

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



Cyber Security Center

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





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



(Cyber) Angriffe auf Unternehmen der KI





CEO-Fraud

Von: [REDACTED] Gesendet: [REDACTED]
An: [REDACTED]
Cc: [REDACTED]
Betreff: Vertraulich

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]
[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 ...



Ransomware



Oops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will double. Also, if you don't pay in 7 days, you won't be able to recover your files. We will have free events for users who are so poor that they couldn't pay.

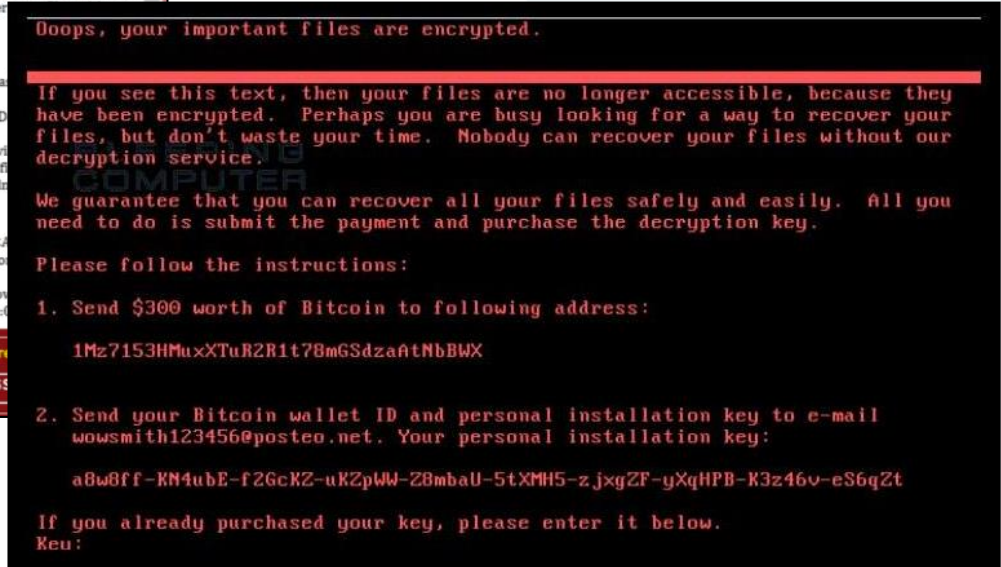
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <How to buy bitcoins>. Please check the current price of Bitcoin and buy some bitcoins. After your payment, click <Check Payment>. Best time to check: 9:00 AM - 5:00 PM (UTC+1).

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6S...

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

About bitcoin
How to buy bitcoins?



Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

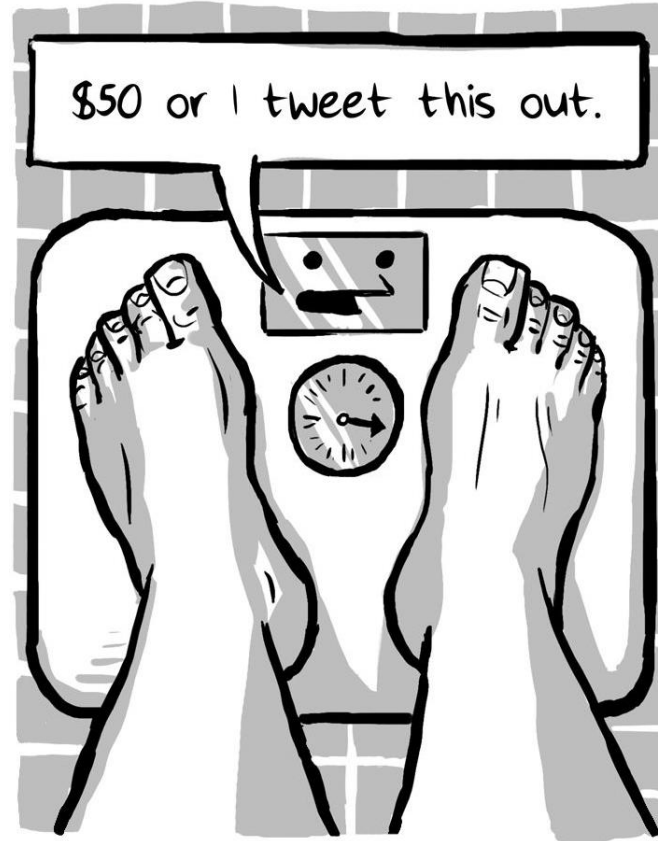
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

- Send \$300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t7BmGSdzaAtNbBWX
- Send your Bitcoin wallet ID and personal installation key to e-mail
wowsmith123456@posteo.net. Your personal installation key:
a8w8ff-KN4ubE-f2GcKZ-uKZpWW-Z8mbaU-5tXMH5-zjxgZF-yXqHPB-K3z46v-eS6qZt

If you already purchased your key, please enter it below.
Key:

Auch Ransomware...



TLP: WHITE

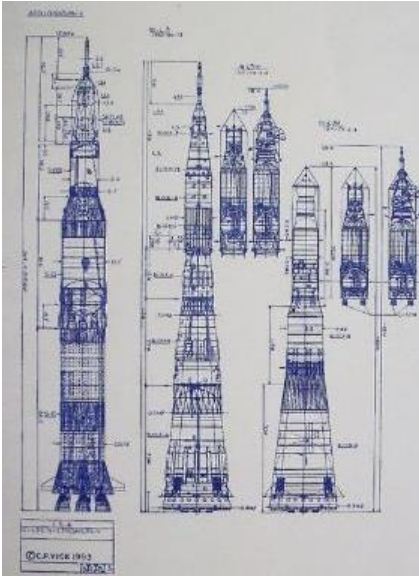




Was tun? Wie schützen? Alles verloren?



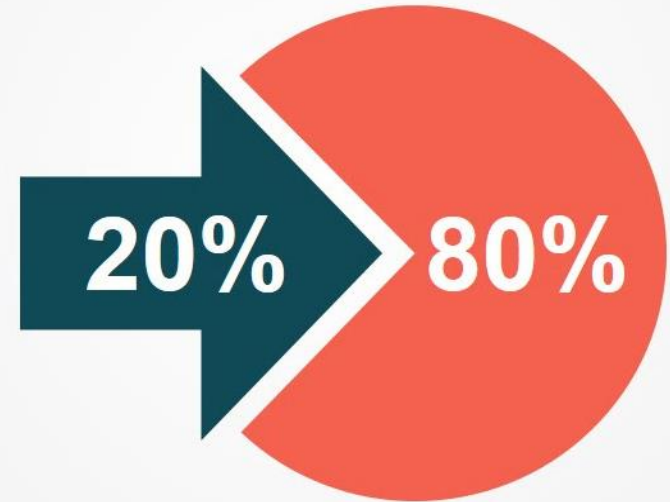
Rocket Science



"Floriani"- Prinzip

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

"Pareto"- Prinzip





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





...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**



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



Danke für Ihre Aufmerksamkeit!