luzerner kantonsspital
LUZERN SURSEE WOLHUSEN

Security@Risk

Information Security in Health Conference
23. Juni 2015, Rotkreuz

Lucerne University of
Applied Sciences and Arts
HOCHSCHULE
LUZERN

Dr. med. Stefan Hunziker

Chief Information Officer

eMBA UZH, Dipl. Wirtschaftsinformatiker FH

Agenda

- Einleitung
- Bedrohungen und Rahmenbedingungen
- Healthcare Challenges
- Faktor Mensch
- Konklusion

Kennzahlen LUKS

Ambulante Patientenkontakte	532 676
Stationäre Patientinnen/Patienten	40 611
Geburten	3163
Mitarbeitende	6315
Personen in Ausbildung	1739
Betten	860
Jahresumsatz	847 Mio.

Quelle: Jahresbericht LUKS 2014

Kennzahlen IT

Informatik LUKS (exkl. Montana)				
	2012	2013	2014	Veränderung 2013/2014
Desktop, Laptop	3'415	3'556	3'697	+ 4.0 %
Mobile Geräte (Smartphone etc.)	60	480	644	+ 34.2 %
Drucker	1'571	1'653	1'651	- 0.1 %
Server	428	440	564	+ 28.2 %
WLAN Access Point	634	760	1'025	+ 34.9 %
Software Pakete	1'334	1'549	1'631	+ 5.3 %
Personal (FTE)	49.0	53.6	58.4	+ 9.0 %

MedFolio Kennzahlen 2014	
Beschreibung	**Anzahl**
Benutzer gesamt	5088
Benutzer Ärzte	1186
Concurrent Users	Max. 800
Briefvorlagen (verwendet)	950
Briefe (angelegt pro Jahr)	400'000
Formulare (angelegt pro Jahr)	1'000'000


Bedrohungen

PC WELT

snowden-Dokumente

NSA kann SIM-Karten-Verschlüsselung knacken

Freitag den 20.02.2015 um 10:18 Uhr

von Panagiotis Kolokythas

NSA und GCHQ haben offenbar die Verschlüsselungscode von SIM-Karten entwendet Vergrößern

Die NSA und der GCHQ sind in der Lage, die Verschlüsselung von vielen SIM-Karten zu knacken. Das geht aus Snowden-Dokumenten hervor.

Die Enthüllungsseite The Intercept berichtet, dass der US-Geheimdienst NSA (National Security Agency) und der britische Geheimdienst GCHQ (Government Communications Headquarters) in der Lage sind, die von vielen SIM-Karten genutzte Verschlüsselung zu knacken. Das gehe aus Dokumenten des NSA-Whistleblowers Edward Snowden hervor, die nun ausgewertet worden seien.

Die Verschlüsselungscodes seien demnach vom niederländischen SIM-Karten-Hersteller Gemalto gestohlen worden. Gemalto gehört zu den wichtigsten SIM-Karten-Herstellern weltweit und stellt um die zwei Milliarden SIM-Karten pro Jahr her.

Diebstahl durch Regierungsstellen ?

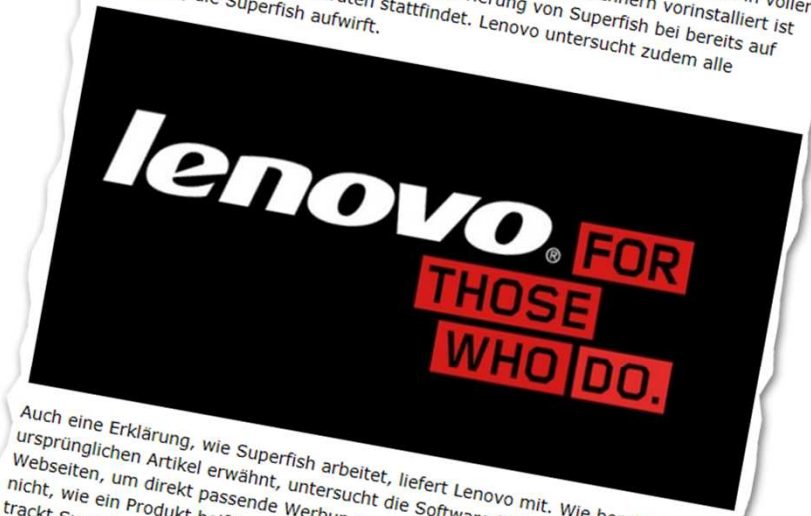
http://www.pcwelt.de/news/NSA-kann-SIM-Karten-Verschluesselung-knacken-Snowden-Dokumente-9572546.html, 23.02 2015

Man-in-the-Middle Angriffe

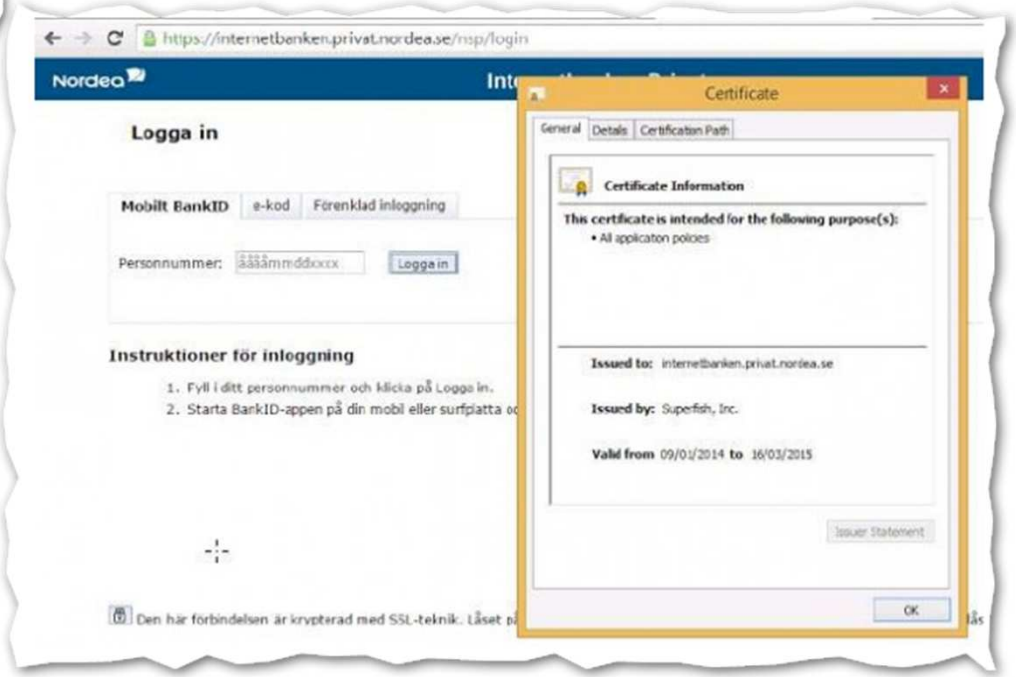
Lenovo Statement zur vorinstallierten Superfish-Adware

19. Februar 2015 Kategorie: Backup & Security, Hardware, Internet, geschrieben von: Sascha Ostermaier

Heute Morgen berichteten wir über Superfish, einer Adware, die bei manchen Lenovo-Laptops vorinstalliert ist und dank eigenem Zertifikat auch HTTPS-Verbindungen "abhören" kann. Den Artikel dazu findet Ihr hier. Nun erreichte uns ein Statement von Lenovo, welches wir Euch natürlich nicht vorenthalten wollen. Viel Neues geht aus diesem aber auch nicht hervor. Im Statement (unten in voller Länge) heißt es, dass seit Anfang 2015 nicht mehr auf Rechnern vorinstalliert ist und seit diesem Zeitpunkt auch keine Aktivierung von Superfish bei bereits auf dem Markt befindlichen Geräten stattfindet. Lenovo untersucht zudem alle Bedenken, die Superfish aufwirft.



Auch eine Erklärung, wie Superfish arbeitet, liefert Lenovo mit. Wie bereits im ursprünglichen Artikel erwähnt, untersucht die Software Bilder auf besuchten Webseiten, um direkt passende Werbung anzuzeigen. Dabei weiß Superfish aber nicht, wie ein Produkt heißt, oder wie man es textbasiert suchen würde. Auch trackt Superfish den Nutzer nicht, lernt also nicht vom Surfverhalten des Nutzers und speichert keinerlei Informationen. Es werden grundsätzlich nur die Bilder analysiert, um ähnliche Bilder (über Werbung) anzuzeigen. Texteingaben werden nicht gespeichert, außerdem ist jede Superfish-Session unabhängig.



http://stadt-bremerhaven.de/lenovo-statement-superfish-adware/, 23.2.2015

Das Reaktorunglück von Tschernobyl

Am 26. April 1986 kam es im Atomkraftwerk von Tschernobyl zum bisher schwersten Unfall in der Geschichte der Kernenergie. Zwei Explosionen zerstörten einen der vier Reaktorblöcke und schleuderten radioaktives Material in die Atmosphäre, das weite Teile Russlands, Weißrusslands und der Ukraine verseucht. Die radioaktive Wolke zieht bis nach Mitteleuropa und

Wenn man Sicherheitsvorschriften verletzt, so wird gewöhnlich dadurch das Leben leichter.

Dietrich Dörner in «Logik des Misslingens»

Auch Jahrzehnte nach dem Unglück ist nicht abschließend geklärt, was in Tschernobyl wirklich geschehen ist. Sicher ist nur, dass viele Faktoren wie die Bauart des Reaktors, fehlende Sicherheitseinrichtungen und die Abschaltung von Sicherheitssystemen zusammenwirkten. Bei der Rekonstruktion des Unglücks und der Suche nach den Ursachen waren die Wissenschaftler auf Beschreibungen der Ereignisse und Schäden angewiesen. So ist bisher noch immer unbekannt, was den ursprünglichen Leistungsabfall ausgelöst hatte. Und es ist in der Fachwelt noch immer umstritten, was letztendlich die beiden Explosionen ausgelöst hat.

http://www.planet-wissen.de/natur_technik/atomkraft/tschernobyl/ 20.06.2015

Die Sicherheitstüren an den Flugzeugcockpits können sich auch zum Boomerang entwickeln. (Foto: Reuters/APA/"Heute.at"-Montage)

Der Entführer der Boeing 767-300 der Ethiopian Airlines am Montag hatte als Copilot leichtes Spiel. Ihm gelang der Coup, weil der Kapitän nach seinem Besuch auf der Toilette schlichtweg nicht mehr zurück ins Cockpit konnte. Der Grund: Seit dem 11. September 2001 und den Flieger-Attacken auf das World Trade Center im New York müssen alle Cockpittüren so umgerüstet sein, dass sie nur noch von innen geöffnet werden können.

Security und Systemfehler

Co-Pilot nutzt die Sicherheit des Schliesssystem zum Aussperren des Flugkapitäns aus und bringt Flugzeug zum Abstürzen.

Untersuchung nach Germanwings-Absturz

Ermittler gehen «Systemfehlern» nach

Nach dem Germanwings-Absturz in den französischen Alpen gehen die französischen Ermittler auch möglichen «Systemfehlern» nach. Insbesondere das Schliesssystem der Cockpit-Türen wird näher untersucht.

31.3.2015, 15:07 Uhr

Ein Mitglied der Rettungscrew wird von einem Helikopter aus der Steilwand hochgezogen in der Nähe von Seyne-les-Alpes gezogen. (Bild: Keystone / AP)

Quelle: NZZ

DDoS Assault on Boston Hospital

Hacktivist Group Suspected of Attacking Children's Hospital

By Marianne Kolbasuk McGee, April 25, 2014.

To date, **distributed-denial-of-service** attacks have been relatively rare in the healthcare sector, especially compared with DDoS assaults in the financial sector. But DDoS attacks on Boston Children's Hospital's **website** have security experts debating whether these attacks could become far more common in healthcare.

See Also: More Threat Vector Challenges

Hacker Gruppen

In a April 25 statement provided to Information Security Media Group, Boston Children's Hospital confirmed a report published by the ***Boston Globe*** that the hospital's public website had been undergoing cyber-attacks for nearly a week, which made some online services, such as patient appointment scheduling, sporadically inaccessible.

"Boston Children's website has been the target of multiple attacks designed to bring down the site by overwhelming its capacity," the statement says. "Boston Children's technical and security professionals are working to resolve the situation as soon as possible. We have also contacted law enforcement authorities, who are investigating the source of the attacks. There is no information to suggest that patient information has been compromised, and patient care has not been interrupted."

The hacktivist group Anonymous is suspected of launching the attacks against the hospital, which threatened the medical center in the weeks leading up to the DDoS assault, according to the *Boston Globe* report. The hacker group is thought to be retaliating against the hospital because of anger over an ongoing child custody case that's drawn national attention.

RELATED CONTENT

- Another Breach Notification Bill Introduced
- Cybercrime Gang: Fraud Estimates Hit $1B
- IoT Security: The Patching Challenge
- Cisco to Launch New Security Platform
- NIST Framework: Is It a Success?

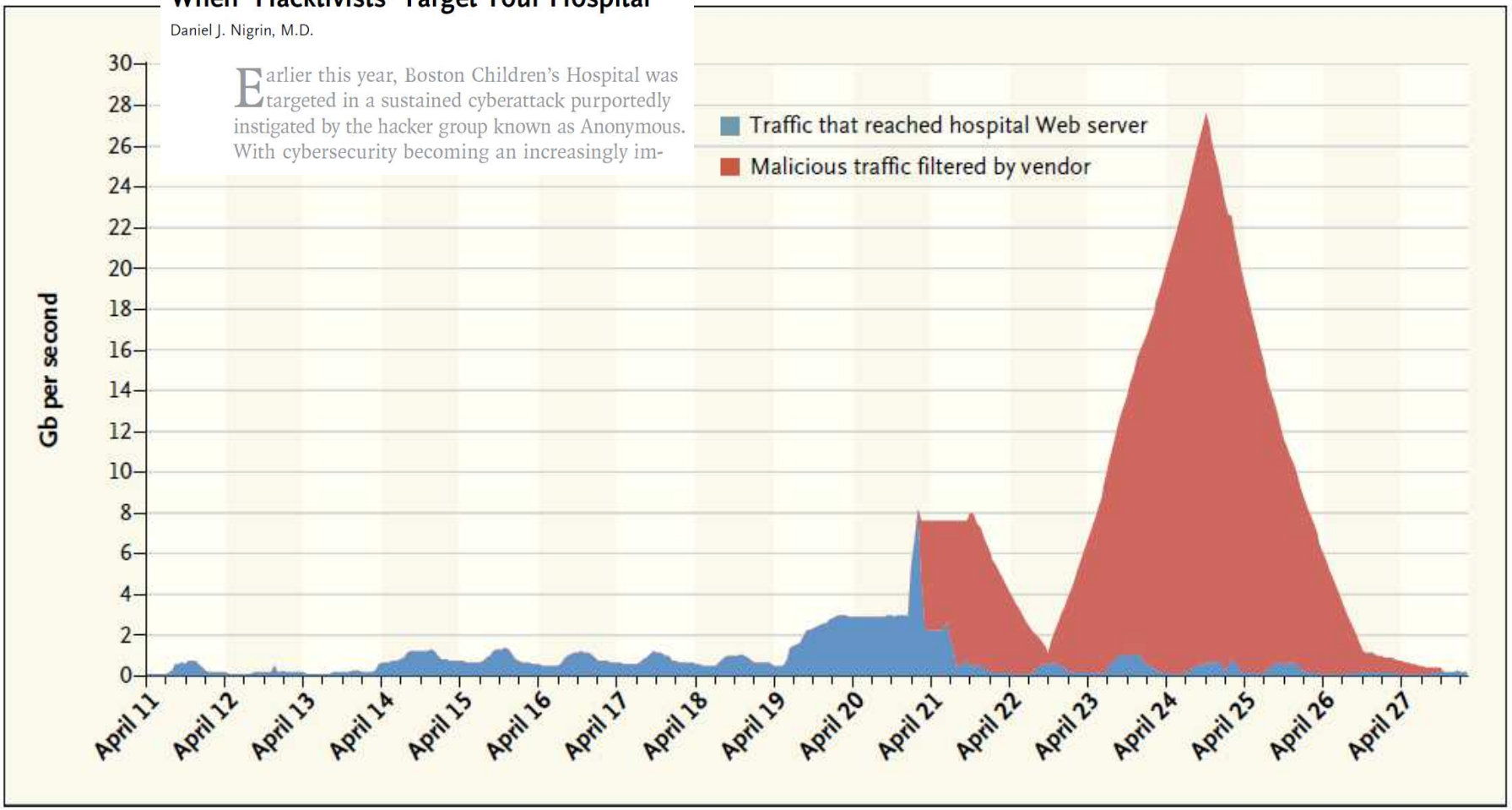
RELATED WHITEPAPERS

- Business Continuity: Leveraging High Availability Clustering
- Information Security Risk and the

When ‘Hacktivists’ Target Your Hospital

Daniel J. Nigrin, M.D.

Earlier this year, Boston Children’s Hospital was targeted in a sustained cyberattack purportedly instigated by the hacker group known as Anonymous. With cybersecurity becoming an increasingly im-

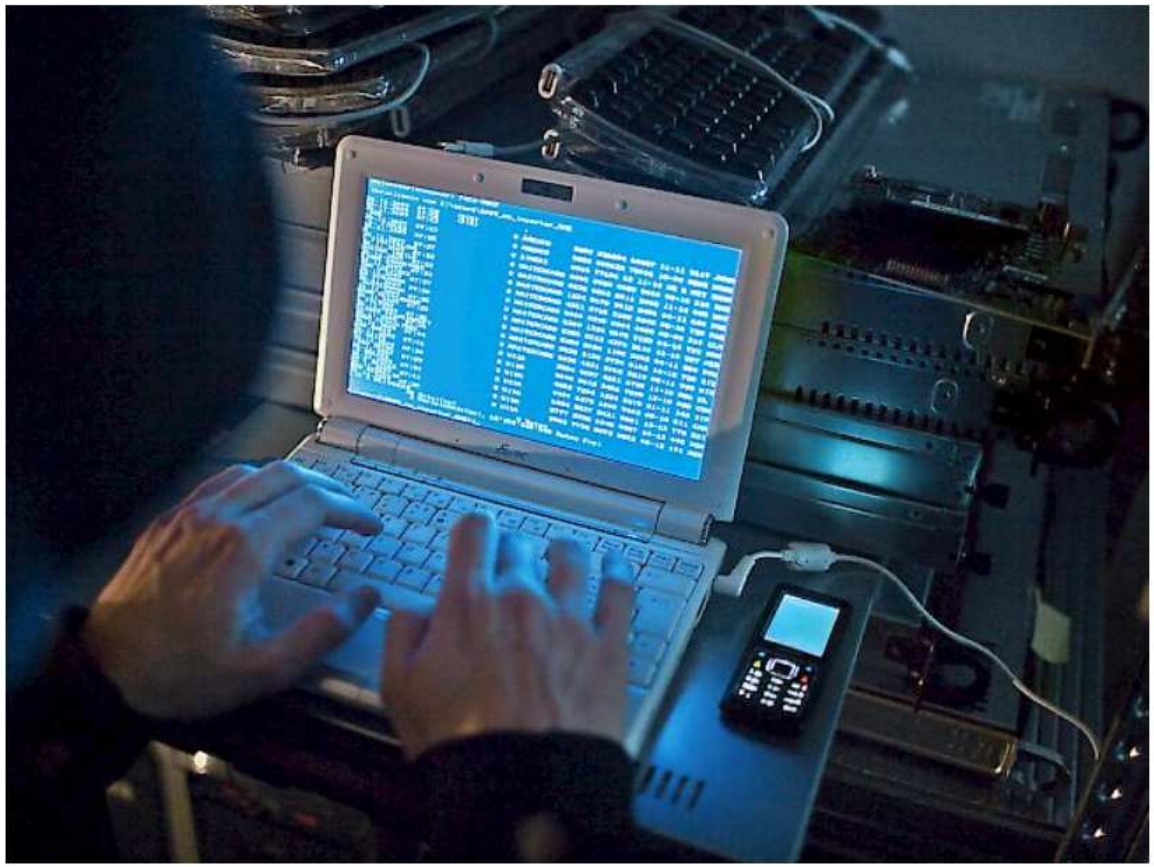


Internet Traffic during DDoS Attack.

The graph shows Internet traffic targeted for the Boston Children’s Hospital external website during the “distributed denial of service” (DDoS) attack. As the attack increased, the hospital worked with a DDoS defense vendor to reroute traffic to the vendor’s filtering center. Traffic that the filter classified as malicious was discarded. The remaining “clean” traffic was forwarded to the hospital. Normal peak traffic is approximately 0.7 gigabits (Gb) per second.

CYBERKRIMINALITÄT | Erpressungen mit Cyberattacken nehmen zu

Cyberangriffe mit Erpressung häufen sich in der Schweiz



1/1 Der Bund warnt vor zunehmenden Cyberattacken, bei denen die Kriminellen versuchen, von ihren Opfern Geld zu erpressen (Symbolbild)
Foto: Keystone

Quelle: SDA

20.05.15

0

In den vergangenen Wochen haben Cyberattacken in der Schweiz zugenommen, um von den Opfern Geld zu erpressen. Der Bund warnt davor, auf die Erpressung einzugehen. Zudem sollen Fälle schnellstmöglich der kantonalen Polizeidienststelle gemeldet werden.

Hackers lock up thousands of Australian computers, demand ransom

September 17, 2014

Comments 25 Read later

Ben Grubb

Technology editor

View more articles from Ben Grubb

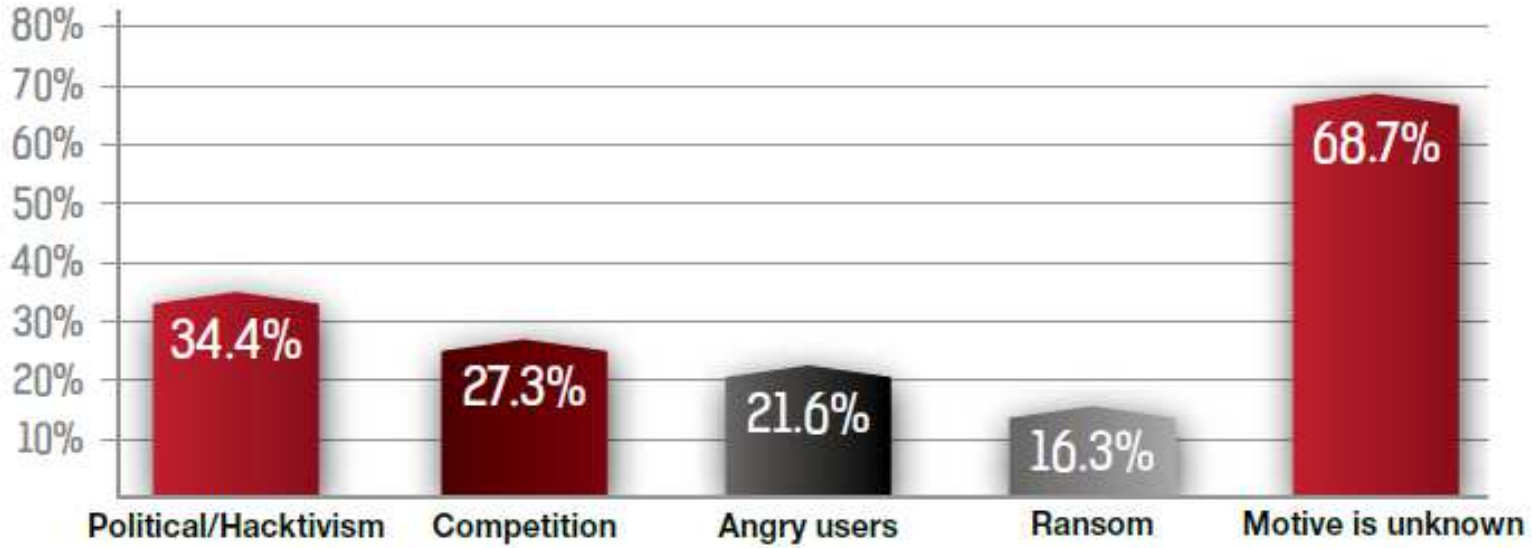
Follow Ben on Twitter Follow Ben on Google+ Email Ben

Tweet Teilen 17 Share Pin it submit

Email article Print

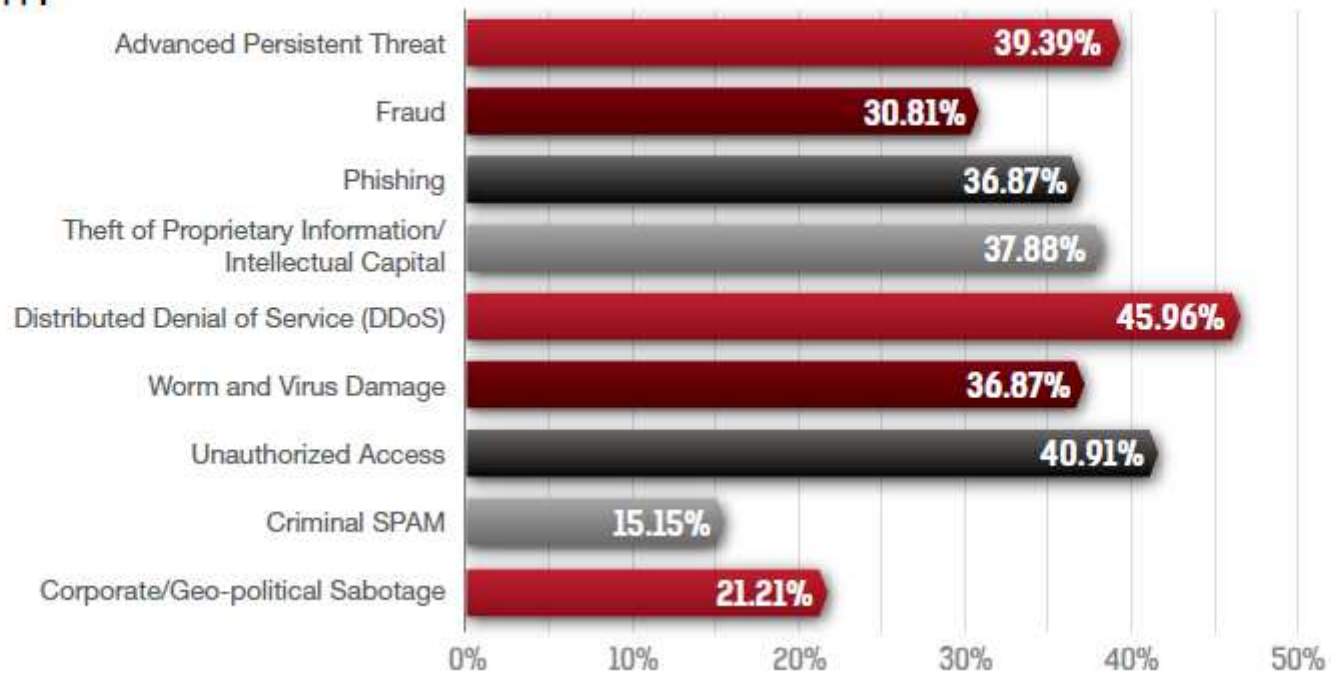
http://www.theage.com.au/it-pro/security-it/hackers-lock-up-thousands-of-australian-computers-demand-ransom-20140917-10hyyh.html, 20.06.2015

Which of the following motives are behind any cyber-attacks your organization experienced?



Quelle: Global Application & Network Security Report 2014-2015, Radware

In your opinion, which of the following cyber-attacks will cause your organization the most harm?



Quelle: Global Application & Network Security Report 2014-2015, Radware

Healthcare Challenges

Healthcare Challenges

	Office IT	Healthcare IT
Anwendungsbereich	Informationsverarbeitung	Diagnose, Analyse, Überwachung usw.
Landschaft	Homogen, standardisiert	Heterogen, vielfältig
Primäres Schutzziel	Vertraulichkeit	Verfügbarkeit
Konsequenz Verletzung Schutzziel	Monetärer Verlust	Bedrohung von Leib und Leben
Verfügbarkeit	Ausfälle möglich	7x24
Fokus der Sicherheit	Sicherheit zentrale Server	Dedizierte Geräte
Lebensdauer	2-3 Jahre	5-10 Jahre
Patchmanagement	Oft	Selten/ Herstellerabhängig
Awareness	Gut	Schlecht
Physische Sicherheit	Abgesicherte Bereiche (Büro)	Teilweise gesicherte Bereiche
Änderungen	Oft	Selten

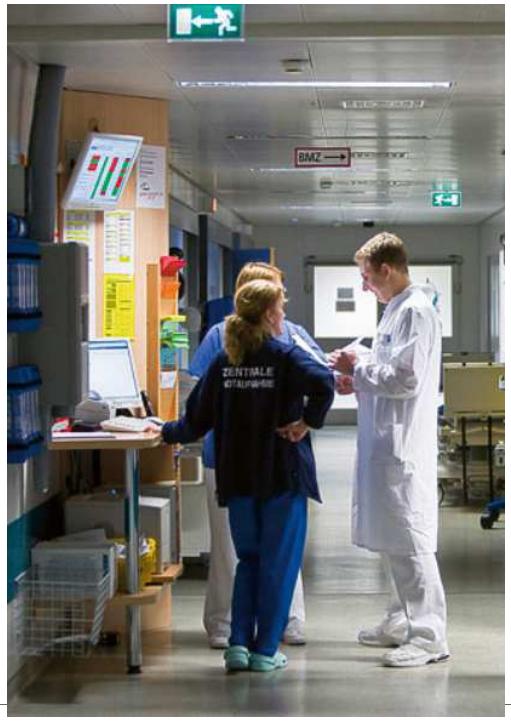
Healthcare Security Landscape

Quelle: Deloitte

Top Security Risks

- Malware, Virus, Spyware, Ransomware,…
- Cybercrime
- Bring your own everything
- Internet of things / medical infrastructure
- The human factor

Öffentliche Zonen



luzerner kantonsspital
LUZERN SURSEE WOLHUSEN

Sicherheitszonen im Krankenhaus

Sicherheits-zone	Beschreibung / Definition
1	**Außenbereich, Areal, Zufahrtswege, Notfallspur, Hubschrauberlandeplatz, Tankstelle** Bereich, zu dem jedermann Zutritt hat, Überwachung nur teilweise möglich
2	**Parkhaus, Parkplatz**
3	**Öffentlicher Bereich inkl. Mieterzone** Bereich ohne direkten Zusammenhang mit der Pflege, wird auch von Dritten benutzt: Cafeteria, Eingangshalle, Kiosk, Blumenladen usw.
4	**Freie Besucherzone, Patientenzimmer** Bereich, in welchem sich die Besucher ohne Anmeldung aufhalten und sich frei bewegen können (während den Besuchszeiten und in Notfällen).
5	**Kontrollierte Besucherzone, allgemeiner Personalbereich** Besucherbereich, in welchem sich die Besucher nach der Anmeldung aufhalten und sich frei bewegen können (z.B. Intensivpflegestation, Säuglingsabteilung). Je nach Krankheitsbild bzw. Zustand des Patienten (z.B. Tuberkulose, SARS, Patienten in kritischem Zustand) gelten besondere Sicherheitsvorschriften. Bereich, in welchem sich das Personal frei bewegen kann.
6	**Kontrollierter Personalbereich** Bereich, zu dem nur bestimmtes Personal Zugang hat (Büro Chefarzt, Personal-wesen, Operationssaal), z.B. nur das Personal der Abteilung (z.B. Diagnose CT & MRI, Schockraum). Patienten werden hier nur in Begleitung zugelassen. Im Normalfall sind diese Räumlichkeiten bei Abwesenheit abgeschlossen.
7	**Nicht vitale Technik (bei Ausfall nicht direkt lebensbedrohliche Auswirkungen)** Technische Räume (Heizung, Lüftung, Klima, Sanitär, Elektro usw.), die nur einer bestimmten Personengruppe zugänglich sind. Im Normalfall sind Räumlichkeiten bei Abwesenheit abgeschlossen.
8	**Vitale Technik (bei Ausfall direkt lebensbedrohliche Auswirkungen)** Vitale technische Räume (z.B. Strom- und Notstromversorgung, Lüftung Operationssaal, Medien, Gase, IT-Räume), die nur einem ausgewählten, techni-schen Personenkreis zugänglich sind. Alle Zutritte werden kontrolliert und regis-triert. Fremdpersonen sind zwingend zu begleiten. Räumlichkeiten müssen zwin-gend abgeschlossen sein.
9	**Sensitiver Personalbereich** Sensitive Personalbereiche (Operationssaal, Apotheke, Lager für radioaktive Materialien, Archive usw.), die nur einem reduzierten und ausgewählten Personenkreis zugänglich sind. Alle Zutritte werden kontrolliert und registriert. Besucher und Fremdpersonen haben keinen Zutritt zu diesen Bereichen. Räumlichkeiten müssen zwingend abgeschlossen sein.

Quelle: Bedrohung im Gesundheitswesen – Effiziente Erkennung und Vorbeugung, Siemens

Risk Management: Wert der Daten?

- **Security and Healthcare?**
- **Electronic health records have many times the black market value of a credit card.**
  - **Valid banking account information (no access on account): 0,5 – 1 USD**
  - **Credit card number: 1,5 USD**
  - **Valid banking account information (access on account): 50 USD**
  - **Single Healthcare record: 50 USD**

(Quelle: Talanx Versicherung)

A report by the Ponemon Institute calculates the average out-of-pocket loss per victim of medical identity theft at **$18,660.**

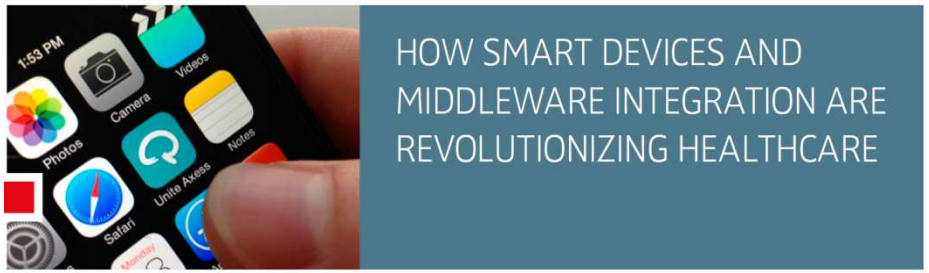
Quelle: Bitglass

Your medical record is worth more to hackers than your credit card

NEW YORK/BOSTON | BY CAROLINE HUMER AND JIM FINKLE

A man types on a computer keyboard in this illustration picture taken in Warsaw February 28, 2013.
REUTERS/KACPER PEMPEL

Chancen / Risiken



Quelle: Ascom

Health-Apps: Behörde warnt vor Fehldiagnosen

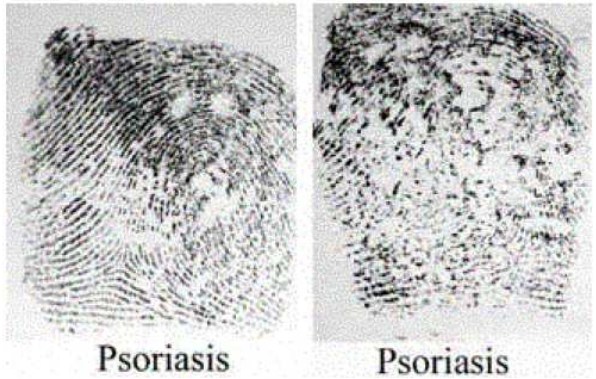
Quelle: Heise

- Neue Technologien/ Gadets revolutionieren den Gesundheitssektor
- Aber: Jeder kann Apps programmieren → Aussagekraft von Medizinapps?
- Fazit: Technologien/ Gadets können helfen/ verbesserte Diagnosen ermöglichen, einen Arztbesuch ersetzen sie aber (noch) nicht

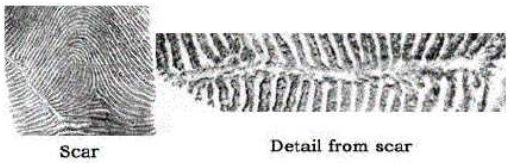
Probleme mit der Sicherheit

Probleme mit Fingerabdrucksystemen

2% aller Menschen haben keinen Fingerabdruck



Krankheiten



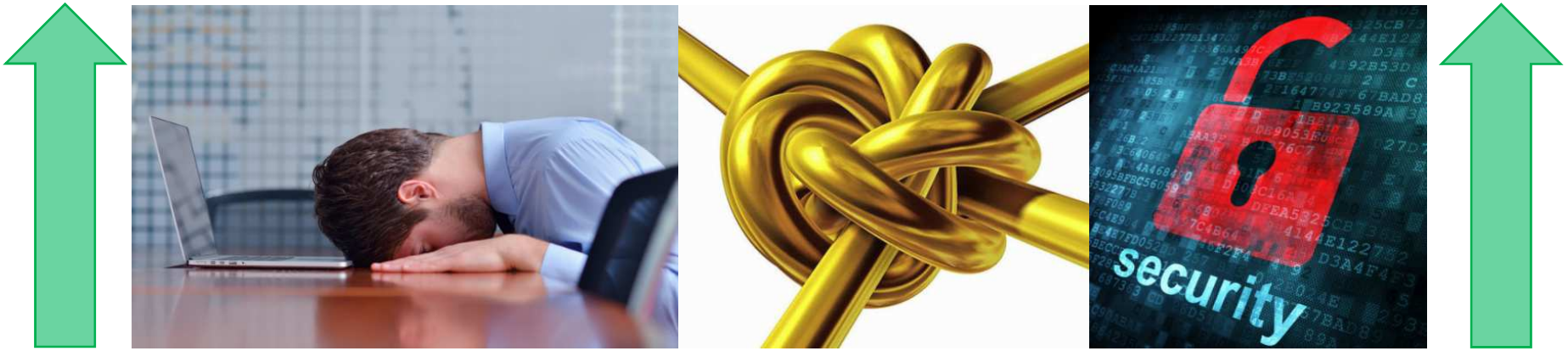
Verletzungen

Hygienische Probleme
Mafia-Finger

Quelle: CAS IS, R. Portmann

Gordischer Knoten

Produktivität, Effizienz und Benutzerfreundlichkeit vs IT Security

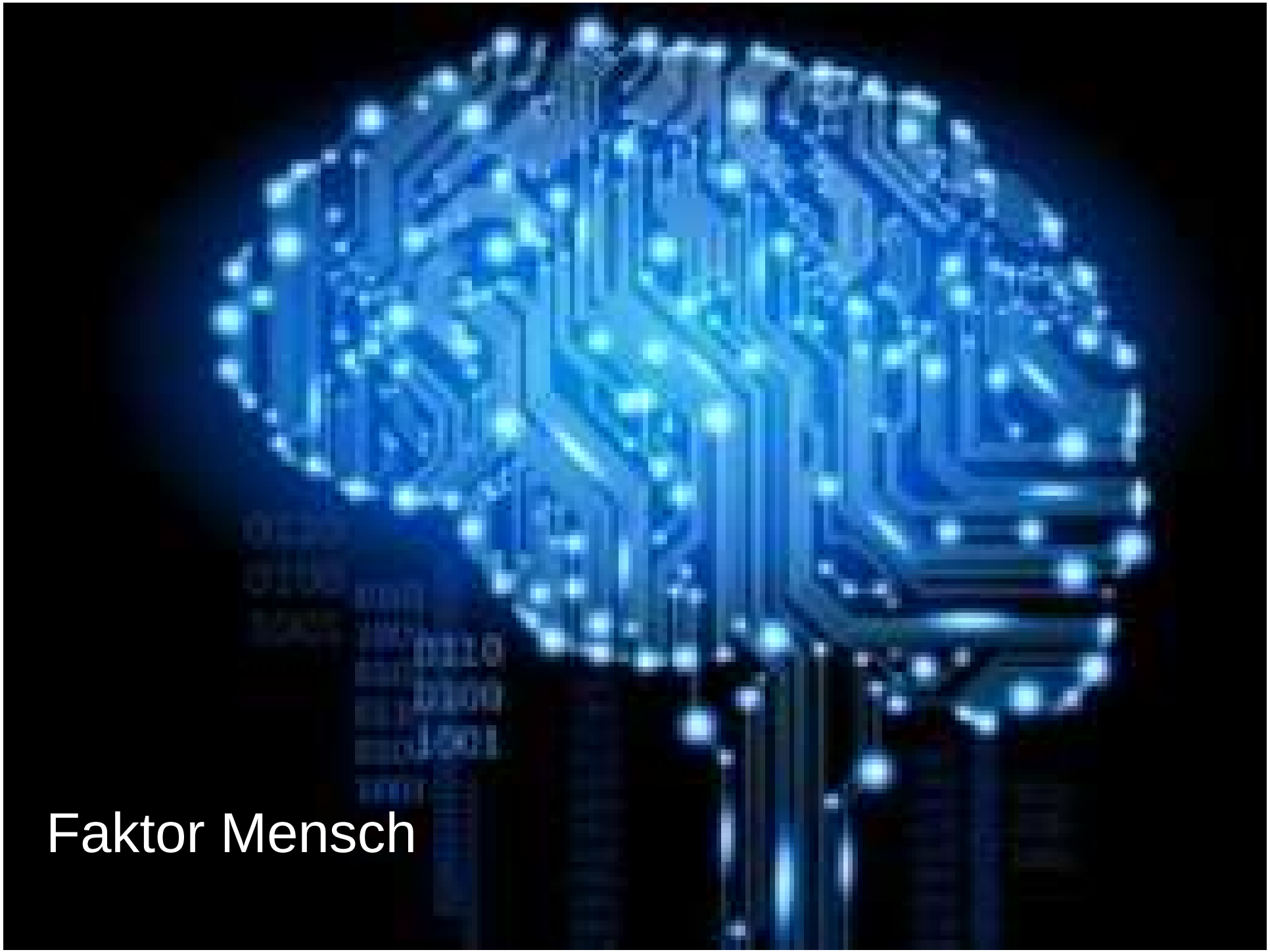


(Digital) Post-it

2 Faktor Authentisierung: Legic + PIN

Analogie:

+ PIN


Faktor Mensch

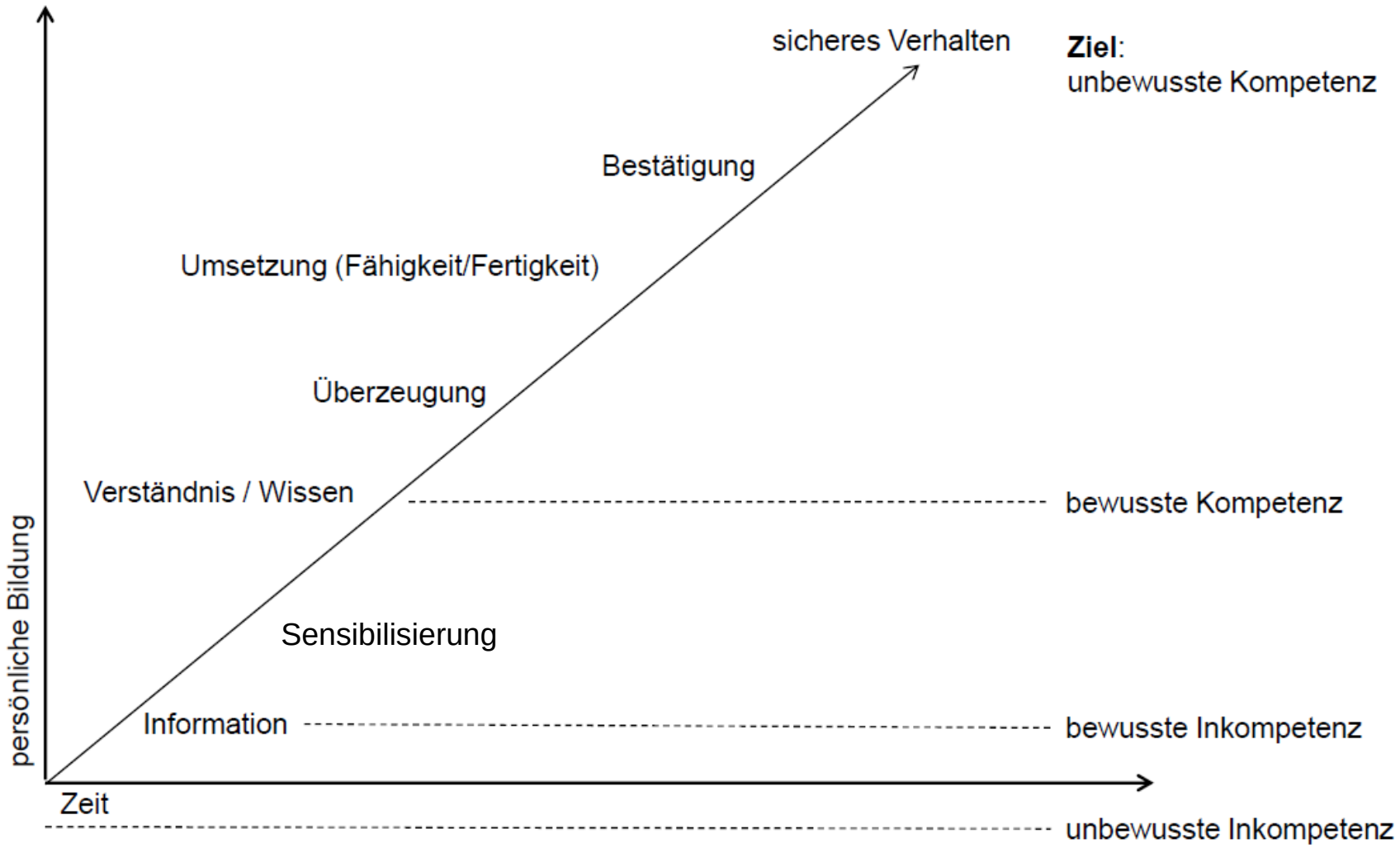
Laptop-Dieb erwischt Daten von 800'000 Ärzten

Wer empfindliche Daten auf seinem Laptop hat, sollte diese verschlüsseln. Ein Ratschlag, der immer wieder missachtet wird. So befanden sich ***persönliche Daten*** (so zum Teil auch die in den USA wichtige Sozialversicherungsnummer) von allen ungefähr 800'000 praktizierenden Ärzten der USA ***unverschlüsselt auf einem Laptop eines Angestellten*** der 'Blue Cross and Shield Association', einem Krankenversicherer. Der ***Laptop*** wurde ***gestohlen***.

Der Angestellte hatte ***verbotenerweise*** die Daten ***unverschlüsselt*** auf seinem Laptop abgelegt. Die Versicherung bietet nun den Ärzten, deren Sozialversicherungsnummer zu den "verlorenen" Daten gehört, an, ihre Kreditkartenkonten durch einen Dienstleister beobachten zu lassen, um einen allfälligen Identitätsdiebstahl rasch zu bemerken. (hc)

Quelle: 16.10.2009/www.inside-it.ch

Lernkurve Menschen



Quelle: www.ispin.ch

Awareness Kampagne

Kampagne

Zutritt und Umgang mit externen Personen!

Halten Sie sich bei der Bekanntgabe von Informationen zurück.

Vertrauliche Dokumente gehören nicht in den Papierkorb.

Lassen Sie vertrauliche Informationen nicht frei zugänglich liegen.

Sperren Sie den PC über die Tasten-kombination [Ctrl] + [Alt] + [Del]

Umgang mit elektronischen Informationen!

Lerneffekte

- Aktuelles Beispiel DHL Mail
- Alte «Masche»: Phishing/ Versenden von gefälschten Mails im Namen Dritter / Anhänge mit Schadcode…..
- Beispiel LUKS:
  - Awareness-Kampagne 2012/3, wiederkehrende Intranet-Meldungen zum Thema (letzte Veröffentlichung Februar 2015),
  - Resultat: ca. YX Personen öffneten den Virenverseuchten Mailanhang
  - ca. AB Mitarbeiter öffnen den Link…

Warnung vor gefälschten SMS mit Absender DHL

18. Juni 2014 | Derzeit werden im Namen der Firma DHL SMS versandt, die eine bislang unbekannte Schadsoftware enthalten. Die Empfänger werden aufgefordert, einen in der SMS enthaltenen Link anzuklicken, um eine entsprechende Paket-Lieferung zu verfolgen.

Diese SMS stammen nicht von der Firma DHL. Die Firma DHL verschickt grundsätzlich keine SMS mit Links auf Internetseiten.

Klicken Sie nicht auf den angegebenen Link, da auf diese Weise versucht wird, Ihr Handy mit Schadsoftware zu infizieren bzw. Ihre persönlichen Daten auszuspähen!

Sollten Sie bereits auf den Link geklickt haben, so ist nicht auszuschließen, dass Ihr Handy mit einer Schadsoftware infiziert wurde. In diesem Fall sollten Sie das Gerät mit einer entsprechenden Anti-Viren-Software überprüfen oder das System komplett neu aufsetzen.

Vorsorglich sollten Sie außerdem alle Passwörter und Zugangsdaten, die Sie auf dem betroffenen Gerät eingegeben haben, mithilfe eines zweiten, nicht-infizierten Gerätes ändern.

Auf der Webseite der Firma DHL finden Sie zusätzliche Sicherheitshinweise.

Bislang sind zwar nur Fälle mit Absender DHL bekannt geworden, es ist jedoch nicht auszuschließen, dass auch andere Firmen als Absender erscheinen können.

DHL

DHL Sendungsverfolgung

Sendungsnummer	11242017452
Produkt / Service	DHL PAKET
Status vom Freitag, 29.05.2015 11:30:56	Die Sendung wurde in das Zustellfahrzeug geladen.
Zugestellt an	Familienangehöriger

Detaillierte Empfängerinformationen anzeigen
(Adobe PDF Format)

Deutsche Post DHL - The Mail & Logistics Group

luzerner kantonsspital
LUZERN SURSEE WOLHUSEN

Point of View

Konklusion

- Bedrohungen nehmen im Gesundheitswesen zu
- Technik: meistens ein Schritt zu spät
- Zuwenig und zu viel Sicherheit kann gefährlich werden
- Awareness: Croudsourcing
- Engpass ist menschliches Verhalten

Sicherheit wird dann gelebt, wenn ihre Umsetzung nicht wahrgenommen wird und im täglichen Leben nicht einschränkt!

Vielen Dank für Ihre Aufmerksamkeit

Dr. med. S. Hunziker, Executive MBA UZH
Wirtschaftsinformatiker FH
Luzerner Kantonsspital

stefan.hunziker@luks.ch

☎ +41 41 205 25 24