LUZERNERPOLIZEI

Aus- und Weiterbildung
Chef/Chefin Bevölkerungsschutz

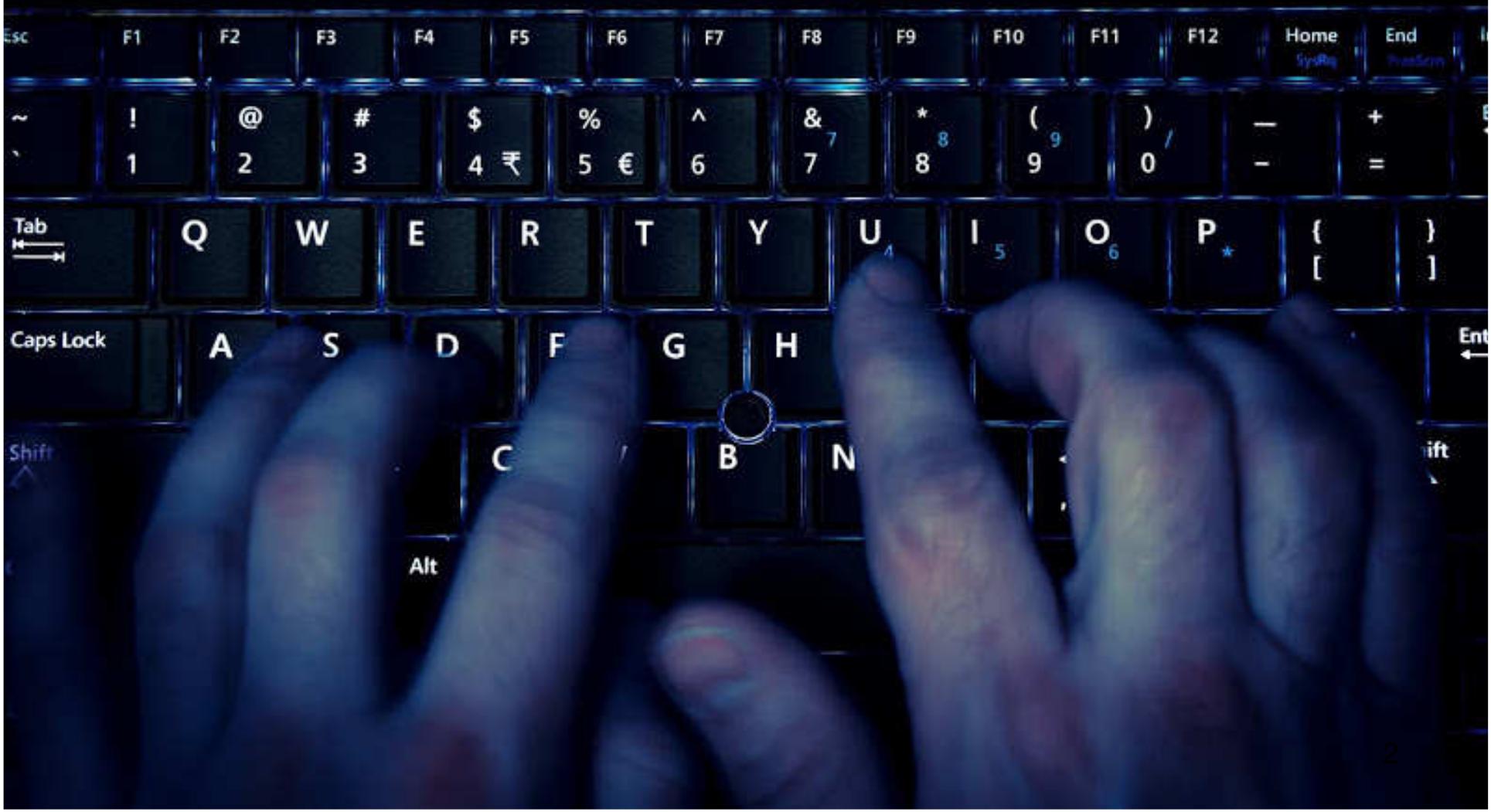
Cyberanschläge und Sicherung von wichtigen Daten

Impulsreferat

Michael Muther, Chef Technik und Logistik
12.09.2016

Worauf müssen wir uns (in Zukunft) gefasst machen?

Die Frage ist nicht ob, sondern wann!



LUZERNERPOLIZEI

Inhalt Impulsreferat

- Vorfälle in der Vergangenheit
- Verwundbarkeit der Zukunft

LUZERNERPOLIZEI

31 Attacken auf Schweizer Wasserkraftwerke

Von Barnaby Skinner, 8. Februar 2015 51 Kommentare »

Die «SonntagsZeitung» gab drei Wochen vor, ein Wasserkraftwerk zu sein - und wurde aus weltweit 15 Destinationen von Hackern angegriffen.

Teilen 477 Tweeten

Russische Hacker enttarnen geheime Schweizer Elitetruppe

Cyber-Attacke gegen Rüstungskonzern Ruag

NZZ am Sonntag / von Stefan Bühler, Andreas Schmid / 8.5.2016, 08:12 Uhr

...griff auf die Ruag sind auch die Personalien der ...entwendet worden. Es wird geprüft, den

Wenn Cyberkriminelle ein Krankenhaus lahmlegen

20. März 2016, 10:05 Uhr Klinikum Neuss

Nach einem Hackerangriff verwenden Chefärzte Klemmbretter statt iPads, Arztbriefe werden wieder per Hand geschrieben. Ein Besuch im Klinikum Neuss.

ANZEIGE

TEILE IHRE

Präpariertes Worddokument 06. Januar 2016 23:09; *Akt: 06.01.2016 23:09*

Hacker stellen 700'000 Menschen den Strom ab

Wegen eines Cyberangriffs sassen 70
Auch in der Schweiz steht kritische In
Fokus von Hackern.

Massive Cyber-Attacke auf Schweizer Webshops?

Dienstag, 15. März 2016, 7:47 Uhr 2 7

Währ ...Stunden gähnende weisse Leere im Browser.
Min ...hweizer Online-Shops sind am Wochenende
un ...ichen gewesen. Ein Anbieter geht
da ...geworden zu sein. Ein
E ...tergrund nahe.

KRITISCHE INFRASTRUKTUR

Wasserversorgung durch Hackerangriffe gestört

Bislang haben Hackerangriffe in Deutschland noch nicht zu Ausfällen bei der Wasserversorgung geführt. Anders als die Sicherheitsbehörden sehen die Versorger dafür auch keine große Gefahr.

Publikation von Kundendaten angedroht

Die Genfer Kantonalbank wird erpresst

9.1.2015, 16:30 Uhr

Die Genfer Kantonalbank ist Opfer eines Hacker-Angriffs geworden. Die He... veröffentlichen falls die Bank nicht 10 000 Euro zahlt.

26.02.15

DIGITAL CYBERANGRIFFE

Hacker zielen auf das Herz der Industrie

Im Internet der Dinge weiten sich Hacker-Angriffe auf physische Ziele aus, wie etwa Infrastruktur und Industrieanlagen. Großkonzerne verzeichnen 50 bis 100 Millionen Eindringversuche – pro Tag.

Regierungen der industriellen Welt, Ihr müden Giganten aus Fleisch und Stahl, ich komme aus dem Cyberspace, der neuen Heimat des Geistes.
Im Namen der Zukunft bitte ich Euch, Vertreter einer vergangenen Zeit: Lasst uns in Ruhe! Ihr seid bei uns nicht willkommen. Wo wir uns versammeln, besitzt Ihr keine Macht mehr.

(Unabhängigkeitserklärung des Cyberspace, John Perry Barlow)

Die neue Heimat des Geistes

- 1996 verabschiedete die US-Regierung den "Telecommunication Reform Act"
- John Perry Barlow verfasste daraufhin seine "Unabhängigkeitserklärung des Cyberspace"

- John Perry Barlow ist amerikanischee Autor, Bürgerrechtler und Mitbegründer der "Electronic Frontier Foundation"

- Wie recht John Perry Barlow hat, wurde uns das erst mal 2007 so richtig bewusst.

Estland 2007

Estland 2007

- Estland ist ein hoch technologisiertes Land
  - Estland führte als erstes Land der Welt online Wahlen ein
  - 97% der Bankgeschäfte via Online Banking
  - High Speed Internet Zugang gilt als Grundrecht
  - die meisten Behördengänge werden online angeboten und durchgeführt

Estland 2007

- Russische Besatzung von Estland nach dem 2. Weltkrieg
  - mehrere Hunderttausende Russen angesiedelt
- Denkmal wurde in Stadtzentrum Tallin errichtet, welches an die gefallenen russischen Soldaten des 2. Weltkrieges erinnern sollte
  - Für Bevölkerung Estland ein geschmackloses Zeichen der Besatzung und Unterdrückung
- 1991 zerfiel Ostblock - Estland war wieder frei
- 2007 beschloss die Estnische Regierung die Statue aus dem Stadtzentrum in einen nahe gelegenen Militärfriedhof zu verlegen
- Die Ankündigung sorgte bei den verbliebenen Russen für Empörung
  - gewaltsame Ausschreitungen

Estland 2007

- 27.04.2007, Angriff auf Webseiten der Regierung (DDOS Angriffe)
- 09.05.2007 DDOS Peak mit 4 Mio Datenpaketen pro Sekunde
  - 2007 hatten gewöhnliche Cyberkriminelle diese Fähigkeiten noch nicht
- Grossangelegter DDOS Angriff auf Webseites und Services von Estland
  - Kein Finanztransaktionen mehr
  - Behörden wurden lahmgelegt
  - Keine Möglichkeit mehr zu kommunizieren (Behörden und Bürger)
    - Keine News mehr für Bevölkerung
- Estland war von der Aussenwelt abgeschnitten

Fazit - Estland 2007

- Kollaps von Regierungen, Bankwesen und Medien
- Dimension des Angriffs übertraf alles, was man bis dato kannte
- Erster, der breiten Öffentlichkeit bewusst gewordener Fall von Cyberkriegsführung
- Internet wurde zum 1. Mal als "Waffe" benutzt um ein ganzes Land lahm zu legen
- Einen Beweis, wer hinter den Angriffen steckt, gibt es bis heute nicht
  - Hacker?
  - Russische Armee?
  - Kriminelle Organisationen?
- Spielregeln einer Kriegsführung im Cyberraum gibt es nicht, weil Angreifer oft unbekannt bleibt

Strassenbahn-Hack in Polen 2008

- Einem 14 Jährigen gelang es in Polen, eine öffentliche Strassenbahn als private Modelleisenbahn zu verwenden.
  - Das System der öffentlichen Trambahn wurde gehackt
- Es gelang dem Teenager Signale zu steuern
- Er hatte eine TV-Fernbedienung zu einem Gerät umfunktioniert, mit dem sich alle Weichen der Strassenbahn schalten liessen
- 4 Bahnen entgleisten, Zwölf Verletzte

LUZERNERPOLIZEI

Präpariertes Worddokument 06. Januar 2016 23:09; *Akt: 06.01.2016 23:09*

Hacker stellen 700'000 Menschen den Strom ab

Wegen eines Cyberangriffs sassen 70
Auch in der Schweiz steht kritische In
Fokus von Hackern.

31 Attacken auf Schweizer Wasserkraftwerke

Von Barnaby Skinner, 8. Februar 2015 51 Kommentare »

Die «SonntagsZeitung» gab drei Wochen vor, ein Wasserkraftwerk zu sein - und wurde aus weltweit 15 Destinationen von Hackern angegriffen.

Teilen 477 Tweeten

Cyber-Attacke gegen Rüstungskonzern Ruag

Russische Hacker enttarnen geheime Schweizer Elitetruppe

NZZ am Sonntag / von Stefan Bühler, Andreas Schmid / 8.5.2016, 08:12 Uhr

griff auf die Ruag sind auch die Personalien der
ntwendet worden. Es wird geprüft, den

20. März 2016, 10:05 Uhr Klinikum Neuss

Wenn Cyberkriminelle ein Krankenhaus lahmlegen

Nach einem Hackerangriff verwenden Chefärzte Klemmbretter statt iPads, Arztbriefe werden wieder per Hand geschrieben. Ein Besuch im Klinikum Neuss.

ANZEIGE

TEILE IHRE

Massive Cyber-Attacke auf Schweizer Webshops?

Dienstag, 15. März 2016, 7:47 Uhr 2 7

Währ Stunden gähnende weisse Leere im Browser.
Min hweizer Online-Shops sind am Wochenende
un ichen gewesen. Ein Anbieter geht
da geworden zu sein. Ein
E tergrund nahe.

KRITISCHE INFRASTRUKTUR

Wasserversorgung durch Hackerangriffe gestört

Bislang haben Hackerangriffe in Deutschland noch nicht zu Ausfällen bei der Wasserversorgung geführt. Anders als die Sicherheitsbehörden sehen die Versorger dafür auch keine große Gefahr.

Publikation von Kundendaten angedroht

Die Genfer Kantonalbank wird erpresst

9.1.2015, 16:30 Uhr

Die Genfer Kantonalbank ist Opfer eines Hacker-Angriffs geworden. Die H
veröffentlichen falls die Bank nicht 10 000 Euro zahlt.

26.02.15

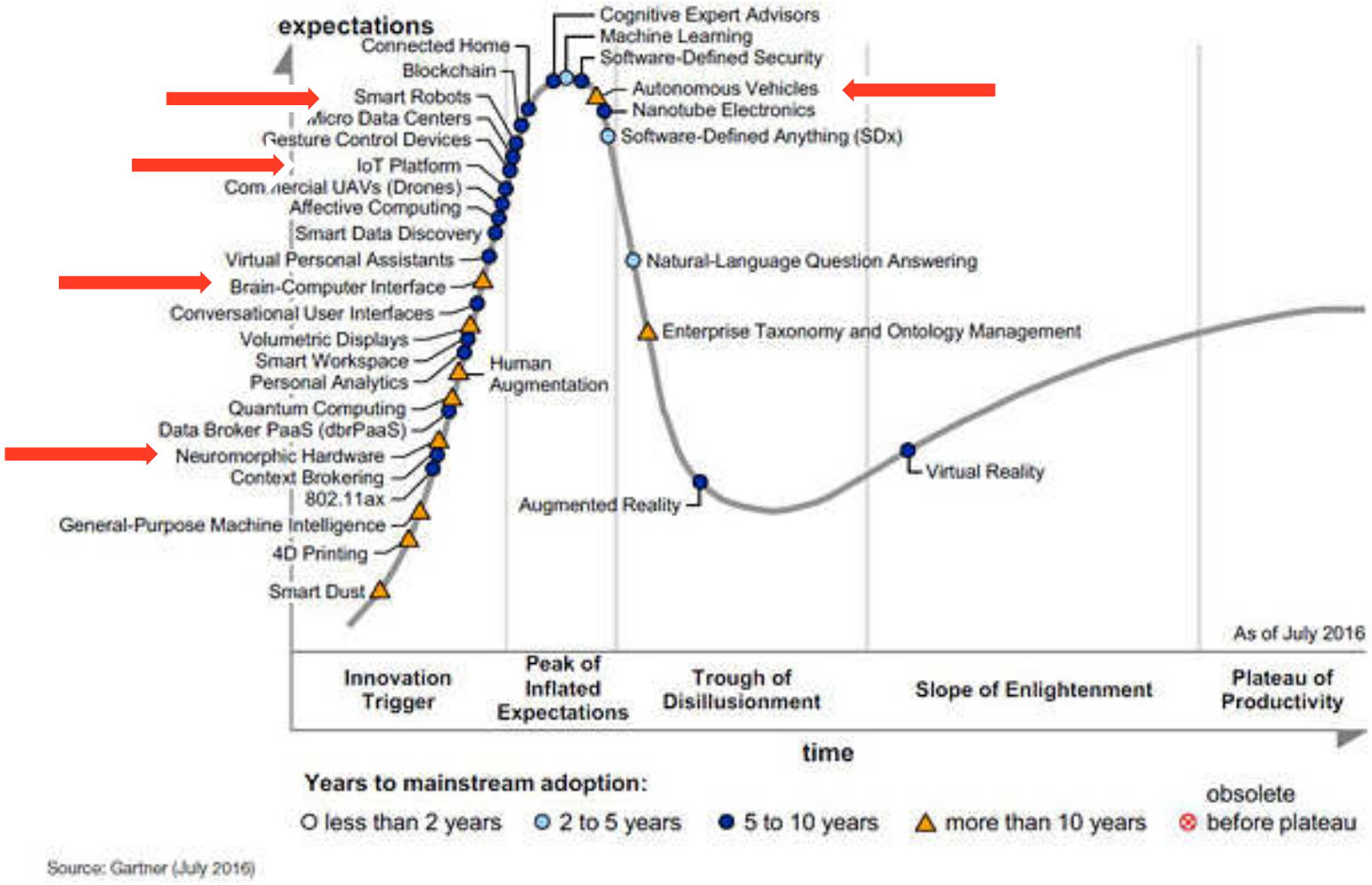
DIGITAL CYBERANGRIFFE

Hacker zielen auf das Herz der Industrie

Im Internet der Dinge weiten sich Hacker-Angriffe auf physische Ziele aus, wie etwa Infrastruktur und Industrieanlagen. Großkonzerne verzeichnen 50 bis 100 Millionen Eindringversuche – pro Tag.

...und die Zukunft?

Emerging Technologies



Source: Gartner (July 2016)

Internet of Things (IoT)

IoT

- Durch die Einführung von IPv6 verfügen wir technisch über so viele IP-Adressen, dass jedes Sandkorn an das Internet angeschlossen werden könnte
- Dies ebnet den Weg für Internet of Things
- IoT ist die Vernetzung herkömmlicher Geräte wie Waschmaschinen, Backöfen, Schliessanlagen, Fahrzeuge, etc zu intelligenten Systemen, die mit der Umwelt und uns kommunizieren können
  - Waschmaschine gibt via Smartphone App bescheid, wann die Wäsche aufgehängt werden kann
  - Haus schliesst sich automatisch ab, wenn wir es verlassen
  - Fahrzeug findet kommt aus Parklücke autonom zu uns, wenn wir es rufen
  - Seldstdimmende Strassenlaternen, wenn niemand in der Nähe ist
- Ziel von IoT ist die Verschmelzung der realen Welt mit der virtuellen Welt.

IoT

- Immer mehr Fahrzeuge werden zu IoT Geräten und mit der Umwelt vernetzt
- Am 1. Juli 2015 rief Fiat Chrysler in den USA 1.4 Millionen Fahrzeuge (Jeep Cherokee) zurück
- Es bestand die Gefahr, dass über das integrierte Entertainment System das Fahrzeug gehackt werden konnte

Was ist gefährlich an IoT?

- Vergrösserung der Angriffsfläche.
  - Anstatt EINEM Ziel-Computer stehen einem Angreifer dutzende Geräte als potentielles Ziel zur Verfügung
  - Neu kann ein Angreifer auch Einfluss auf Licht, Storen, Kühlschränke, Videoüberwachungsysteme, Alarmanlagen, etc. nehmen
- Potentielle Erweiterung von IoT Geräten durch Einschleusung von Schadsoftware zu Bot-Netzen für DDOS Angriffe
  - Bot Netze mit Millionen von Rechnern!!!

SCADA

- Speicher Programmierbare Steuerungen (SPS) steuern heute die gesamte Welt:
  - Liftsteuerungen
  - Heizungen
  - Klimaanlagen
  - Verkehrsampeln
- SCADA ist auch Antrieb der Smarten Industrie (Industrie 4.0)
- In der Grossindustrie werden einzelne SPS in einem zentralen Steuerungssystem SCADA zusammengefasst (**S**upervisory **C**ontrol **a**nd **D**ata **A**cquisition)
- SCADA Systeme (Software) sind teilweise Jahrzehnte alt und in die IT-Infrastruktur via Netzwerk integriert. Beim Design von SCADA stand Sicherheit nicht im Vordergrund

SCADA

- Industriebetriebe setzen SCADA-Systeme ein, um per Fernzugriff Produktionsanlagen zu steuern.
  - Kraftwerke (auch Kernkraftwerke!!)
  - Fabriken
  - Öl-Raffinerien
  - Wasserpipelines
- SCADA Systeme sind auch Basis unserer Stromversorgung
- Dell SonicWALL hat 2014 eine Verdoppelung der SCADA-Attacken beobachtet

SCADA-Angriffe

- AURORA Experiment
  - Isolierter Generator, welche via SCADA gesteuert wird
  - Ziel war Zerstörung des Generators
  - ….es gelang problemlos…

- Stuxnet
  - Computerwurm mit der Fähigkeit SCADA Systeme zu manipulieren (z.B. Frequenzumrichter)
    - Frequenzumrichter braucht man, um Geschwindigkeit von Motoren zu steuern
    - Störung des iranischen Atomprogramms

Fakt ist..

- …..Software wird durch Menschen geschrieben und Software ist nie perfekt (Bug-Dichte ca. 3 Fehler pro 1000 Zeilen Code). Windows 7 besteht aus ca. 40 Millionen Codezeilen.
- …..durch stetig zunehmende Rechnerleistung und höherer Internetgeschwindigkeit erhalten Cyberkriminelle und Cyberterroristen potentielle Waffen in die Hände (exponentielles Wachstum)
- ….die Auswirkungen eines Menschen mit krimineller Energie auf Opfer steigt exponentiell (z.B. Sony Playstation Hack 2011, Kreditkartendaten von 77 Millionen Menschen wurden entwendet)
- ….IPv6 ermöglicht die Anbindung ALLER Geräte ans Internet (Internet of Things). Das hat radikale Implikationen auf unsere Sicherheit, weil mehr verbundene Geräte mehr Schwachstellen besitzen, welche ausgenutzt werden können.
- …Gartner Group geht davon aus, dass bis ins Jahr 2020 25 Milliarden intelligente Geräte ans Netz gehen werden (3 x mehr als Weltbevölkerung)

Mögliche Ziele der Zukunft

- SCADA Systeme
- SmartHome und IoT-Technologien
- Selbstfahrende Fahrzeuge
- Wearables
- Implantate wie Herzschrittmacher, Insulinpumpen, Defibrillatoren
- Digitale Währungen (BitCoin, etc)

- **Alle Dinge die unser modernes Leben ausmachen und an die wir uns gewöhnt haben, sind in Gefahr!**

Fazit

- Staatliche Cyberwaffen können sich in Zukunft vermehr in den Händen von Cyberkriminellen befinden
- Wir müssen uns darauf gefasst machen, dass die GFS und KFS nicht mehr nur Unfälle und Naturereignisse zu bewältigen haben
- Wir müssen uns darauf vorbereiten, dass wir eine Lage auch dann bewältigen können, wenn kein Strom vorhanden ist und unsere Kommunikationssysteme gestört sind
- Die Bevölkerung muss sensibilisiert werden
- Die Strafverfolgung im Bereich Cyberkriminalität muss aufgerüstet und zusammengelegt werden (Kompetenzzentren)
- Die Industrie und vor allem die Unterhaltungsindustrie müssen sich Gedanken über "Sicherheit" machen
- IT-Sicherheit ist Thema für das Top-Management der Unternehmen und erfordert Geld, Know-how und personelle Ressourcen