzbeauftragter des Kantons Luzern

Grundziele

- Verfügbarkeit
- Vertraulichkeit
- Integrität
- Verbindlichkeit

Zeitpunkt der Entdeckung eines Grundzielverlustes

Verfügbarkeit

Integrität

Vertraulichkeit,
Verbindlichkeit

frühzeitig

bald

Sehr spät oder gar nie

12.11.2009
Seite 59

Datenschutzbeauftragter des Kantons Luzern

Die 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

12.11.2009
Seite 60

Datenschutzbeauftragter des Kantons Luzern

Wie sieht es bei Ihnen aus?



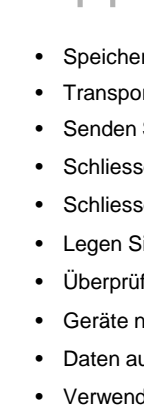
- Sensitive Informationen werden ungeschützt verschickt oder auf externen Speichermedien abgelegt
- Notebooks, PDAs, Smartphones, USB-Sticks etc. gehen verloren
- Zutritt zu Gebäuden ist kaum gesichert und fremde Personen können sich unbehelligt bewegen
- Mitarbeitende sind hilfsbereit und geben bereitwillig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

12.11.2009

Seite 61

Datenschutzbeauftragter des Kantons Luzern

Tipps vom Sicherheits-Experten



- Speichern Sie vertrauliche Daten auf mobilen Geräten immer verschlüsselt.
- Transportieren Sie vertrauliche Daten nur geschützt.
- Senden Sie vertrauliche eMails nur verschlüsselt.
- Schliessen Sie keine USB-Sticks mit unbekannter Herkunft an Ihren Computer an.
- Schliessen Sie Ihren USB-Stick nicht an einem fremden Notebook/PC an.
- Legen Sie keine CD ein, von der Sie nicht wissen, woher sie stammt.
- Überprüfen Sie USB-Sticks und CDs nach Viren, bevor Sie sie verwenden.
- Geräte nicht automatisch starten lassen (Windows Autorun Funktion).
- Daten auf sichere Art löschen; braucht zusätzliche Software.
- Verwenden Sie einen Display-Einsicht-Schutz (Privacy).
- Sichern Sie Ihre Daten regelmässig und lagern Sie eine Kopie (verschlüsselt) physisch an einem anderen Ort (z.B. Bank-Safe).

12.11.2009

Seite 62

Datenschutzbeauftragter des Kantons Luzern

Tipps vom Sicherheits-Experten

- Behandeln Sie geschäftliche Themen in der Öffentlichkeit vertraulich.
- Lassen Sie andere nicht mithören.
- Lassen Sie sich nicht aushorchen.
- Lassen Sie Notebook, Handy oder PDA nie unbeaufsichtigt, wenn, dann aktivieren Sie den Screen-Lock (Bildschirmschoner).
- Vermeiden Sie Ihr mobiles Gerät auf irgendeine Weise mit Ihrer Firma in Verbindung zu bringen (Logos, Kleber etc.).
- Aktivieren Sie Bluetooth nur dann, wenn Sie Bluetooth wirklich benötigen (z.B. Headset im Auto). Oder deaktivieren Sie die Funktion „Sichtbarkeit“.

Seite 63


Datenschutzbeauftragter des Kantons Luzern

«Passwort»

- Passwort: Schutz vor dem Zugriff Unberechtigter
- Ein gutes – oder «starkes» Passwort
 - mind. 8 oder besser aus 10 Zeichen
 - enthält Zahlen, Buchstaben und Sonderzeichen kombiniert
 - hat Gross- und Kleinbuchstaben
 - können Sie sich gut merken, andere aber nicht erraten, zum Beispiel Sonn**EN00schein, fRan?ziska57
 - besteht nicht nur aus Wörtern – auch nicht in einer Fremdsprache – oder Namen
- Anleitung für sichere Passwörter
 - Bilden Sie einen Satz: «Im August schien die Sonne nur 1x!» ergibt das starke Passwort: <IASdSn1x!>

Passwörter sind wie Zahnbürsten

- Regelmässig anwenden
- Häufig wechseln
- Nicht in Gruppen verwenden



Seite 64

Luzern

Datenschutzbeauftragter des Kantons Luzern

Umgang «Passwort»

- Handhabung des Passwortes
 - Halten Sie das Passwort geheim
 - Ändern Sie das Passwort spätestens nach vier Monaten, oder wenn Sie vom System aufgefordert werden.
 - Verwenden Sie für verschiedene Anwendungen verschiedene Passwörter
 - Keine Weitergabe an Mitarbeiter oder Dritte (auch bei Stellvertretung!)
 - Verwenden Sie privat und geschäftlich andere Passwörter
- Wichtige zusätzliche Informationen zum Passwort
 - Hier können Sie überprüfen, wie gut Ihr Passwort ist:
<https://passwortcheck.datenschutz.ch/check.php?lang=de>
 - Weitere Hinweise des Datenschutzbeauftragten des Kantons Zürich zum Passwort:
<http://www.datenschutz.ch/wbt/sicherheit/index1.htm>

12.11.2009

Seite 65

Luzern

Datenschutzbeauftragter des Kantons Luzern

«Der sichere Umgang mit E-Mail»

- Eile mit Weile!
 - Ein Klick und Ihr Mail ist unwiderruflich weg
- Wissen Sie wirklich, wer der Adressat ist?
- Versand innerhalb des verwaltungseigenen Netzes
 - Endet die Adresse auf «xy@lu.ch», erfolgt die Zustellung über das eigene Netz
- Versand via Internet
 - E-Mail geht unverschlüsselt im Klartext wie eine Postkarte über das Internet!
- Erhalt von E-Mails
 - Mails von zweifelhafter Herkunft sind ungeöffnet zu löschen
 - Ebenso ungeöffnet zu löschen sind Dateien mit der Endung «.scr», ausführbare Dateien («.exe», «.bat», «.vbs» etc.) und Bilder von zweifelhafter Herkunft
 - Fehlende Gewissheit über Identität des Absenders erfordert telefonisches Nachfragen beim Absender
- Vorgehen bei Ferienabwesenheit
 - Eingehende E-Mails nicht automatisch an eine E-Mail-Adresse ausserhalb des eigenen Netzes weiterleiten
 - Absenderinnen und Absender von E-Mails mit einer automatischen Antwort über Ihre Ferienabwesenheit und Ihre Stellvertretung informieren

12.11.2009

Seite 66

Datenschutzbeauftragter des Kantons Luzern

«Mobile Geräte»


- Mobile Geräte (Laptops/Notebooks, PDA, Mobiltelefone/Smartphones, USB-Sticks etc.)
 - Grundsätzlich dieselben Sicherheitsbestimmungen wie für feste Arbeitsstationen
 - Schutz des Gerätes durch ein starkes Passwort
 - Diverse Möglichkeiten zur drahtlosen Kommunikation (WLAN, Bluetooth, Infrarot, GSM etc.)
 - Nutzung von öffentlichen «Hotspots» ist zu vermeiden oder nur mittels VPN (verschlüsselt)
 - Aktualisierung des Virenschutzes
 - Umgehende Information an IT-Verantwortlichen bei Verlust oder Diebstahl
- Verschlüsselung der Festplatte
- SMS, MMS und E-Mail (vorsichtiger Umgang)
- Vertrauliches gehört nicht an die Öffentlichkeit (Restaurant, Zug etc.)

Seite 67

Datenschutzbeauftragter des Kantons Luzern

Ihr Nutzen

- Geringere Verwundbarkeit
- Keine falsche Sicherheit
- Bewussterer Umgang mit Information
- Gefahren kennen, Restrisiko ist bekannt
- Sorgfaltspflicht erfüllt
- Positive Audits (interne und externe Revision)
- Erhöhtes Kundenvertrauen
- Einhalten aller Gesetze (IKS, Datenschutz, GebüV etc.)
- Wettbewerbsvorteil -> Sicherheit = Vertrauen
- Reduziert das Risiko einer Geschäftsunterbrechung erheblich (hohe Verfügbarkeit)
- Fördert das „Sicherheitsbewusstsein“ der Mitarbeiter (Sicherheitskultur)




Seite 68

Datenschutzbeauftragter des Kantons Luzern

Verantwortung

- Geschäftsfortgang stören / verunmöglichen
- Sorgfaltspflicht des Managements
- Verantwortung kann nicht delegiert werden

**Informationssicherheit
t
ist Chefsache!**

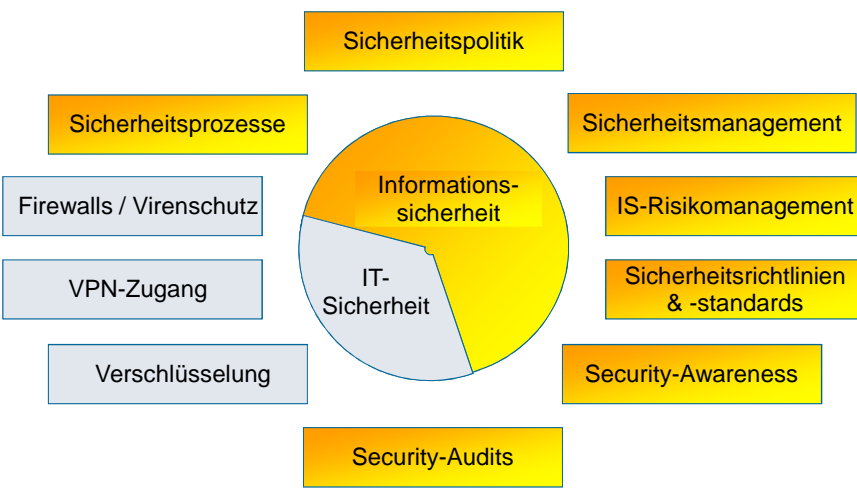


KANTON LUZERN

12.11.2009 Seite 69

Datenschutzbeauftragter des Kantons Luzern

IT-Sicherheit und Informationssicherheit




KANTON LUZERN

12.11.2009 Seite 70

Datenschutzbeauftragter des Kantons Luzern

Integrale Sicherheit

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



The diagram shows 'Integrale Sicherheit' at the center, surrounded by ten circles representing different security aspects: Logische Sicherheit, Physische Sicherheit, Datenschutz, Personenschutz, Arbeits-sicherheit, Qualitäts-sicherung, Umweltschutz, Versicherungs-schutz, Notfall-planung, and Informations-schutz.


KANTON LUZERN

12.11.2009 Seite 71

Datenschutzbeauftragter des Kantons Luzern

Zutritts-, Zugangs-, Zugriffskontrolle

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



The diagram consists of three nested rectangles: an outer green rectangle labeled 'Zutrittskontrolle', a middle orange rectangle labeled 'Zugangskontrolle', and an inner red rectangle labeled 'Zugriffskontrolle'.

KANTON LUZERN

12.11.2009 Seite 72

Datenschutzbeauftragter des Kantons Luzern

Zusammenspiel Mensch – Technologie, Organisation und Management

Mensch

Technologie

Organisation und Management

KANTON LUZERN

12.11.2009

Seite 73

Datenschutzbeauftragter des Kantons Luzern

Information Security Management Prozess

Planung (plan)
Aufbau des ISMS

Implementierung (do)
Implementierung und Betrieb des ISMS

Überprüfung (check)
Überwachen und Review des ISMS

Verbesserung (act)
Entwicklung, Unterhalt und Verbesserungszyklus
Unterhalt und Verbesserung des ISMS

Interessierte Parteien
Anforderungen und Erwartung an die Informationssicherheit

Interessierte Parteien
Aktive Informationssicherheit

KANTON LUZERN

12.11.2009

Seite 74

Datenschutzbeauftragter des Kantons Luzern

Umsetzung der Informationssicherheits-Strategie

LUZERN

KANTON LUZERN

12.11.2009 Seite 75

Datenschutzbeauftragter des Kantons Luzern

Risiko

- Ein Risiko ist die *kalkulierte Prognose* eines möglichen *Schadens bzw. Verlustes im negativen Fall (Gefahr)* oder eines möglichen *Nutzens bzw. Gewinns im positiven Fall (Chance)*. Was als Schaden oder Nutzen aufgefasst wird, hängt von **Wertvorstellungen** ab.
- „Management“ des Risikos durch Vermeidung, Übertragung, Begrenzung, Akzeptanz, Ignoranz
- Abhängig von Risikotyp und Risikokultur

R = Wahrscheinlichkeit (Häufigkeit) * Ausmass des Schadenereignisses

KANTON LUZERN

12.11.2009 Seite 76

Datenschutzbeauftragter des Kantons Luzern

Operative Risiken

```

graph TD
    OR[Operative Risiken] --> TS[Technologie System]
    OR --> P[Personal]
    OR --> OP[Organisation Prozesse]
    OR --> E[Extern]

```

Technologie System	Personal	Organisation Prozesse	Extern
<ul style="list-style-type: none"> • Anwendungs-Risiken • Prozessbezogene Risiken IT • Infrastrukturelle Risiken • Datenrisiken • Modellrisiken • etc. 	<ul style="list-style-type: none"> • Verlust/Krankheit • Unfallrisiken • Kulturrisiken • Fluktuationsrisiken • Streikrisiken • Nicht autorisierte Handlungen • Kriminelle Handlungen • etc. 	<ul style="list-style-type: none"> • Managementfehler • Fehlerhafte Aufbau-Org. • Fehlerhafte Ablauf-Org. • Compliance Risiken • etc. 	<ul style="list-style-type: none"> • Brand, Explosion • Naturereignisse • Politische Risiken • Risiken infolge rechtlicher Entwicklungen • Risiken infolge gesellschaftlicher Veränderungen • Regulatorische Risiken • Risiken durch externe Dienstleister • Drittpartei-Risiken • etc.

KANTON LUZERN

12.11.2009 Seite 77

Datenschutzbeauftragter des Kantons Luzern

Risiken melden!

- Beobachten Sie Ihr Umfeld sorgfältig.
- Melden Sie entdeckte Risiken Ihrem Vorgesetzten.
- Sie sind unser bester Sicherheitssensor!

Besten Dank!

KANTON LUZERN

12.11.2009 Seite 78

Datenschutzbeauftragter des Kantons Luzern

Ausblick / Trends

- Weiter wachsende Mobilität, "Intelligente" Geräte, Spontane Netzwerke (GPS, RFID, DNA, Genforschung, Nanotechnik etc.), mehr Funktionalität in den Applikationen
- Virtualisierung & Miniaturisierung der Hardware, Cloud-Computing
- Datensicherung und Archivierung (Datenklassifikation, Data Rights Management)
- Kommunikations-Tools (Skype, Teamviewer etc.) -> Umgehen die Firewalls
- Erhöhte Abhängigkeit von komplexer Technologie
- Erhöhte rechtliche und regulatorische Anforderungen
- Die Trojaner werden raffinierter und tarnen sich als Microsoft oder Java Update
- Open-Source Angebote werden missbraucht (Abofallen)
- Datendiebstahl und Identitäts-Diebstahl werden zunehmen.
- Kosten- / Nutzen-Betrachtungen / Sourcing / Fusionen / Übernahmen
(CH-Unternehmen wird durch ein Unternehmen in den USA oder China übernommen)

Seite 79

Datenschutzbeauftragter des Kantons Luzern

Spezial-Angebot

Sie erhalten heute das „IT-Sicherheitshandbuch“ für nur

CHF 80.- (statt 98.-)



IT-Sicherheitshandbuch für die Praxis ISBN: 3-9521208-3-9

Seite 80

Datenschutzbeauftragter des Kantons Luzern



LUZERN

KANTON
LUZERN

12.11.2009

Seite 81