FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Datensicherheit im Anlagenmanagement

Dr. Klaus Gebeshuber
10.Oktober 2019

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

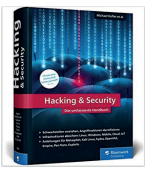
About me

- Study of Electronic Engineering / Computer Science
- Industrial Software Development / Warehouse Logistics

- Lectures @FH JOANNEUM
  - Network Technologies
  - IT-Security
  - Ethical Hacking
  - Network Security

- Research Activities
  - Industrial Penetration Testing
  - Wireless Security
  - 0day hunting

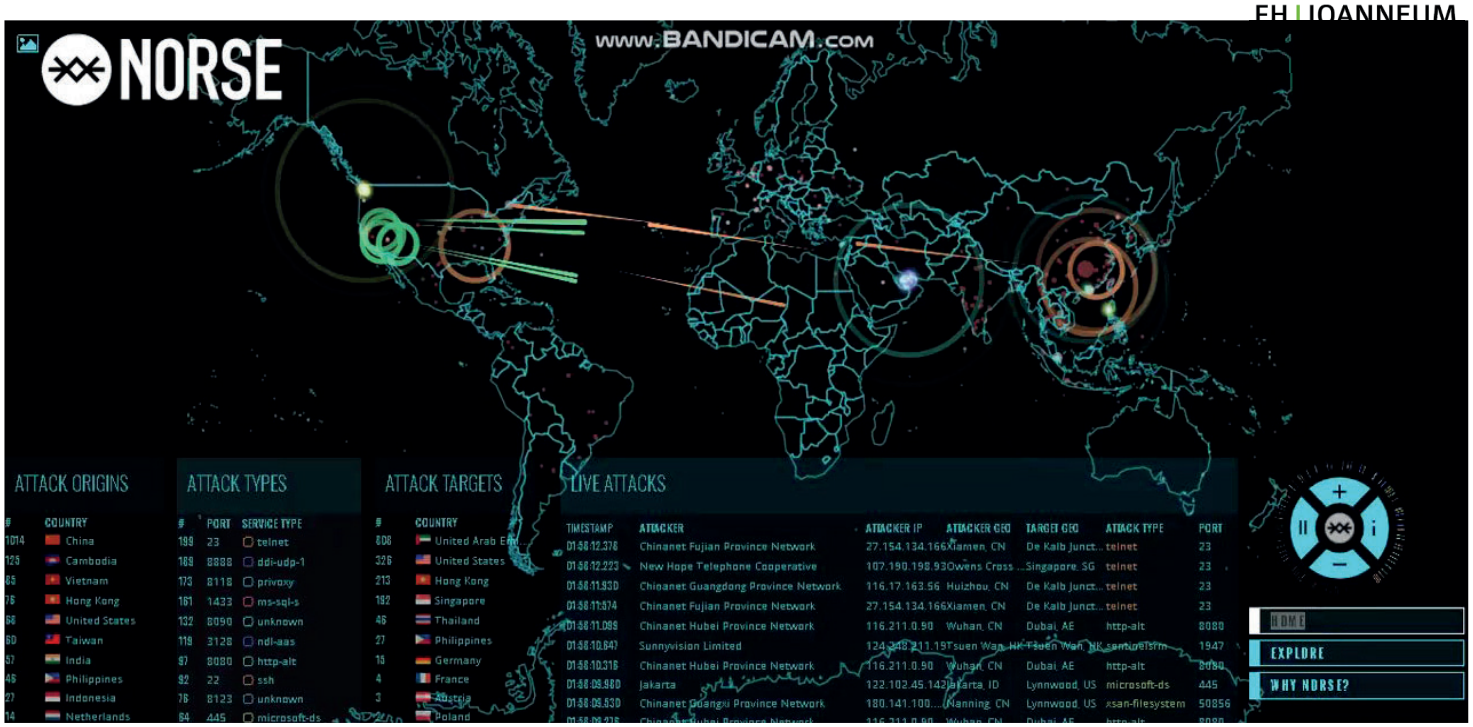
- Industrial Certifications
  - OSCP, OSCE, CISSP, OSWP, CCNA, eCPPT, CSM, eMAPT



AGENDA

https://pixabay.com/

- Bedrohungslage
- Angriffsszenarien
- Erfahrungen aus Projekten
- Schutzmaßnahmen
  Empfehlungen



https://www.youtube.com/watch?v=dDWxp9kJ4G8

Bedrohungen - Who are the enemies?

- Script Kiddies
- Hacktivisten
- Mitarbeiter
- Ehemalige Mitarbeiter
- Regierungen / Geheimdienste
- Mitbewerb
- Organisierte Kriminalität

Ransomware

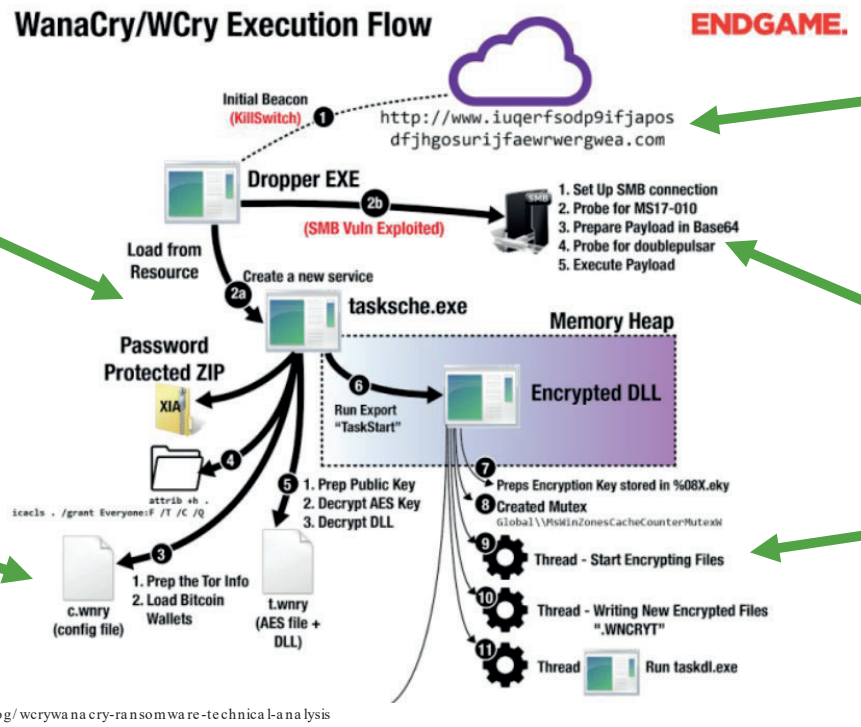
- Virus infiziert Computer
- Virus verschlüsselt die Festplatte(n)
- Bezahlung von Lösegeld für die Entschlüsselung

- Kryptographisch sichere Verfahren – RSA, AES
- Teilweise Implementierungsfehler

Druck

Erklärung

Zahlung



Kill Switch

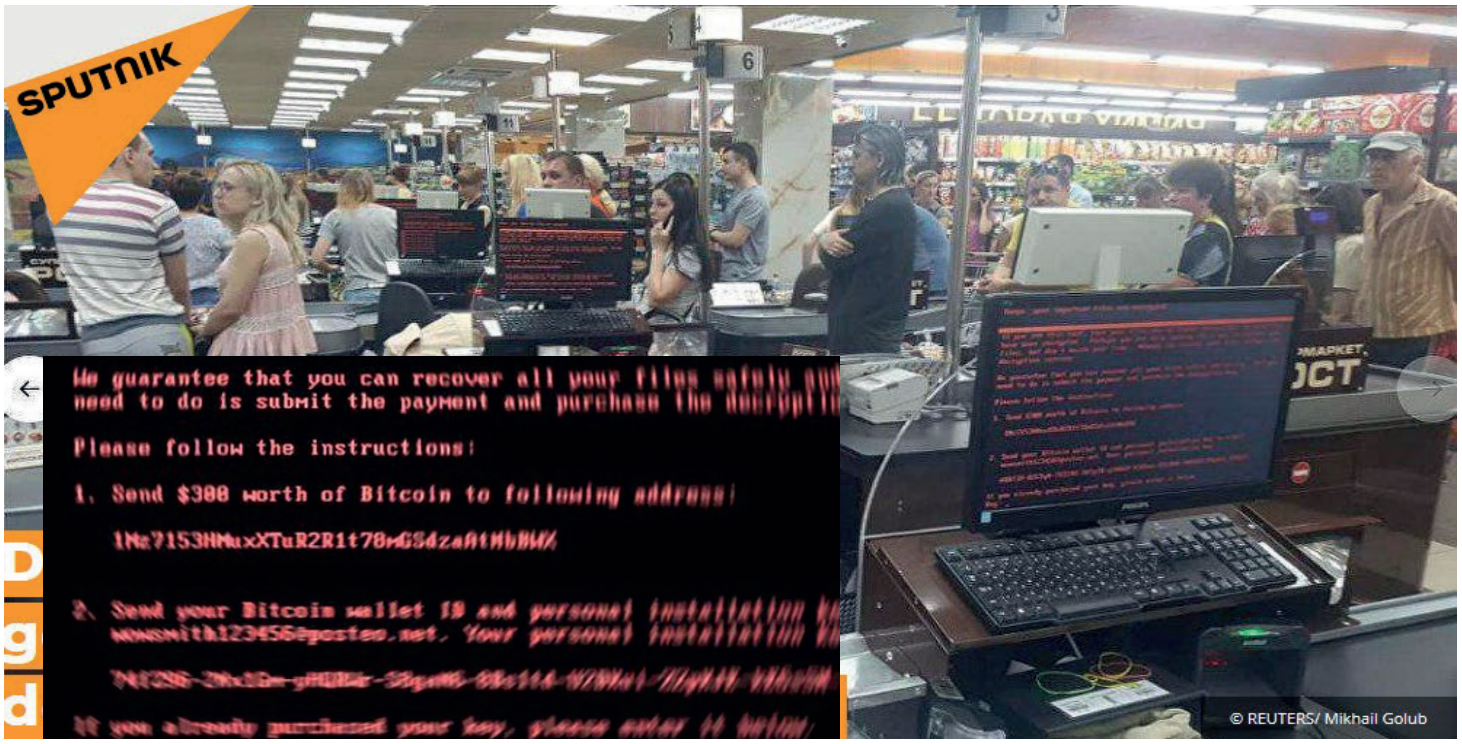
Zugang

Verbreitung

Zahlung

Ransomware
Funktionalität

https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis



https://de.sputniknews.com/panorama/20170628316360307-warum-das-neue-virus-gefaehrlicher-als-seine-vorgaenger-ist/
https://www.heise.de/security/meldung/Petya-Attacke-oder-NotPetya-Erstes-Angriffsziel-offenbar-in-der-Ukraine-3757496.html

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Norsk Hydro ransomware incident losses reach $40 million after one week

Hydro became victim of an extensive cyber-attack in the early hours of Tuesday (CET), impacting operations in several of the company's business areas.

IT-systems in most business areas are impacted and Hydro is switching to manual operations as far as possible. Hydro is working to contain and neutralize the attack, but does not yet know the full extent of the situation.

Investor contact
Stian Hasle
+47 97736022
Stian.Hasle@hydro.com

Press contact
Halvor Molland
+47 92979797
Halvor.Molland@hydro.com

Follow us on Facebook:
facebook.com/norskhydroasa

Alun anual
oper tion

UPDATE: Cy

By Catalin

Norsk hand
and v

Microsoft em k.

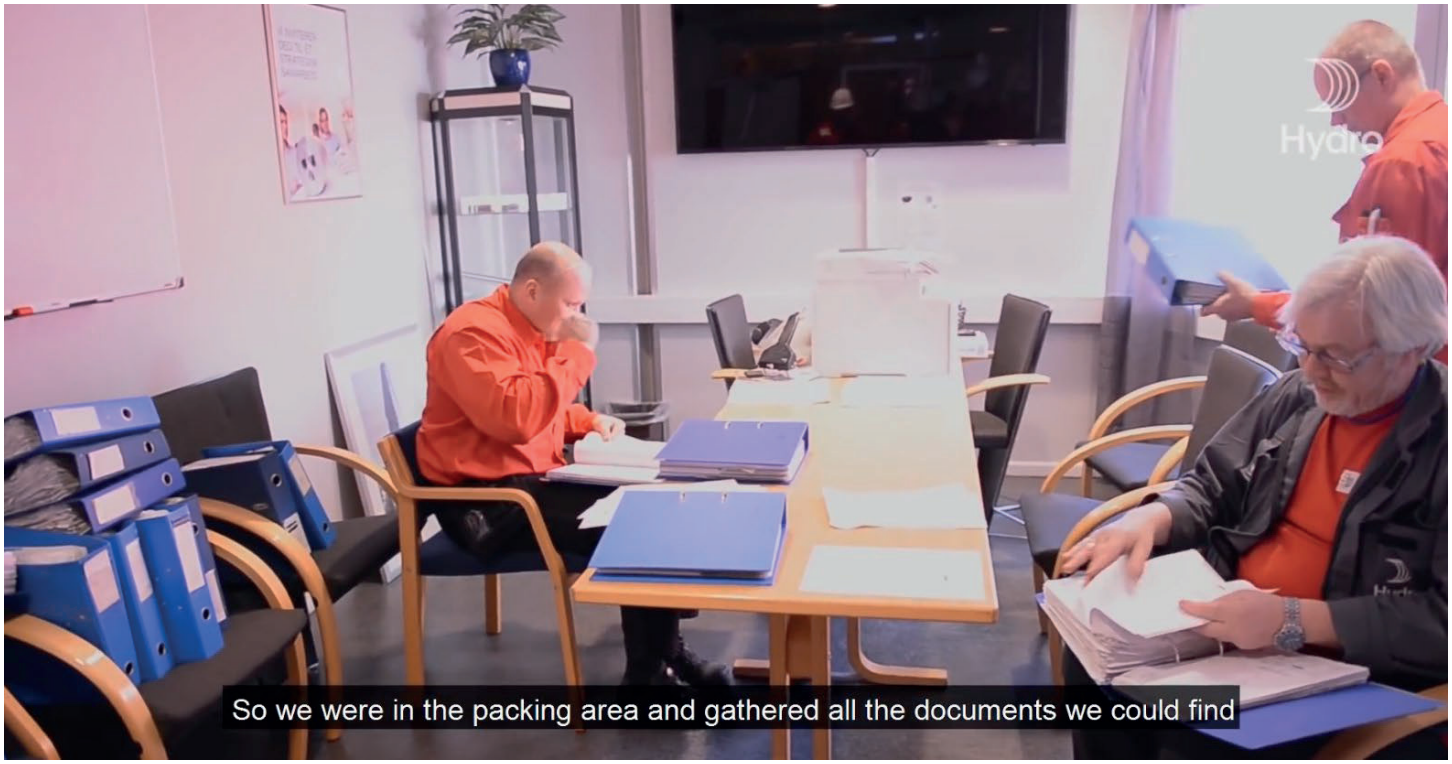
By Catalin Ci

README_LOCKED - Notepad

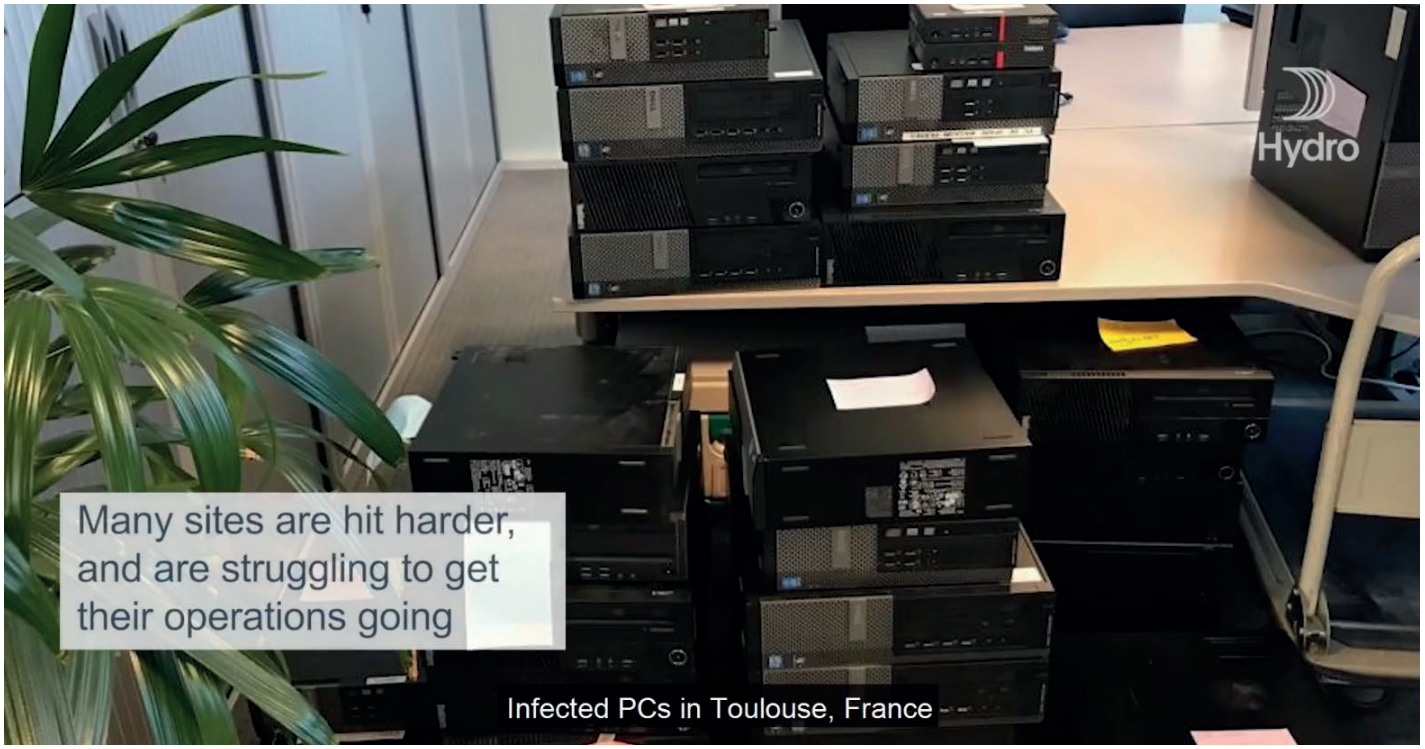
File Edit Format View Help

```
Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts every
Sample files we unlock for free (files should not be related to any kind of backups).

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and
instructions on how to improve your systems security

To get information on the price of the decoder contact us at:

DharmaParrack@protonmail.com
wyattpettigrew8922555@mail.com
```

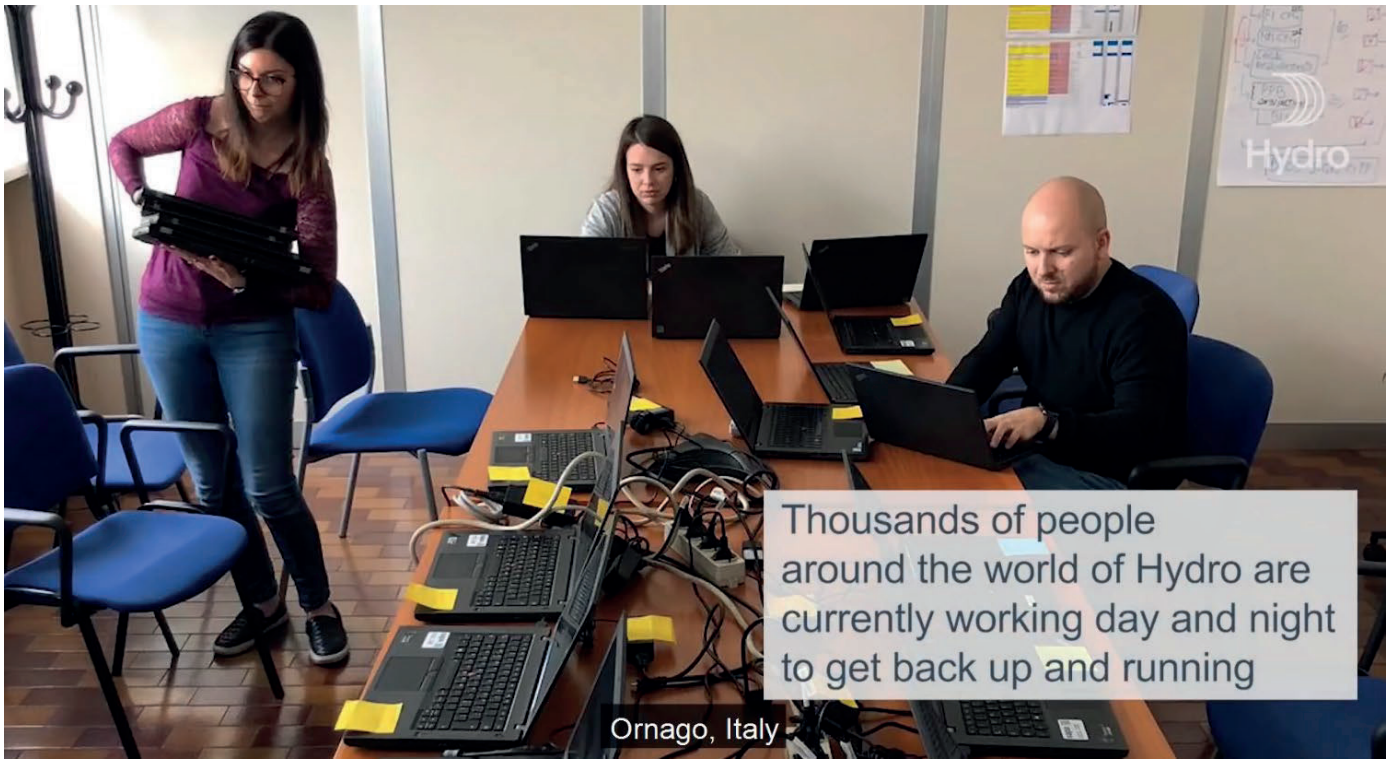
FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security



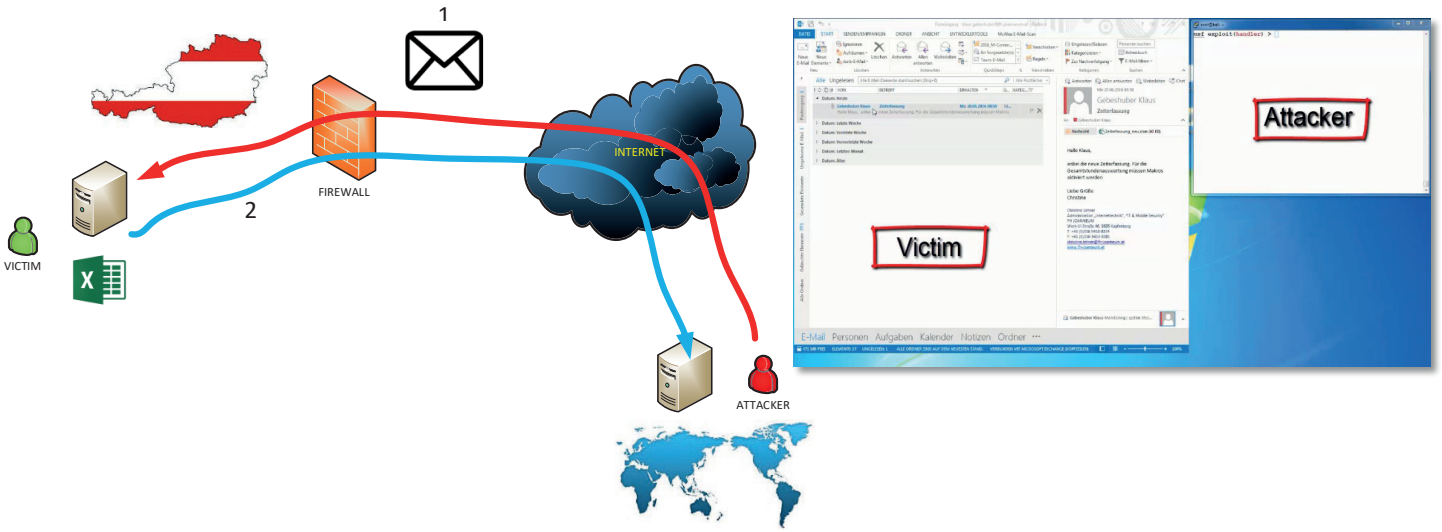
FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security



FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security



Initialer Zugriff



Phishing

» Phishing
  » Daten u…iten

» Spear Ph…
  » Gezielte…

Lieber Herr, Frau Paketempfänger,

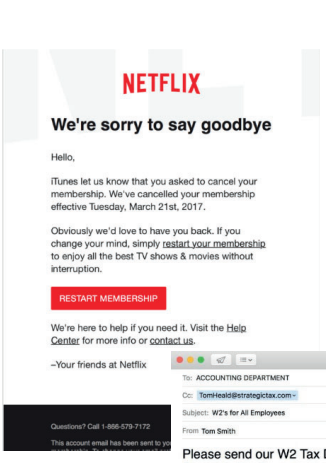
leider haben wir uns verpasst, Ihr/e Paket/e mit dem Auftragsnummer 0978168123 wird/werden zum nächstmöglichen Termin erneut versendet.

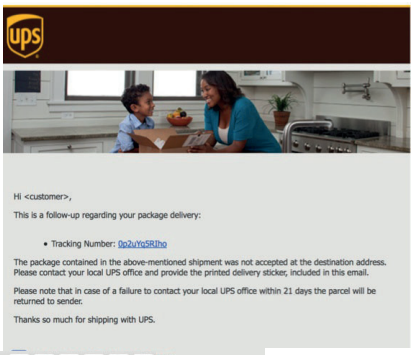
Bitte wählen sie unter **www.dpd-versandinfo.com** einen für Sie möglichen Termin aus.

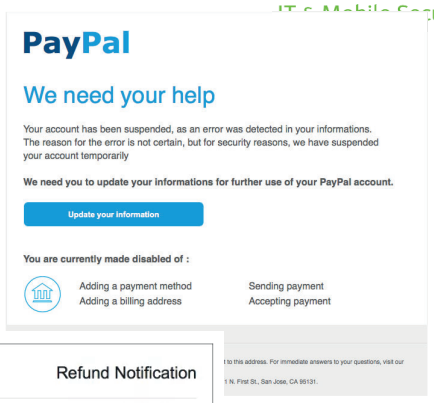
Lieber Grüße,

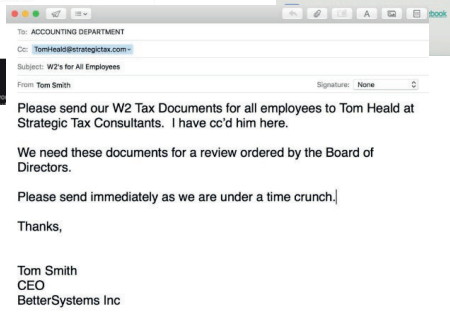
Ihr DPD Team

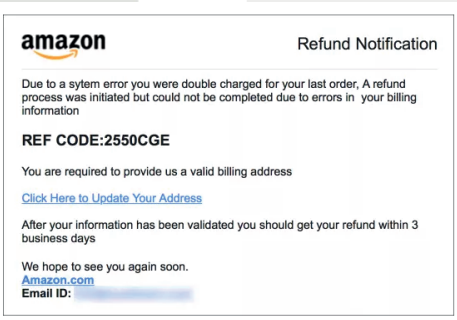
FH | JOANNEUM
University of Applied Sciences









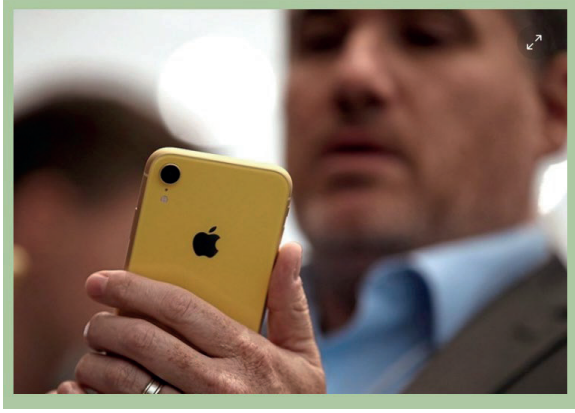


https://www.edts.com/edts-blog/15-examples-of-phishing-emails-from-2016-2017

Mysteriöser iOS-Hack: Websites infizierten jahrelang iPhones

Der größte iPhone-Hack aller Zeiten erlaubt eine gänzliche Kontrollübernahme. Die unbekannten, wahrscheinlich staatsnahen Täter nutzten 14 verschiedene Sicherheitslücken

31. August 2019, 00:21 259 Postings

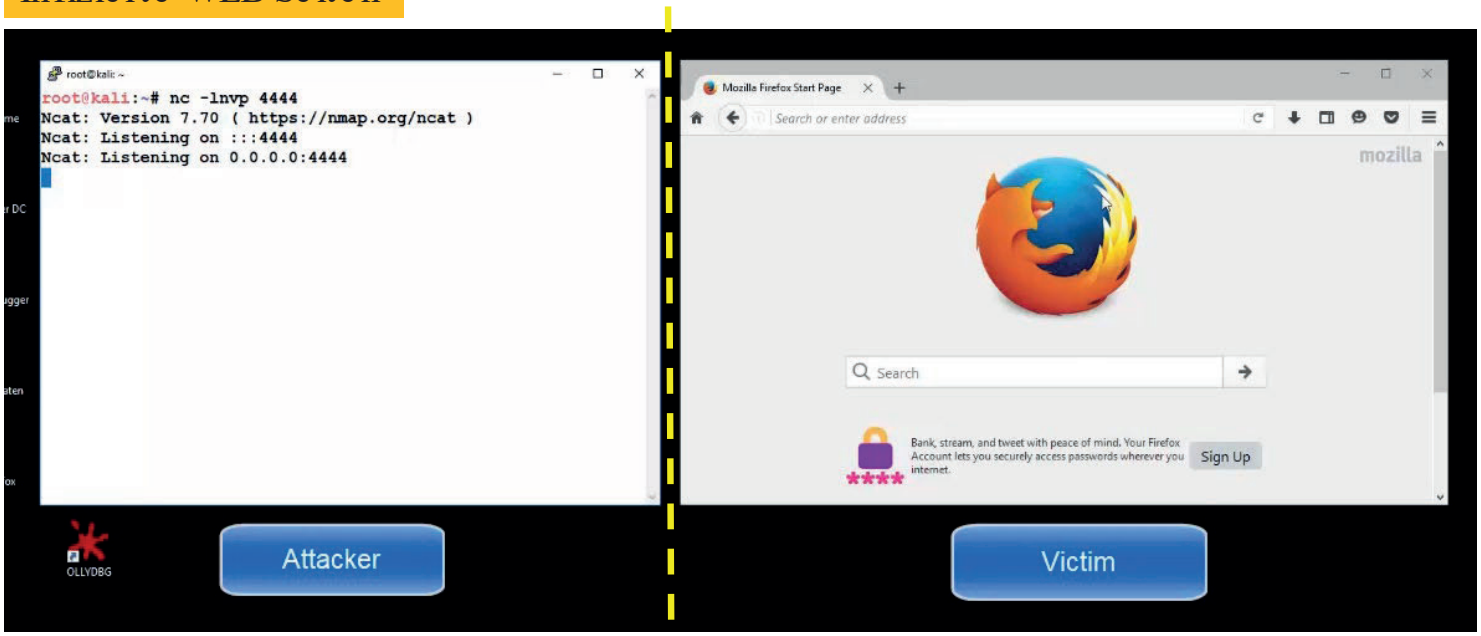


Angriffe auf iPhones laut Experten stümperhaft umgesetzt

Der IT-Sicherheitsexperte Jake Williams von der Firma Rendition Infosec vermutete im Magazin Wired, dass hinter den Attacken relativ unerfahrene Programmierer einer Regierungsbehörde stecken könnten, die Informationen über Schwachstellen von einem darauf spezialisierten Anbieter bekommen hätten. Dass die Attacken trotz der eher stümperhaften Umsetzung so lange unentdeckt geblieben seien, könne darauf hinweisen, dass sie sich innerhalb eines einzelnen Landes abspielten, mutmaßte Williams.

https://www.derstandard.at/story/2000108046751/mysterioeser-ios-hack-websites-infizierten-jahrelang-iphones https://t3n.de/news/google-experten-hacker-konnten-1193426/

Infizierte WEB Seiten



Dangerous Links

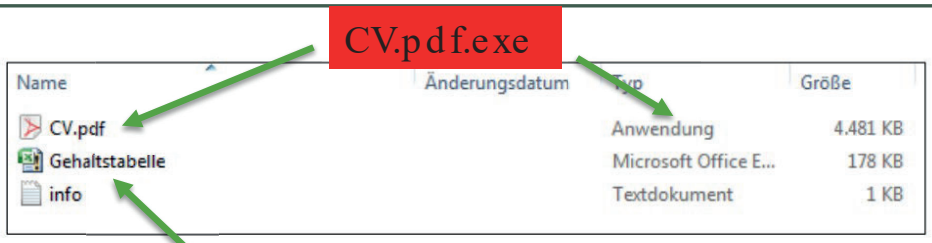
(c) klaus.gebeshuber@fh-joanneum.at

USB Devices

» Günstige Geräte
» Können Schadprogramme beinhalten

» Vor dem Gebäude abgelegt
» Am Parkplatz ausgestreut
» In der Toilette verloren
» Als Geschenk versendet
» …

USB devices

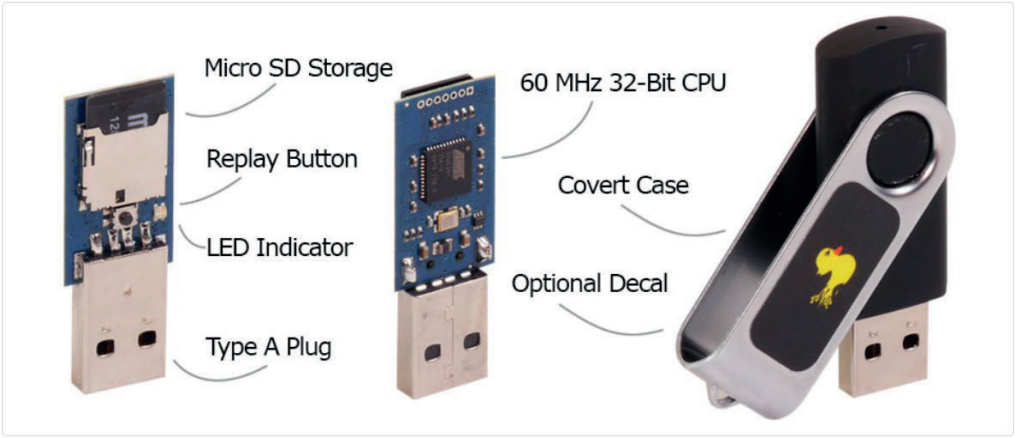


Excel with Macros

Beispiele:
- Ausführbarer Code
- Fileformat Exploits
- BadUSB

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

USB devices



» Spezielles USB Gerät
» Arbeitet als Tastatur
» Kann tippen
» Günstiges Gerät

USB Stick dropping

Getarnte Netzwerk Geräte

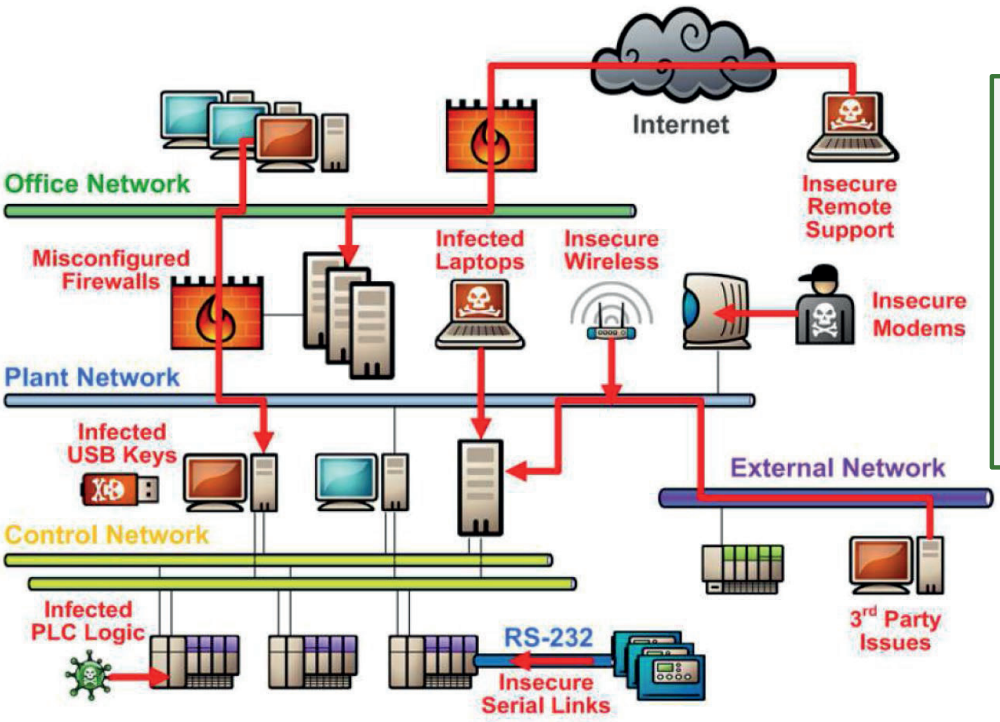
PwnPlug –Network Attack Device

- Eine Minute Zugang zu einem Raum reicht aus
- Mit Batterie betrieben
- “Calling home” Geräte

Tests in der Industrie

- Ethical Hacking
  - Vulnerability Assessment
  - Penetration Test
  - Red Team Assessment

- Tests um den Sicherheitsstatus festzustellen
- In der IT bereits etabliert
- In der OT nur eingeschränkt möglich



- Alte Systeme XP, 2000
- Keine Segmentierung
- Weg ins Internet frei
- Lokale Admin Rechte
- Passwörter
- Physischer Schutz fehlt
- Angriffe nicht erkannt
- IT/OT Kommunikation

https://www.tofinosecurity.com/sites/default/files/common/white -papers/Using -ISA_IEC62443 -Standards -WP-v1.2%20(May%20201

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Schutzmaßnahmen (1)

- Patch Management (Software Updates)
- Aktueller Virenschutz
- Passwort Policy
- Datensicherung, Aufbewahrung von Sicherungsdaten
- Datenverschlüsselung + Schlüssel Handling
- Firewall + Regelwerk, WAF (Web Application Firewall)
- Einsatz von IDS (Intrusion Detection) und IPS (Intrusion Prevention) Systemen
- Einsatz von Honeypots / Honeynets

Schutzmaßnahmen (2)

- Gute Ausbildung der Mitarbeiter
- Trainings in realer Umgebung, Security Lab, Cyber Range
- Gemeinsame Trainings mit IT/OT
- Regelmäßige Sicherheitsüberprüfungen
- Gesundes Misstrauen, Awareness

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Vielen Dank!

klaus.gebeshuber@fh-joanneum.at