Cybersecurity und Security Management für kritische Infrastrukturen

6. VKÖ-Stadtwerketag 2018

Cyber Security Center BMI
Wien, 29. November 2018

Agenda

- Vorstellung
- Trends 2018
- Cyber Angriffe auf Kritische Infrastrukturen
- Schutz vor Angriffen

Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

Cyber Security Center

- Schutz kritischer Infrastrukturen
  - Frühwarnungen
  - Awarenessschulungen
  - Technische Analysen
- NIS-Richtlinie
  - NIS-Behörde (ab 2019)
- Cyber Krisen Management
- Operative Koordinierung zwischen Ressorts

Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

Trends 2018

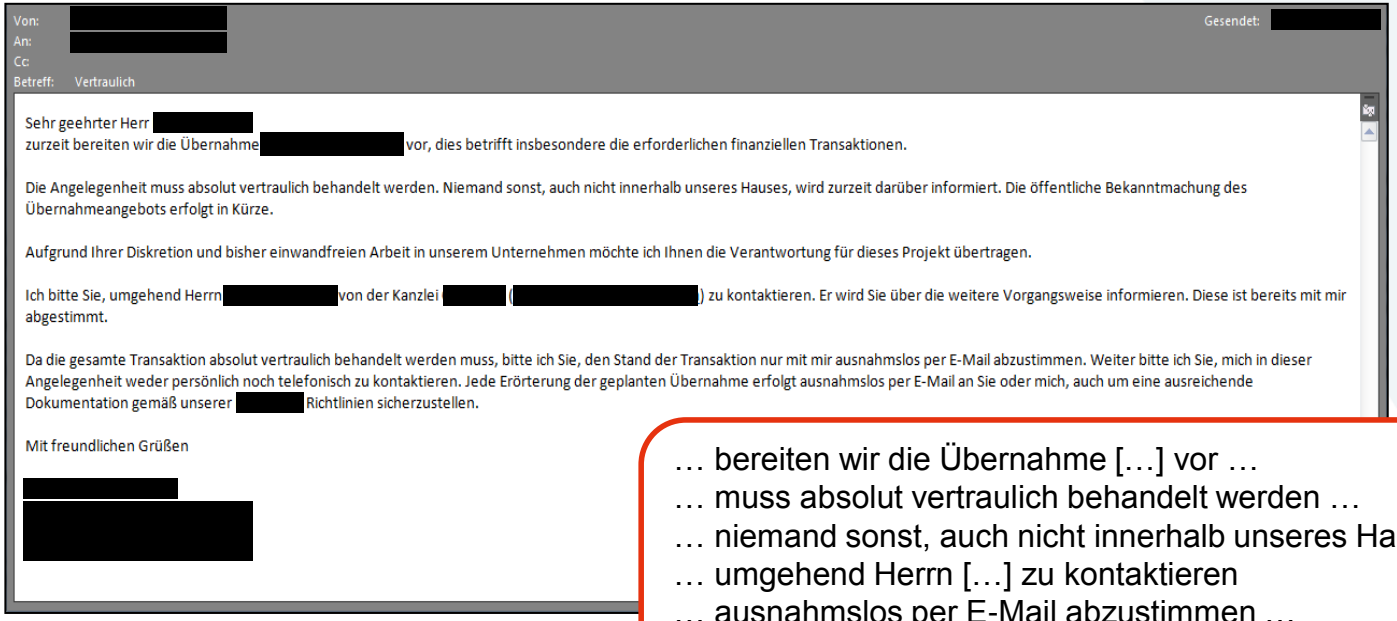
- Hosted Security und SOC-as-a-Service
- Machine Learning sowohl im Angriff als auch Verteidigung
- Angriffe auf Blockchains und Smart Contracts
- Kommerzialisierung und Konsolidierung des Cyber Crime Marktes
- Fachkräftemangel im IT-Sicherheitsbereich
- Cloud Computing, weniger Angriffe und Ausfälle, dafür mit drastischeren Folgen

Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

(Cyber) Angriffe auf Unternehmen der KI

Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

CEO-Fraud



Von: [redacted]
An: [redacted]
Cc:
Betreff: Vertraulich

Gesendet: [redacted]

Sehr geehrter Herr [redacted]
zurzeit bereiten wir die Übernahme [redacted] vor, dies betrifft insbesondere die erforderlichen finanziellen Transaktionen.

Die Angelegenheit muss absolut vertraulich behandelt werden. Niemand sonst, auch nicht innerhalb unseres Hauses, wird zurzeit darüber informiert. Die öffentliche Bekanntmachung des Übernahmeangebots erfolgt in Kürze.

Aufgrund Ihrer Diskretion und bisher einwandfreien Arbeit in unserem Unternehmen möchte ich Ihnen die Verantwortung für dieses Projekt übertragen.

Ich bitte Sie, umgehend Herrn [redacted] von der Kanzlei [redacted] ([redacted]) zu kontaktieren. Er wird Sie über die weitere Vorgangsweise informieren. Diese ist bereits mit mir abgestimmt.

Da die gesamte Transaktion absolut vertraulich behandelt werden muss, bitte ich Sie, den Stand der Transaktion nur mit mir ausnahmslos per E-Mail abzustimmen. Weiter bitte ich Sie, mich in dieser Angelegenheit weder persönlich noch telefonisch zu kontaktieren. Jede Erörterung der geplanten Übernahme erfolgt ausnahmslos per E-Mail an Sie oder mich, auch um eine ausreichende Dokumentation gemäß unserer [redacted] Richtlinien sicherzustellen.

Mit freundlichen Grüßen

[redacted]

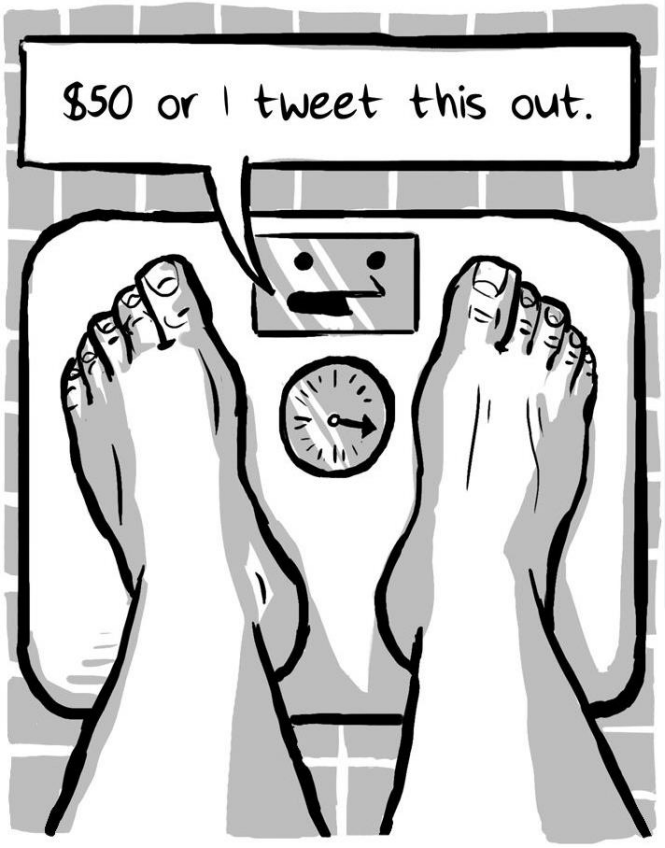
… bereiten wir die Übernahme […] vor …
… muss absolut vertraulich behandelt werden …
… niemand sonst, auch nicht innerhalb unseres Hauses …
… umgehend Herrn […] zu kontaktieren
… ausnahmslos per E-Mail abzustimmen …
… weder persönlich noch telefonisch zu kontaktieren …

Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

Ransomware

Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

Auch Ransomware…

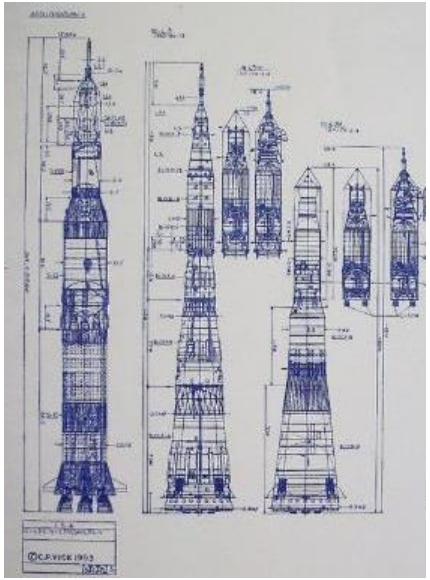


Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

Was tun? Wie schützen? Alles verloren?

Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

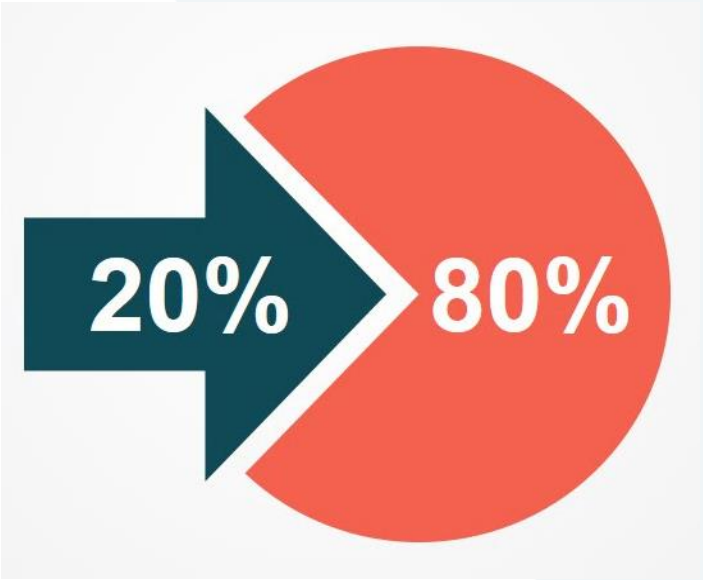
Rocket Science



”Floriani”- Prinzip

Heiliger Sankt Florian,
Verschon' mein Haus,
Zünd' and're an!

”Pareto”- Prinzip



Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

Was tun? Wie schützen? Alles verloren?

Über 80% aller Cyber Angriffe lassen sich durch grundlegende Maßnahmen und entsprechendes Sicherheitsbewusstsein verhindern

- **Awareness** der Mitarbeiter!
- **Technische** Vorkehrungen treffen!

Beispiel: **CIS Critical Security Controls**

- Frei verfügbar
- Ausgehend von tatsächlichen Angriffen und Bedrohungen
- Priorisierung und Auswahl der fundamentalsten Sicherheitsmaßnahmen mit dem größten Nutzen

CIS Center for Internet Security®

Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

…und die restlichen 20%?

„You can't defend. You can't prevent. The only thing you can do is detect and respond.“

Bruce Schneier

- Monitoring des eigenen Netzes nach erfolgreichen Angriffen
- Wonach genau soll gesucht werden? **Threat Intelligence**
- Betrieb von SIEM - Lösungen
- Benötigt Personal

- **Abwägung der Kosten gegen Risiko**

Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

Cyber-Sicherheit

- … ist nicht die Aufgabe anderer
- … ist ein Prozess und kein Zustand
- … findet permanent bei jedem/r Einzelnen statt
- … erfordert Management-Commitment
- … erfordert Verankerung in Organisationskultur

Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

Danke für Ihre Aufmerksamkeit!

Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert