LUZERN

KANTON LUZERN

Schutz vor Cyberbedrohungen

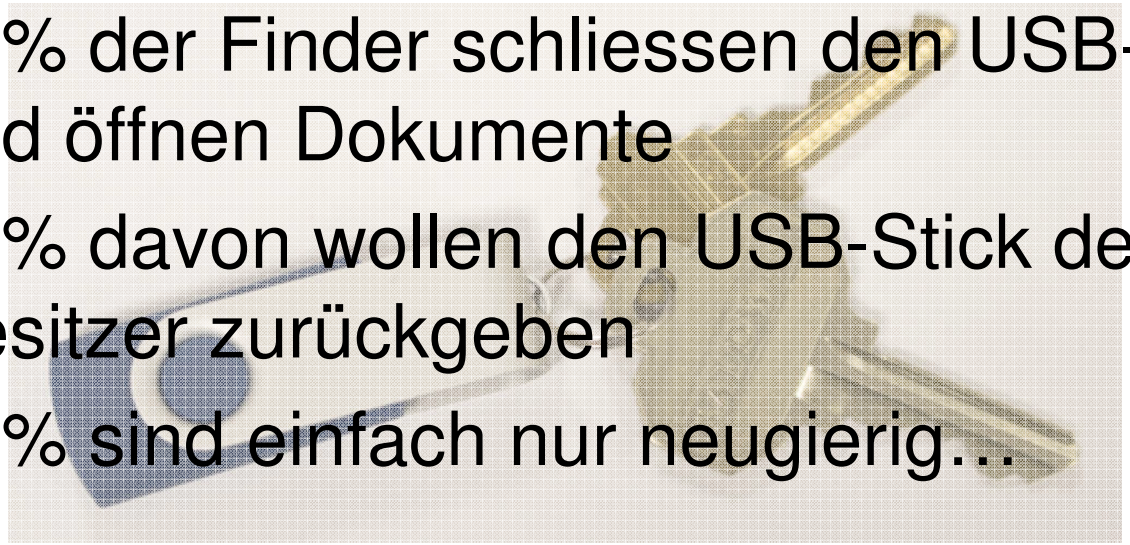
Schutzmassnahmen

12.09.2016 - MUM

Dienststelle Informatik | informatik.lu.ch

Frage 1

Was machen Sie mit einem gefundenen USB-Stick?

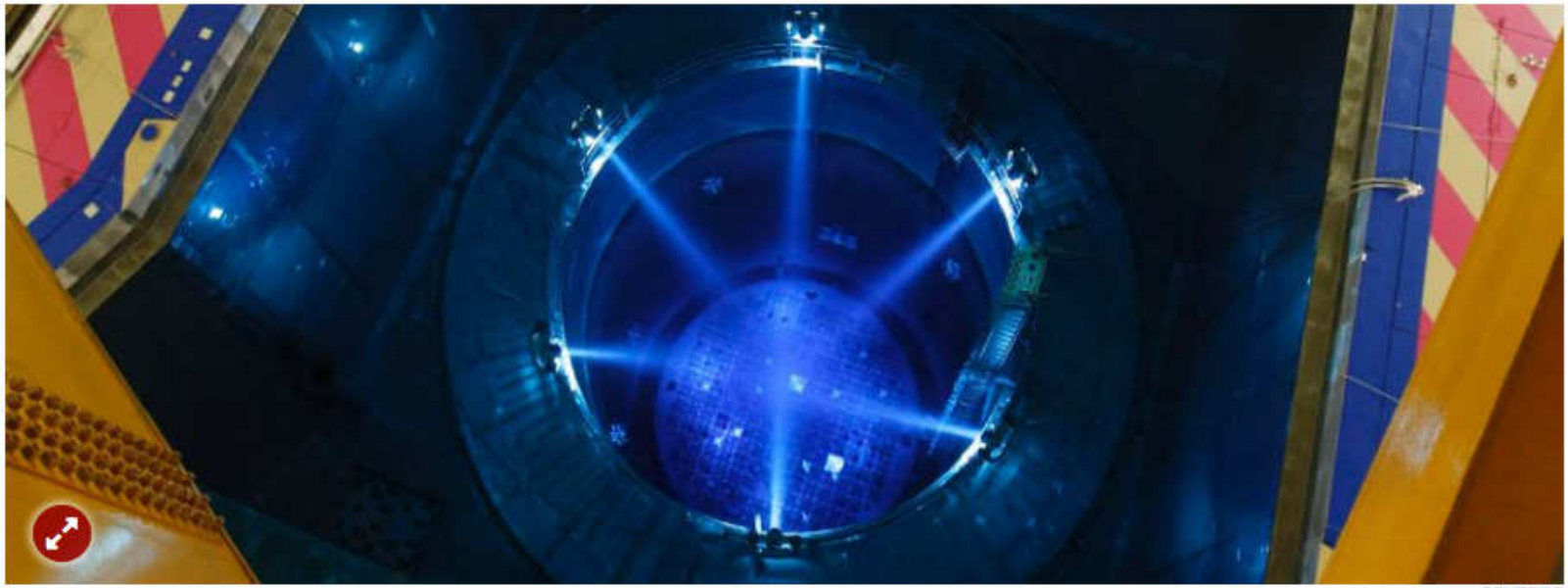


- 48% der Finder schliessen den USB-Stick an und öffnen Dokumente
- 68% davon wollen den USB-Stick dem Besitzer zurückgeben
- 19% sind einfach nur neugierig…

Quelle: Studie Universität Illinois, Universität Michigan und Google, April 2016, https://zakird.com/papers/usb.pdf

Virus im Atomkraftwerk kam über USB-Stick

Die Quelle ist ausgemacht: Die Schadsoftware, die im bayerischen Atomkraftwerk Gundremmingen entdeckt worden war, gelangte laut Innenministerium über einen USB-Stick auf das Computersystem.



REUTERS

Quelle: http://www.spiegel.de/netzwelt/web/gundremmingen-virus-im-atomkraftwerk-kam-ueber-usb-stick-a-1095331.html

Frage 2

Sie erhalten eine E-Mail von info@coop.ch mit dem Betreff: Bestellung, im Anhang ein Word-Dokument.

- Aktuelles Beispiel vom Kanton Luzern
- Antivirus erkannte Schadsoftware nicht
- ~300 Mails an Mitarbeitende (vor Blockade)
- 5 Computer neu aufgesetzt (1,6%)
- Dunkelziffer?

Folgerung?

- USB-Port sperren!
- Anhänge bei Mails-Blockieren!

  … und Links in Mails!

- Die richtigen, zahlbaren Massnahmen auszuwählen ist eine Herausforderung

Richtige Massnahmen?

Quelle: http://www.forum-3dcenter.org/vbulletin/showthread.php?t=549211

Ziele

- **Umfassender Schutz vor Cyberbedrohungen**

- Preiswert
- Nicht kompliziert, Mitarbeiter müssen arbeiten können

Inhalt

1. Zur Person
2. Risiko-Felder
3. Organisatorische Massnahmen
4. Technische Massnahmen
5. Wer hilft?
6. Tipp für den Bevölkerungsschutz

Zur Person

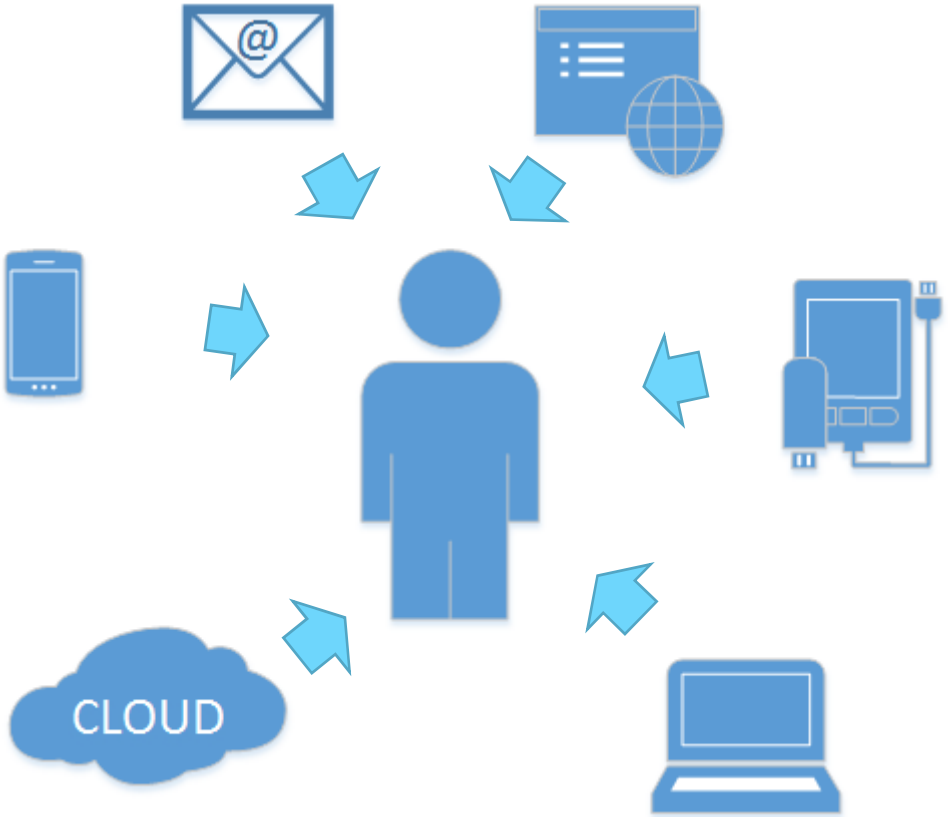
Martin Müller
IT-Security und Risikomanager
Dienststelle Informatik (DIIN), Kanton Luzern

- Internationale Erfahrung im Regierungsumfeld ("Notfallorganisationen")
- Dienstleister im Bank/Zahlungs-Umfeld

Risiko-Felder Cyberbedrohungen

- Mensch
- Vernetzung/Internet
  - E-Mail
  - Browsen/Internet
  - Prozess-Automation
  - Auslagerung von Informationen
- Infrastruktur
  - IT Systeme, Netzwerk
  - Gebäudeautomation
  - Überwachung, Alarm
- Informationen
  - Manipulierte Daten
  - Kein Zugriff
- Angriffe auf Dritte
  - Kein Strom
  - Kein Zahlungsverkehr
  - Falschinformationen in den Medien
  - Falsche Informationen
- **Abhängigkeit**

Risikofeld Mensch



Wie darf/muss sich der Mitarbeitende verhalten?

Organisatorische Massnahmen

- Sensibilisieren,
  Neu-Deutsch: Awareness erhöhen
  - Umgang mit Informationen (Telefon, Papier)
  - Umgang mit Informatikmittel (E-Mail, USB-Stick)
  - Regelmässig schulen und prüfen

- Weitere organisatorische Massnahmen:
  - Klassifizieren von Informationen und Vorgängen
  - Weisungen erstellen, durchsetzen, überprüfen
  - Bei kritischen Vorgängen: 4-Augen Prinzip

Massnahmen - Mensch

- Beispiel E-Mail:
  - Vorsichtiger Umgang mit der E-Mail Adresse
  - Vorsicht bei E-Mails mit unbekannten Absender
  - Vorsicht bei Anhängen
- Beispiel Internet/Surfen:
  - Auf "seriöse" Anbieter achten
  - Keine unbekannten Programme herunterladen
  - Vorsicht Weitergabe von Informationen, z.B. in Foren

Massnahmen - Mensch

Aktuelles Beispiel: Dridex

- Malware, welche elektronische Zahlungen "anpasst"
- Spannungsfeld:
  Automatisierung (Kosteneinsparungen) vs Kontrolle

Organisatorische Massnahmen

- Empfehlungen E-Mail und Internet/Surfen
- Überprüfung der Zahlungen
- Freigabeprozess (4-Augen)
- **Nicht nur auf das Total schauen!**

Risikofeld Mensch - Fazit:

- **Der Mensch bleibt immer ein Faktor**

- Sensibilisieren
- Organisatorische Massnahmen
- Technisch unterstützen

Risikofeld Technik

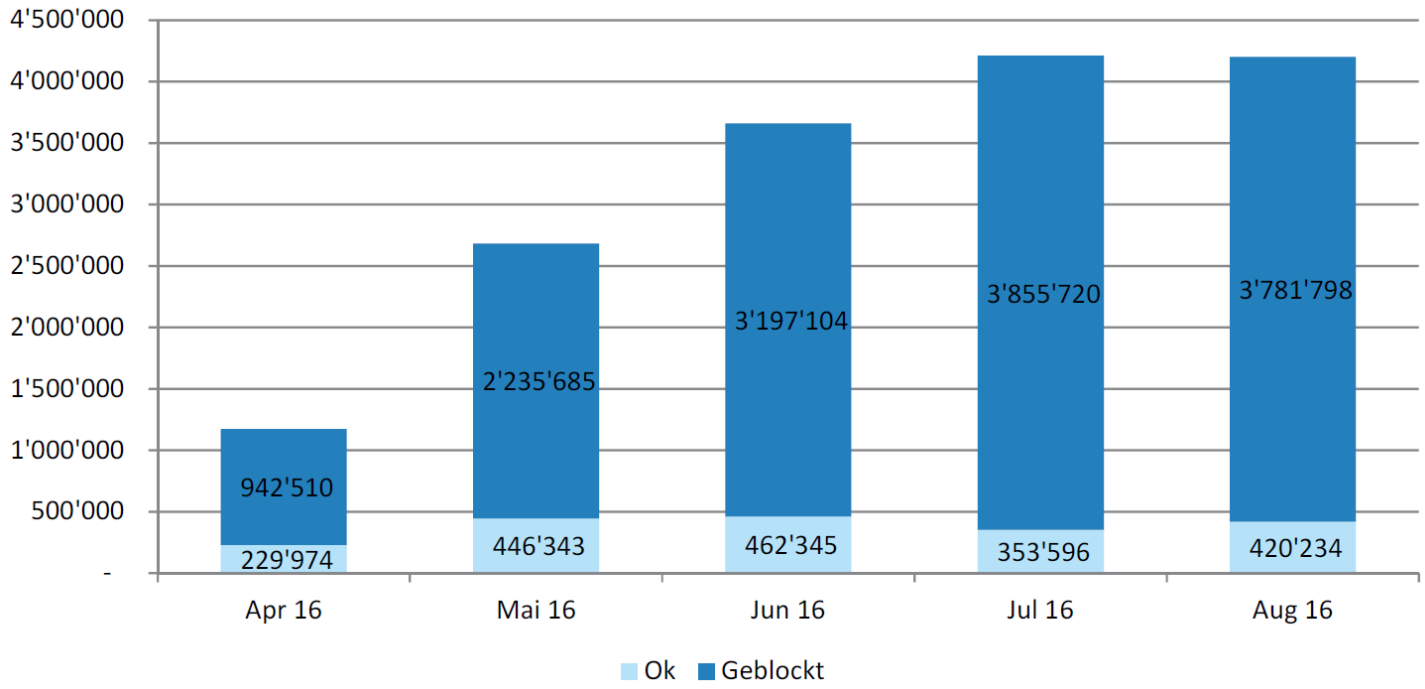
Was für Schnittstellen hat der Mitarbeitende zur "Aussenwelt"?

Massnahmen - E-Mail

- Beispiel E-Mail:
  Einsatz von Security Gateway
  - Filter von E-Mails nach Reputation des Senders, Inhalt (Wörter) etc.
  - Blockieren von speziellen Anhang-Typen
  - Anti-Malware Check

Massnahmen - E-Mail

- Analyse E-Mail Gateway Kanton Luzern:



Massnahmen - Internet

- Beispiel Internet:
  Einsatz von Security Gateway
  - Filter von Webseiten nach Reputation
  - Blockieren von verdächtigen Seiten
  - Überprüfung der Verbindungen
  - Anti-Malware Check

- Beispiele 2016 (2x bei News-Portalen CH)
  - Werbenetzwerke verteilen Schadsoftware
  - Reaktion: Blockieren von Werbe-Netzwerken

Technische Massnahmen - Beispiele

- Angriffserkennung
- Firewall

→ Netzwerk

- Berechtigungssystem
- Benutzermanagement

→ Management

- Aktuelle Software (mit den neusten Sicherheitsupdates)
- Datensicherung

→ Infrastruktur

Massnahmen - Technik

Aktuelles Beispiel: Dridex

- Malware, welche elektronische Zahlungen "anpasst"
- Spannungsfeld:
  Automatisierung (Kosteneinsparungen) vs Kontrolle

Technische Massnahmen

- E-Mail Filterung (Security Gateway)
- Nur mit minimalen Benutzerrechten arbeiten
- Rechte ausführbare Programme einschränken
- Optimal: Computer nur für elektronische Zahlungen

Technische Massnahmen - Fazit

- **Technischer Schutz ist möglich, ABER:**

- ist als Unterstützung zu den organisatorischen Massnahmen zu sehen
- ist zum Teil reaktiv (Security Gateways)
- benötigt Unterhalt

Kritische Infrastruktur

Will man Schutz vor Cyberbedrohungen, ist kritische Infrastruktur vom Internet zu trennen

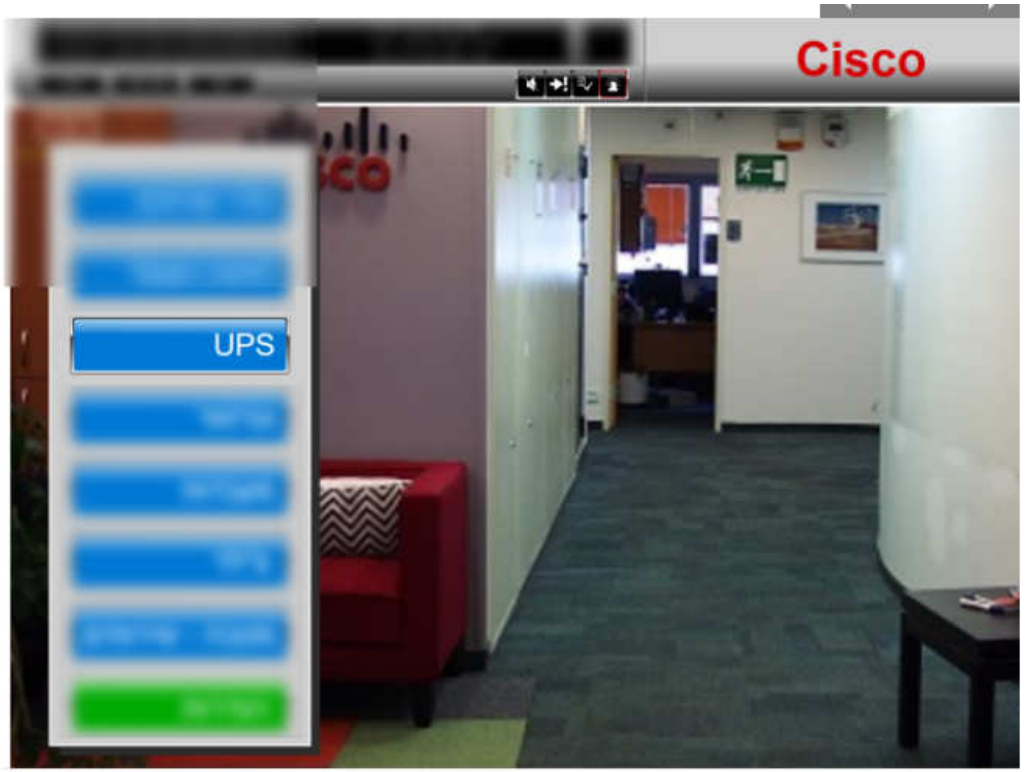
- Alarmierung?
- Überwachung?

Kritische Infrastruktur

- Nicht über Internet oder "Office"-Netzwerk
- Falls nicht anders möglich:
  "Passive" Sensoren ohne Schreib-Funktionalität

- Organisatorische Massnahmen!
- Technische Massnahmen!

Cisco-USV hilft Online-Ganoven beim Krypto-Mining



Quelle: http://http://www.golem.de/news/kritische-infrastrukturen-wenn-die-usv-kryptowaehrungen-schuerft-1608-122837-5.html

Und nun?

- Was ist abzusichern?
- Wer definiert die Massnahmen?
- Wer konfiguriert die Massnahmen?
- Wer betreibt die Massnahmen?
- Wer zahlt die Massnahmen?
- Wer reagiert auf Angriffe?
- Wie reagiert man auf Angriffe?

Und nun?

- Nur nicht den Kopf verlieren..

Wer kann helfen?

- Gute Zusammenstellung von Themen: https://www.melani.admin.ch/

Organisatorisch:

- Spezialisierte Firmen
- Austausch mit Partner

Technisch:

- Ihr IT-Anbieter
- Security-Provider
- Für Gemeinden: Kanton Luzern bietet Services geschützt durch Security Gateways an

Tipps für Bevölkerungsschutz

- **Hypothese: Cyberangriff entspricht totalem Stromausfall**

- IT vereinfacht Abläufe und soll benutzt werden
- Gehen Sie immer davon aus, in einer Kriese keine IT-Infrastruktur zu haben!
  - Kommunikation
  - Listen (Inventar, Kontakte) in Papierform
  - Aktualität?

Fazit Schutzmassnahmen

- Schutzmassnahmen sind organisatorisch und technisch notwendig
- Je mehr technischen Schutz, desto komplexer wird die Infrastruktur
- Anpassen der Massnahmen auf Ihre Organisation
- Sensibilisierung der Mitarbeitenden

Danksagung & Fragen

- Vielen Dank Ihre Aufmerksamkeit
- Fragen?

Quelle: http://www.hoax-slayer.com/images/unsubstantiated-cat-page.jpg