DIHSÜD

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

DIH Süd - IT-Security Infoveranstaltung
Spannendes aus der Welt der IT-Security

30.11.2021

Dr. Klaus Gebeshuber
klaus.gebeshuber@fh-joanneum.at

DIHSÜD

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Fachvorträge:

Verbrecherjagd mit Zahlen Joachim Schauer – FH JOANNEUM

Ein Cyber Vorfall legt uns lahm – Lessons Learned Martin Strommer – Pilz GmbH

Gängige Schwachstellen in Unternehmensnetzwerken Klaus Gebeshuber – FH JOANNEUM

Digital Innovation Hub Süd – Geplante Aktivitäten Klaus Gebeshuber – FH JOANNEUM

DIHSÜD

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Gängige Schwachstellen in Unternehmensnetzwerken

Netzwerk Zugriff (1)

- Physischer Zugang ohne Einschränkungen
  - IP-Adresse via DHCP
  - Kein 802.1X
  - Direkter Zugang ins Internet
- Gäste WLAN
  - Verbindung zum internen Netz
  - Kein Passwort
  - Klartext, kein WPA
- Internet Zugang beschränkt
  - Blockiert – via HTTP Proxy
  - Ping erlaubt - Tunnel über ICMP
  - DNS Requests erlaubt – Tunnel über DNS

Passwörter (1)

- Standard Passwörter
  - admin, root, 1234, 0000, pass0rd, vnc, <leer>
- Default Passwörter
  - https://github.com/danielmiessler/SecLists
- Schwache Passwörter
  - Sommer2021
  - Winter2021
  - dieter
  - **1** (Administrator!)
- Data Breaches
  - https://haveibeenpwned.com/

Vendor	Username	Password
2Wire, Inc.	http	<BLANK>
360 Systems	factory	factory
3COM	3comcso	RIP000
3COM	<BLANK>	12345
3COM	<BLANK>	1234admin

Passwörter (2)

- Active Directory
  - Zugriff ohne Domain Account möglich
  - Passwort im Kommentar Feld
- Password Spraying
  - Winter2021!
  - Initial Passwort (welcome, ChangeMe,...)
- Hersteller (Backdoor Account)
  - Download Config File via FTP – root PW im Klartext
  - Download Firmware Image – Crack Password Hash

Password Spraying Attack

Author: Rishu Ranjan

Description

Password spraying is a type of brute force attack. In this attack, an attacker will brute force logins based on list of usernames with default passwords on the application. For example, an attacker will use one password (say, Secure@123) against many different accounts on the application to avoid account lockouts that would normally occur when brute forcing a single account with many passwords.

This attack can be found commonly where the application or admin sets a default password for the new users.

https://owasp.org/www-community/attacks/Password_Spraying_Attack

Passwörter (3)

- NBNS, LLMNR
  - Fehlende Namensauflösung via DNS
  - Alte Systemnamen
  - wpad
  - Password Hashes von Domain Benutzer
  - 20-30% Knackbar innerhalb von 2 Tagen
- IPv6 DNS, DHCP
  - IPv6 parallel zu IPv4 aktiv
  - Info Rogue DNS Server verteilen
  - IPv6 wird bevorzugt
- IPMI – Protokoll Schwachstelle
  - Passwort Hash auslesen
  - Passwort Cracking
  - Default Passwort – 8 Stellen Alphanumerisch

Privilege escalation, lateral movement

- Lokale Adminrechte von Domain Benutzer
  - Zugriff auf lokale SAM DB
  - Lokalen Administrator Hash auslesen

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:edfc4c90d11bc45fae0aa785e3f27d55:::
```

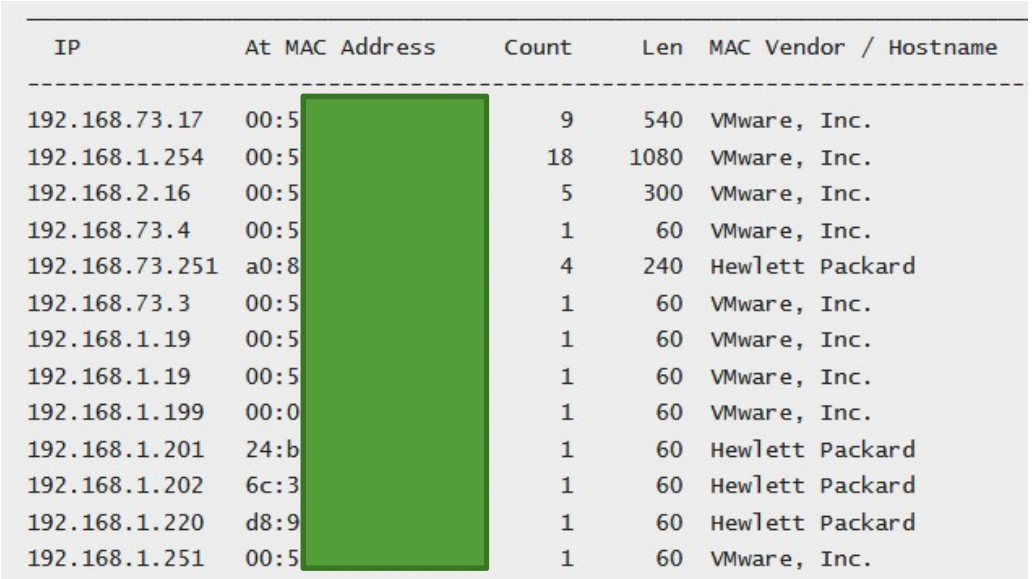
  - Password Crack
  - Password Rainbow Table

- Lokaler Admin Account
  - Passwort ident auf vielen Systemen
  - Pass the hash

https://crackstation.net/

Netzwerk Zugriff (2)

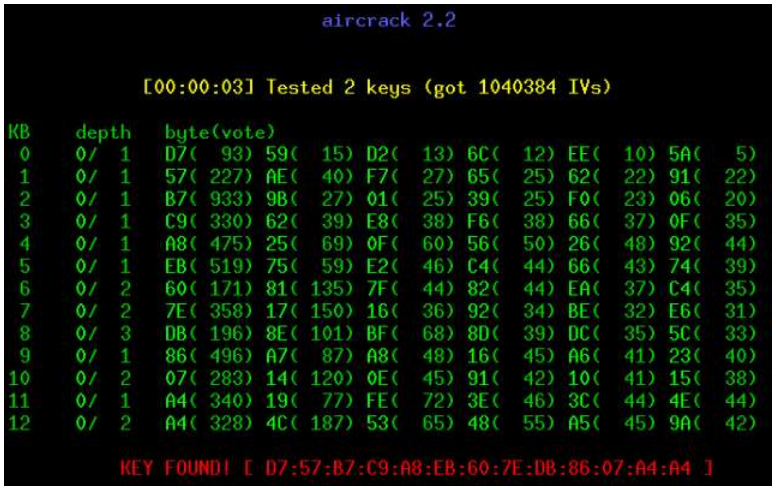
- Unbekannte Geräte
  - Falsche/Standard IP Konfiguration
  - Layer 2 – Netzwerkscan
- Dual Homed
  - Geräte mit zwei Netzwerk-Karten
  - Firewall Bypass
- Design Fehler – VLAN?
  - Layer 2 vs. Layer 3 Trennung



IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.73.17	00:5	9	540	VMware, Inc.
192.168.1.254	00:5	18	1080	VMware, Inc.
192.168.2.16	00:5	5	300	VMware, Inc.
192.168.73.4	00:5	1	60	VMware, Inc.
192.168.73.251	a0:8	4	240	Hewlett Packard
192.168.73.3	00:5	1	60	VMware, Inc.
192.168.1.19	00:5	1	60	VMware, Inc.
192.168.1.19	00:5	1	60	VMware, Inc.
192.168.1.199	00:0	1	60	VMware, Inc.
192.168.1.201	24:b	1	60	Hewlett Packard
192.168.1.202	6c:3	1	60	Hewlett Packard
192.168.1.220	d8:9	1	60	Hewlett Packard
192.168.1.251	00:5	1	60	VMware, Inc.

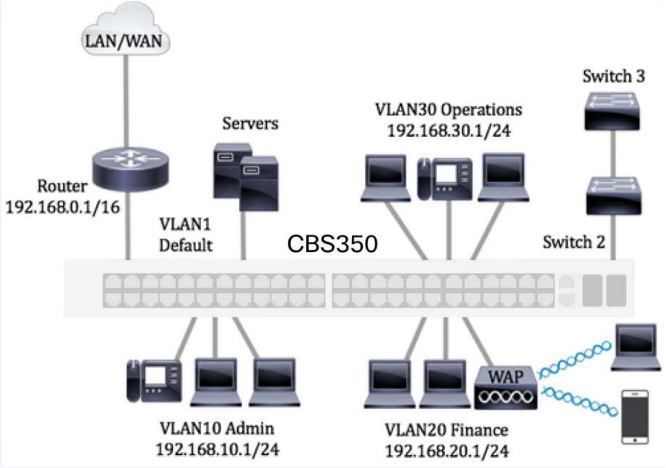
Netzwerk Zugriff (3) - WLAN

- WLAN – WPA-2
  - Numerisches Passwort 8 Stellen
  - Leicht zu knacken
- WLAN – WPA-2 - PSK
  - Ein geheimes Passwort für das Netzwerk
  - Allen Benutzern bekannt
  - Mitarbeiter verlässt das Unternehmen…
- WLAN - WEP
  - Unbekannter Access Point im Schaltschrank
  - Innerhalb von 3 min zu knacken



Cisco Switch– Default Config - DTP

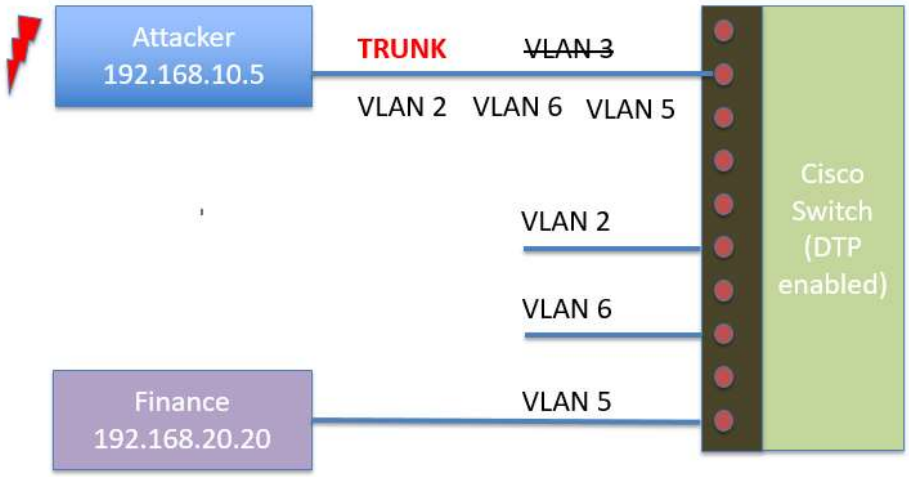
- *Switch/Port Config*
  - *switchport mode access*
  - *switchport access vlan 5*



www.cisco.com

Das **Dynamic Trunking Protocol** (DTP) ist ein proprietäres Netzwerkprotokoll der Firma Cisco Systems.[1] Es dient in lokalen Netzwerken (LANs) dazu, auf Ethernet-Links das VLAN-Trunking (d. h. ob der Link zu einem Trunk oder zu einem Access-Port wird, oder inaktiv bleibt) sowie ggf. die Art der Einkapselung (ISL oder IEEE 802.1q) selbständig zu verhandeln. Dazu versendet das Interface DTP-Frames an die Multicast-MAC-Adresse 01-00-0C-CC-CC-CC, die auch von weiteren proprietären Cisco-Protokollen wie z. B. VTP, PAgP oder UDLD verwendet wird.

de.wikipedia.org



Sensitive Informationen im Netzwerk (1)

- Drucker / Scanner
  - Keine Zugriffsbeschränkung
  - Gescannte, vertrauliche Dokumente
- SMB Shares
  - Schreibbar für alle User
  - Konfigurationsdateien von Cisco Geräten
  - Konfigurationsdateien von Anwendungen

```
security passwords min-length 8
no logging console
enable secret 5 $1$p8Y6$MCdRLBzuGlfOs9S.hXOp0.
!
username hub password 7 02501705B3907344E
username admin privilege 15 password 7 10181A325528130F010D24
username guest password 7 124F163C42340B112F3830
```

https://www.ifm.net.nz/cookbooks/passwordcracker.html

Sensitive Informationen im Netzwerk (2)

» .SVN Directory eines Kunden WEB-Portals aus dem Internet erreichbar

Sensitive Informationen im Netzwerk (2)

- .SVN Directory eines Kunden WEB-Portals aus dem Internet erreichbar
  - Repository der gesamten WEB-Anwendung lesbar

Sensitive Informationen im Netzwerk (2)

- .SVN Directory eines Kunden WEB-Portals aus dem Internet erreichbar
  - Repository der gesamten WEB-Anwendung lesbar
  - Auslesen von Datenbank Zugangsdaten aus einer Konfigurationsdatei

Sensitive Informationen im Netzwerk (2)

- .SVN Directory eines Kunden WEB-Portals aus dem Internet erreichbar
  - Repository der gesamten WEB-Anwendung lesbar
  - Auslesen von Datenbank Zugangsdaten aus einer Konfigurationsdatei
  - Zugriff auf die Datenbank via phpmyadmin

Sensitive Informationen im Netzwerk (2)

- .SVN Directory eines Kunden WEB-Portals aus dem Internet erreichbar
  - Repository der gesamten WEB-Anwendung lesbar
  - Auslesen von Datenbank Zugangsdaten aus einer Konfigurationsdatei
  - Zugriff auf die Datenbank via phpmyadmin
  - Auslesen von Benutzer Hashes aus der Datenbank

Sensitive Informationen im Netzwerk (2)

- .SVN Directory eines Kunden WEB-Portals aus dem Internet erreichbar
  - Repository der gesamten WEB-Anwendung lesbar
  - Auslesen von Datenbank Zugangsdaten aus einer Konfigurationsdatei
  - Zugriff auf die Datenbank via phpmyadmin
  - Auslesen von Benutzer Hashes aus der Datenbank
  - Passwort Crack der Hashes (md5)

Sensitive Informationen im Netzwerk (2)

- .SVN Directory eines Kunden WEB-Portals aus dem Internet erreichbar
  - Repository der gesamten WEB-Anwendung lesbar
  - Auslesen von Datenbank Zugangsdaten aus einer Konfigurationsdatei
  - Zugriff auf die Datenbank via phpmyadmin
  - Auslesen von Benutzer Hashes aus der Datenbank
  - Passwort Crack der Hashes (md5)
  - ~1000 Passwörter im Klartext ermittelt

Sensitive Informationen im Netzwerk (2)

- .SVN Directory eines Kunden WEB-Portals aus dem Internet erreichbar
  - Repository der gesamten WEB-Anwendung lesbar
  - Auslesen von Datenbank Zugangsdaten aus einer Konfigurationsdatei
  - Zugriff auf die Datenbank via phpmyadmin
  - Auslesen von Benutzer Hashes aus der Datenbank
  - Passwort Crack der Hashes (md5)
  - ~1000 Passwörter im Klartext ermittelt
  - Passwörter von Kunden und Mitarbeitern

Sensitive Informationen im Netzwerk (2)

- .SVN Directory eines Kunden WEB-Portals aus dem Internet erreichbar
  - Repository der gesamten WEB-Anwendung lesbar
  - Auslesen von Datenbank Zugangsdaten aus einer Konfigurationsdatei
  - Zugriff auf die Datenbank via phpmyadmin
  - Auslesen von Benutzer Hashes aus der Datenbank
  - Passwort Crack der Hashes (md5)
  - ~1000 Passwörter im Klartext ermittelt
  - Passwörter von Kunden und Mitarbeitern
  - Test der Mitarbeiter Passwörter am Outlook Web Access

Sensitive Informationen im Netzwerk (2)

- .SVN Directory eines Kunden WEB-Portals aus dem Internet erreichbar
  - Repository der gesamten WEB-Anwendung lesbar
  - Auslesen von Datenbank Zugangsdaten aus einer Konfigurationsdatei
  - Zugriff auf die Datenbank via phpmyadmin
  - Auslesen von Benutzer Hashes aus der Datenbank
  - Passwort Crack der Hashes (md5)
  - ~1000 Passwörter im Klartext ermittelt
  - Passwörter von Kunden und Mitarbeitern
  - Test der Mitarbeiter Passwörter am Outlook Web Access
  - 2 Mitarbeiter Passwörter ident mit dem Domänen Passwort

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

DIH-SÜD – Digital Innovation Hub Süd

DIH SÜD - Digital Innovation Hub Süd

Was ist der DIH SÜD?

Der **Digital Innovation Hub Süd** ist ein nicht-wirtschaftlich tätiges Kompetenznetzwerk, das als Koordinations- und Anlaufstelle für Selbstständige und Unternehmen zum Thema Digitalisierung im Raum Süd-Österreich dient.

Unser Ziel ist es Digitalisierung in KMU zu ermöglichen, indem wir:

- Bewusstsein für digitale Herausforderungen und Chancen schaffen
- bestehendes Angebot einfach kommunizieren und zugänglich machen
- Anwender und Anbieter zusammenbringen
- spannende Projekte initiieren
- Wissenstransfer zwischen F&E und Wirtschaft fördern.

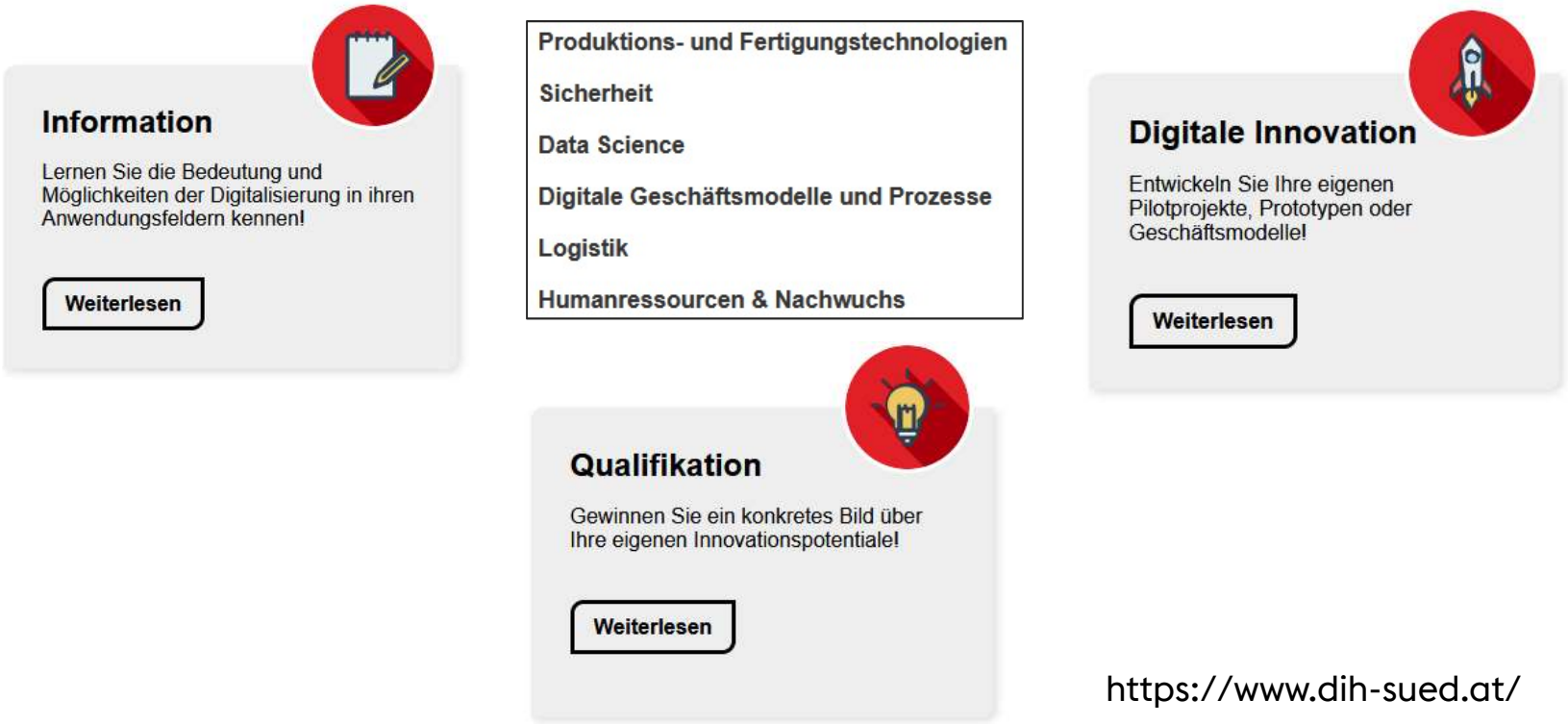
https://www.dih-sued.at/

FFG Forschung wirkt.

Das Land Steiermark

LAND KÄRNTEN

DIH SÜD - Digital Innovation Hub Süd



https://www.dih-sued.at/

DIH SÜD

- Angebot der FH JOANNEUM/IIT
  - Security Infoveranstaltungen
  - IT-SEC Talks für KMU
    - Security in der Welt der Internet of Things – 15.12.2021
    - Cloud Computing - Security Aspekte- 19.01.2022
  - Penetration Testing Trainings (4 tägig) für KMU
    - 14.03.2022 – 29.03.2022

https://www.dih-sued.at/

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Vielen Dank

https://fragebogen.joanneum.at/dihsued_feedback/?q=base&r=AR898718

FH | JOANNEUM
University of Applied Sciences

Verbrecherjagd mit Zahlen

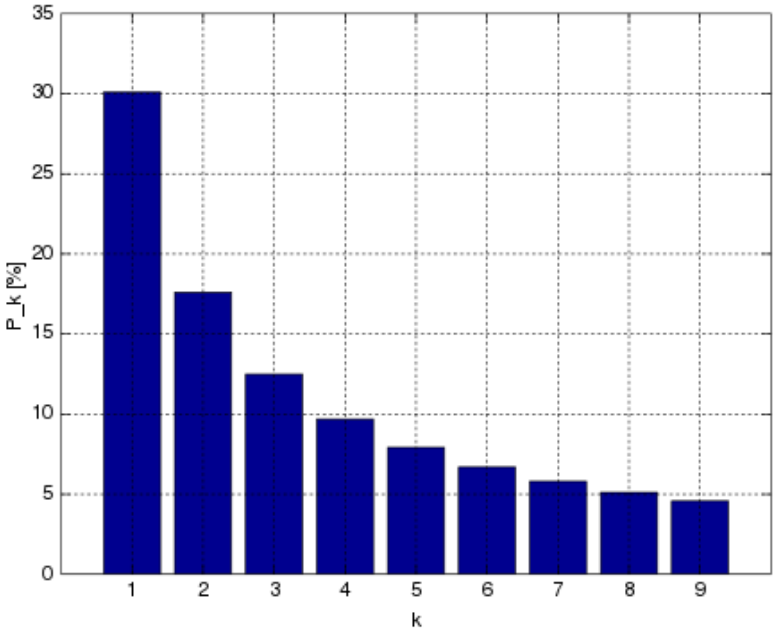
Joachim Schauer
Institut für Internet-Technologien & -Anwendungen
FH-JOANNEUM (Standort Kapfenberg)

Ziel: Erkennen von Manipulationen

- Buchungsdaten im Finanzumfeld
- Ein- und Ausbuchungen von Waren
- Kilometergeldabrechnungen
- Wahldaten? (Meldung von Sprengelergebnissen)

Beobachtung Frank Benford 1938 (und Simon Newcomb 1881)

- In empirischen Datensätzen mit großer Bandbreite sind die führenden Ziffern speziell verteilt:



Voraussetzungen

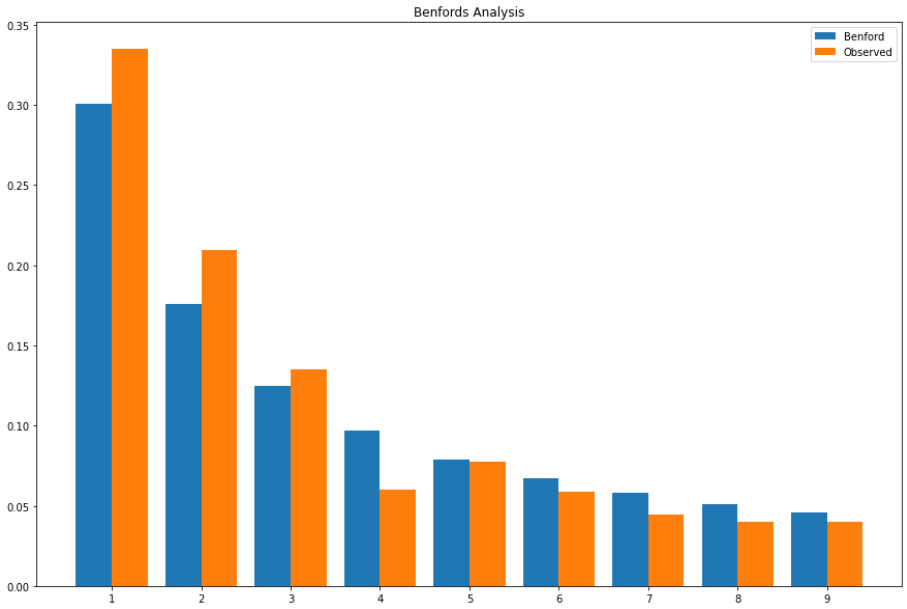
- Datensatz hat ausreichenden Umfang
- Werte erstrecken sich über mehrere Magnituden
- Werte habe einen "multiplikativen Ursprung"
    - Preis x Menge
    - Kilometer x 0.42
    - Einwohner x Infektionsrate

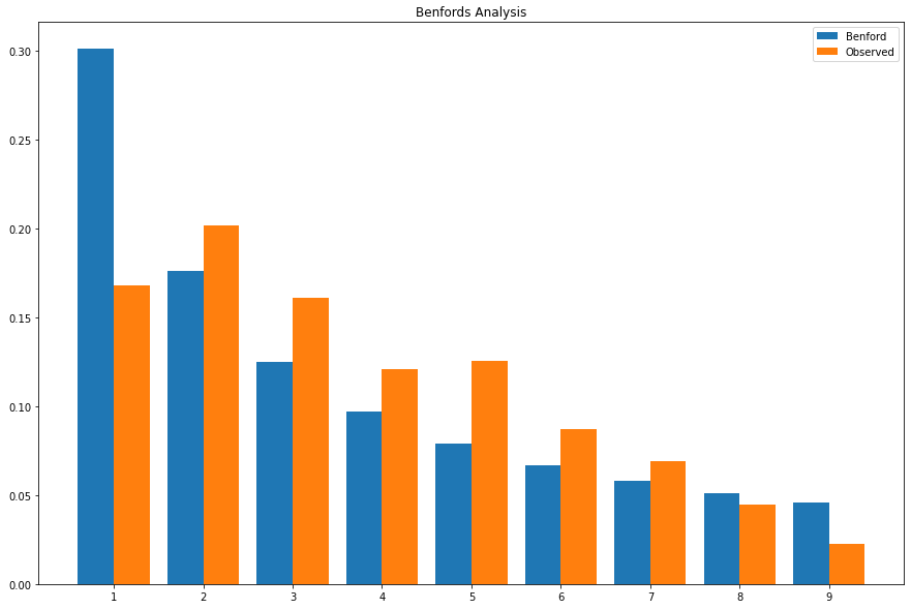
Klassiker: Kilometergeld (tausche 1 mit 7)

Covid Neuinfektionen Österreich vs. Brasilien

- Berachtet werden die Neuinfektionen pro Tag
- Wie schaut der Vergleich zwischen der empirischen Verteilung und Benford aus?
- Welche Schlüsse können wir ziehen?

Österreich (links) vs. Brasilien (rechts)





Konkreter Anwendungsfall

- Int. Getränkehersteller mit diversen Lagern
  - Unterschiedliche Gebindeformen
  - Beschädigte Gebinde werden vernichtet
  - Gebinde sind untereinander schwer vergleichbar (historisches Datenbankdesign...)

Betrugsszenario im Anwendungsfall

Wann ist ein Gebinde beschädigt– wie wird das geprüft?

- **Fakt:** Beschädigte Gebinde werden im System als beschädigt verbucht.
- **Problem:** Ohne großen Datenbereinigungsaufwand waren für eine Analyse nur die jeweilige Anzahl an verbuchten Gebinden pro Typ, pro Person und Zeit verwertbar.

Mögliche Probleme

Betrügerische Buchungen vs. mehrere Magnituden

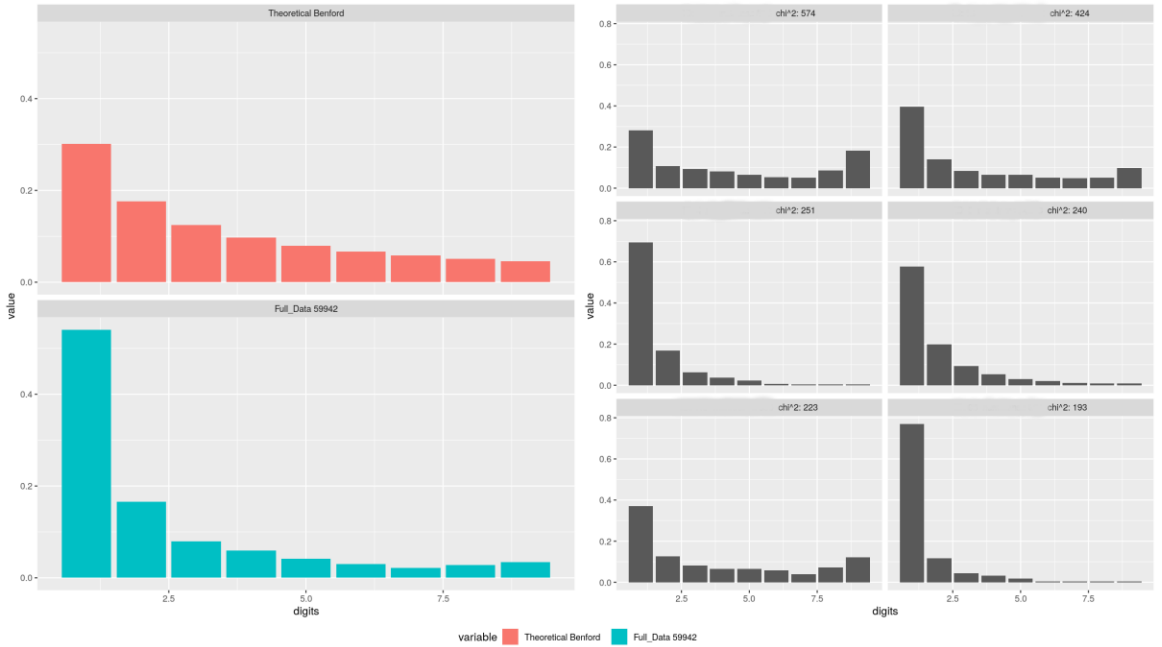
- Datensatz umspannt mehrere Magnituden (1 ~100000)
- Vorteil ist, das unabhängig vom Gebinde, nur mit der Zahl die in der Buchung steht, gearbeitet wurde.

Hauptproblem

Folgt die Ausbuchungs-verteilung Benford?

Nein: In allen Lagern sah die Verteilung sehr ähnlich aus

Eigene statistische Verfahren notwendig!



Ergebnis

Unsere Analyse soll zukünftige Verdachtsfälle aufzeigen.

- Vorteil: Historischer Betrugsfall zum Validieren
  - Unter Top 8 Abweichungen, war der Haupttäter und weitere Komplizen.
  - Aber auch ganz redliche Mitarbeiter.

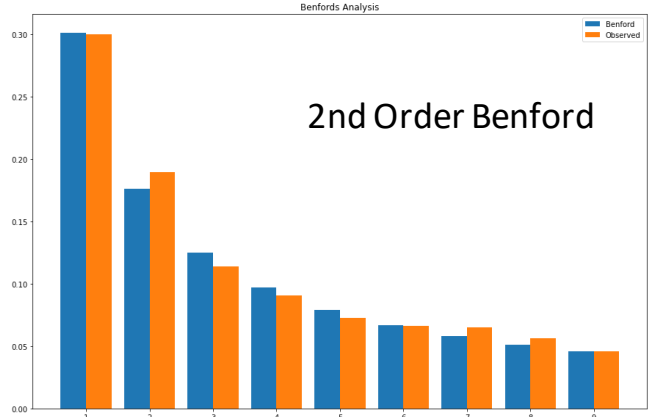
Vorsicht: Benford liefert maximal ein Indiz, nie aber einen Beweis.

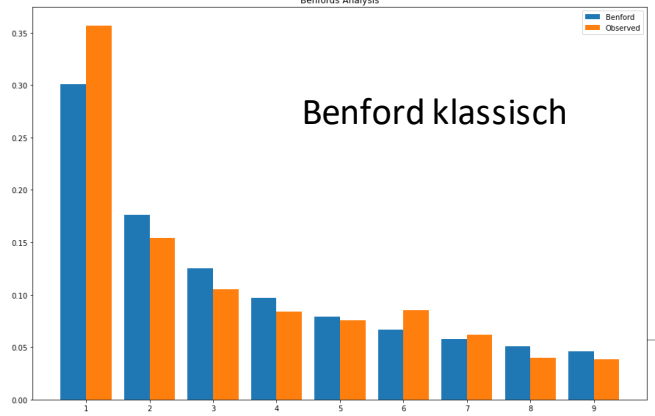
Weitere Verfahren zu Betrugserkennung

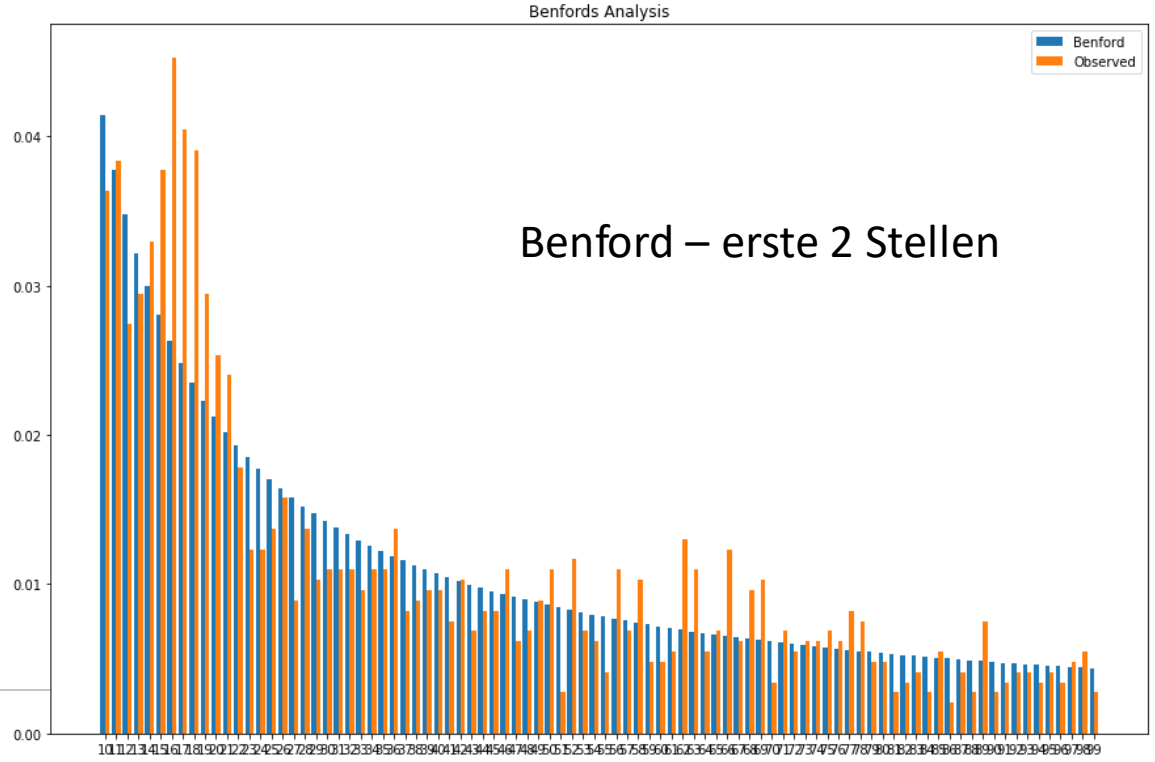
Annahme: Ein Betrüger kennt Benford.

- Ähnliche Verteilungen gelten auch für:
  - Die ersten 2 Stellen
  - 2nd order Test:
    - Reihe die Daten aufsteigend
    - Bilde die Differenzen

Tägliches Transaktionsvolumen Dogecoin USA

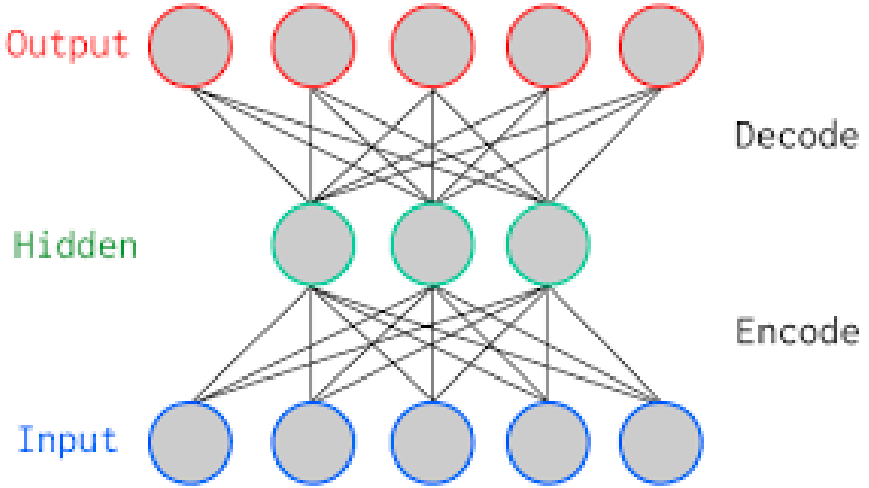






Maschinelles Lernen - Autoencoder

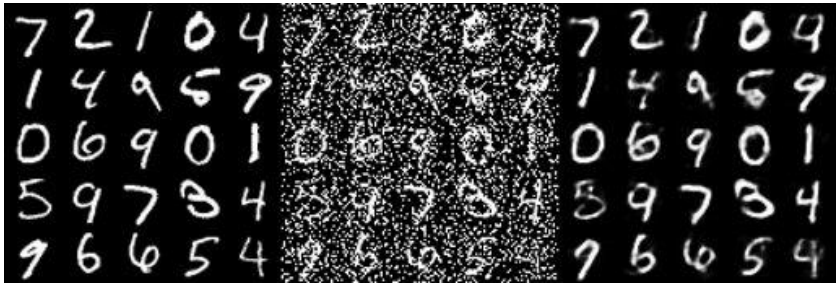
- Input wird auf wenig Information reduziert
- Daraus wird der Input wieder rekonstruiert
- Möglichst ohne Verlust



MuhammadAbuHijleh, CC BY-SA 4.0 , via Wikimedia Commons

Maschinelles Lernen

Ziel: Autoencoder lernt und erkennt die Essenz der Daten.



Färbung von Bildern, Nachschärfen, ...

Maschinelles Lernen

- Klassische Anwendung: Kreditkartenbetrug
- Ausbuchungsdaten haben unterschiedliche Inputdimension
  - Involvierte Personen buchen unterschiedlich häufig
  - Lösung: Ziehe zufällige Samples für die jeweiligen Personen
    - Füttere AE mit je 2000 Buchungen pro Person
    - Bewerte wie gut dieser die Rekonstruktion schafft

Haupttäter und Komplizen fielen durch schlechte Rekonstruktion auf!

Ein Cybervorfall legt uns lahm: Lessons Learned

FH JOANNEUM
University of Applied Sciences

PILZ
THE SPIRIT OF SAFETY

Auf Basis eines Vortrages
von Thomas Pilz – Geschäftsführender Gesellschafter

Ing. Martin Strommer, BSc

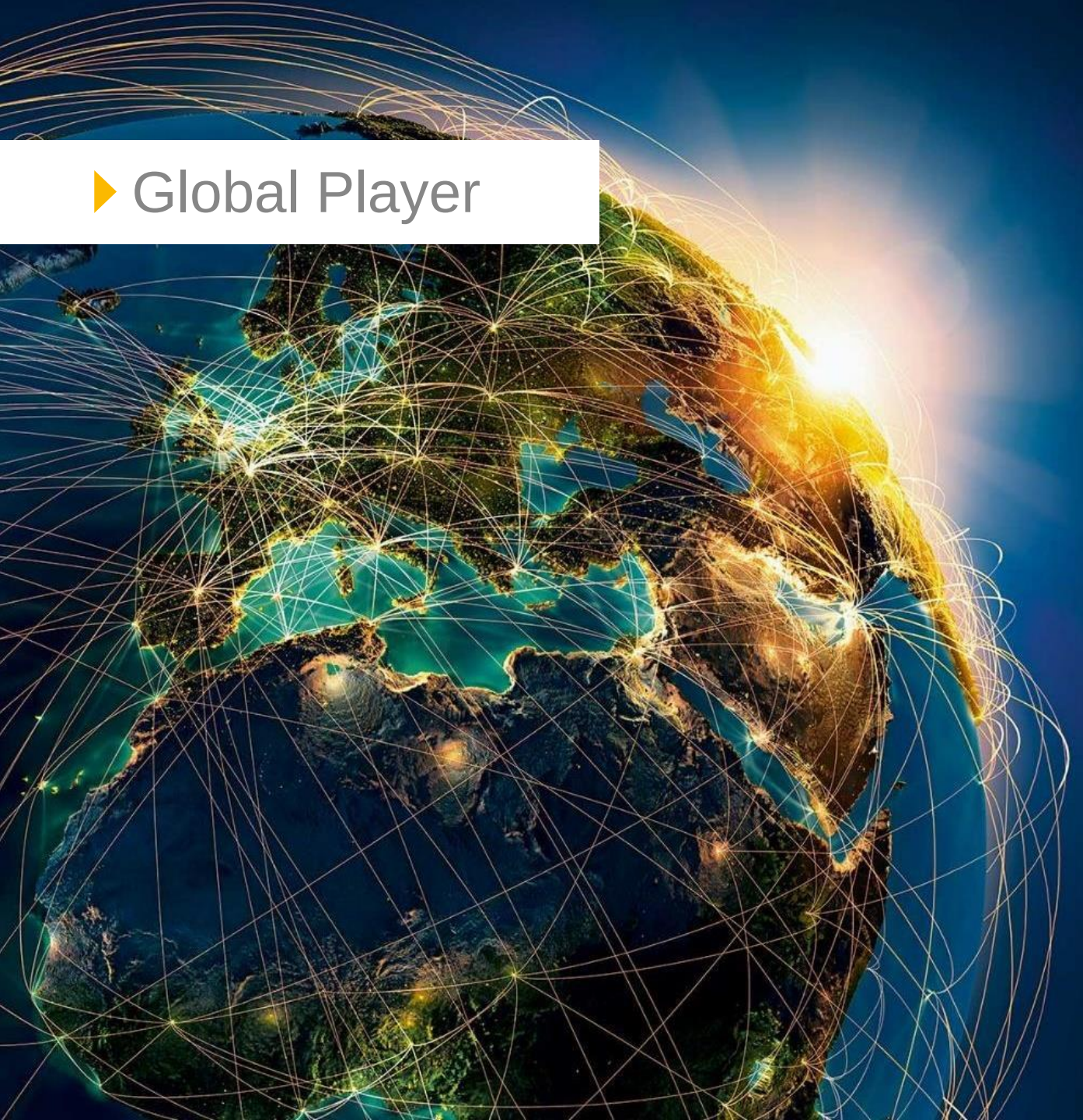
CMSE ®, Certified Machinery Safety Expert (TÜV Nord)

Customer Support / Technical Support
Spezialisierung: Industrie 4.0, Security

- **HTL – Mechatronik**
- **seit 01/2015 Mitarbeiter der Fa. Pilz**
- **2018-2021 Studium „Software Design“, FH Joanneum Kapfenberg - berufsbegleitend**
- **seit 2021 Studium „Information Security“, FH St. Pölten - berufsbegleitend**

E-Mail: m.strommer@pilz.at

Our Mission



Global Player

- **42 Niederlassungen**
- **27 Handelspartner**

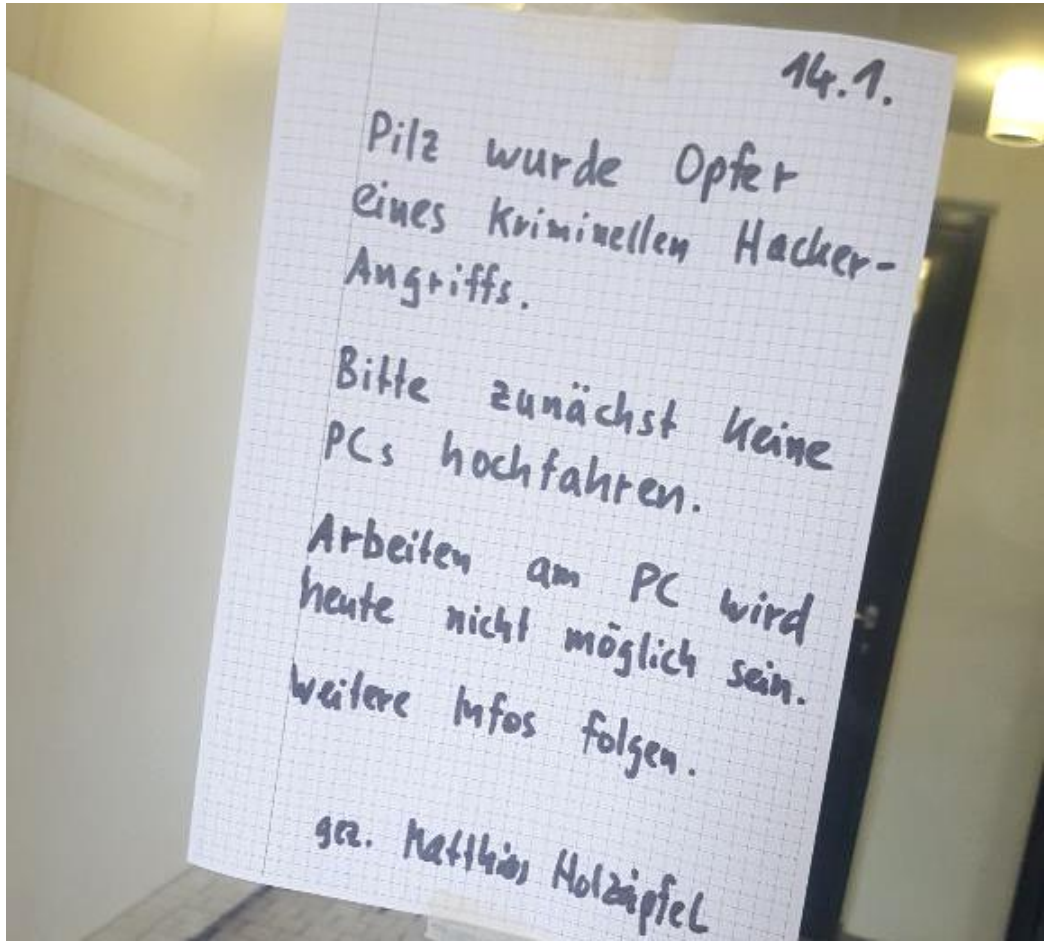
- **Know-how weltweiter und auch lokaler Normen und Gesetze**

- **Schneller on-site support**

Security – Sind wir uns der Problematik bewusst?

- Ende 2016 erste Veranstaltungen in Richtung Security um Awareness zu schaffen.
  - Mäßiger Erfolg weil kaum Interesse vorhanden.
- Onlinebefragung unserer Kunden (Betreiber und Hersteller von Maschinen).
  - Resultat zusammengefasst:
    - Das Thema ist bekannt, aber die innerbetriebliche Verantwortung nicht definiert.
    - Mehr Bewusstsein für IT Security als für OT Security.
    - Keine Vorbereitung auf den Tag X, wenn´s dann mal doch passiert.
      - Stichwort: „Man wird sich noch wundern was alles **NICHT** mehr möglich ist“
    - Mit unseren Learnings aus dem Angriff auf Pilz wollen wir Awareness schaffen und unsere Unterstützung anbieten, damit Ihnen das nicht passiert!

Der Angriff



- Am **Sonntag, 13. Oktober**
  schlugen die Monitoring-Systeme Alarm
- (Cyber-) Kriminelle waren ins Unternehmensnetz eingedrungen
- **Verschlüsselung von Daten**
  auf Rechnern und Servern - weltweit !!!
- Ziel: Erpressung von Lösegeld
  für die Entschlüsselung
- **Es handelt sich um einen sorgfältig geplanten und gezielten Angriff auf Pilz (Bitpaymer)**

Die Tragweite von Bitpaymer

Gehacktes System: Angreifer haben das Netzwerk von Pilz lahmgelegt. (Bild: James Thew/AdobeStock)

- Die **Erstinfektion**: E-Mails mit bösartigen Anhängen oder Links werden blind verschickt, damit Empfänger draufklicken und so Schadsoftware ins Unternehmen hereinlassen.
- Über diese Schadsoftware **spionieren** die Hacker Unternehmen aus und sammeln Kenntnisse, wie z. B. über die IT-Infrastruktur.
- Danach werden die ausgespähten Daten genutzt, um maßgeschneiderte **Programme** für einen Angriff anzusetzen.
- **Der Angriff** wird sichtbar. Gleichzeitig werden weltweit Verschlüsselungstrojaner vollautomatisiert aktiv. Daten werden verschlüsselt und Lösegeldforderungen hinterlegt. Mittel zur Verteidigung – wie Antivirenserver – werden ebenfalls verschlüsselt.
- Der letzte Schritt wäre/ist eine Lösegeldzahlung in Kryptowährung bzw. mit Bitcoins.

Die Maßnahmen

- Abschalten aller IT-Systeme weltweit
- Information aller Mitarbeiter
- Bildung eines Krisenstabs und Arbeitsgruppen
- Information von Ermittlungsbehörden und Aufsichtsbehörden
- Einbeziehung externer Forensik Spezialisten
- **Aber: Kein Eingehen auf die Forderungen der Erpresser!**

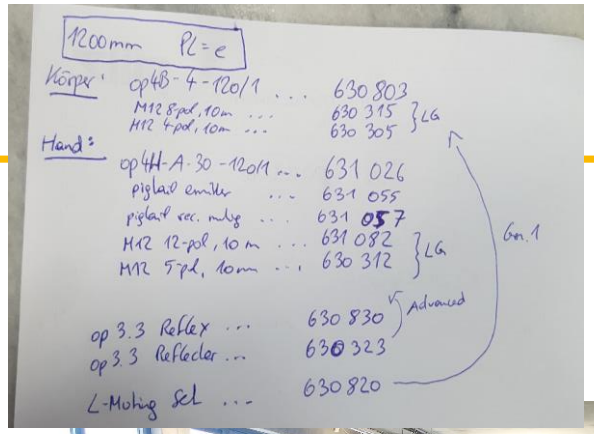
Die Herausforderung

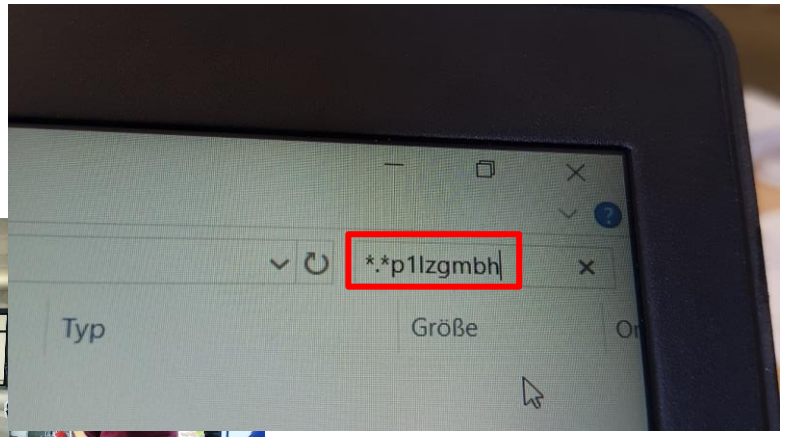
- Information von Mitarbeitern, Kunden und Partnern
- Abwehr des Angriffs
- Planung und Koordination des Wiederaufbaus
- … eines Unternehmens mit 2.500 Mitarbeitern in 42 Tochtergesellschaften und internationalen Entwicklungs- und Produktionsstandorten in Deutschland, Schweiz, Frankreich, Irland und China
- … ohne Computer, E-Mail, Festnetztelefon, Website, CRM-Systeme, Adressdatenbanken und Telefonverzeichnisse, Dateiablage, Intranet, SAP, …

Wie haben wir uns nach dem Angriff aufgestellt?

- Da alle Computer **weltweit** ausgeschaltet bleiben mussten und die Produktionsstandorte still standen, wurde der **persönliche Kontakt und Austausch** – intern und extern – unser wichtigstes Werkzeug.
- Wir waren anfangs weder über Festnetztelefone noch per E-Mail für unsere Kunden und Partner erreichbar. Auch die Website war erstmal nicht verfügbar. Als einziges Kommunikationsmittel blieben also die **Mobiltelefone**.
- Für den internen Austausch – speziell auch für unsere weltweiten Mitarbeiter – richteten wir einen sicheren **Messenger-Dienst** ein und hielten tägliche **Telefonkonferenzen** ab.
- Für die Außenwelt wurde eine zentrale **Telefonhotline** und eine **Mailadresse** eingerichtet, um unsere Erreichbarkeit zu gewährleisten.

Organisation intern





Kurzer zeitlicher Abriss

- Eine Woche nach dem Angriff konnten wir wieder ausliefern.
- Ende Oktober lief unsere Endmontage in Ostfildern wieder an.
- Anfang November folgten die SMD-Linie in Ostfildern und die Produktion an unserem französischen Standort Betschdorf.
- An unserem Schweizer Standort wurde einen Monat nach dem Angriff wieder produziert.
- Ende November ging auch unsere chinesische Produktionsstätte wieder in Betrieb.

Die Zeit danach
Security als immerwährende Aufgabe der Systemerneuerung

Ransomware hat die Serverdaten bei Pilz verschlüsselt. Der Unternehmer will aber nicht zahlen. (Foto: Den Rise/Shutterstock)

- Wir haben gelernt, dass die Investition in Security Software alleine nicht ausreicht!
- Wir haben gelernt, dass Cyber Abwehr die heute gut ist, in spätestens 3 Jahren veraltet und verwundbar ist!
- Wir haben gelernt, dass Offline-Backups unbedingt notwendig sind.
- Wir haben gelernt, dass die Wirtschaft ein Ziel ist!
- Wir haben gelernt, dass wir uns wehren können!
- Wir haben gelernt, dass wir konstant in die Veränderung und dadurch Verbesserung unserer Security-Konzepte investieren müssen!

Die Erfahrungen als Chance nutzen

Gehen gestärkt aus Hackerangriff: Die Pilz-Geschäftsführer Susanne Kunschert und Thomas Pilz. - Bild: Pilz

- Aus der Cyberattacke konnten wir wertvolle Erfahrungen sammeln und nutzen diese als Chance.
- Es gilt Prozesse zu hinterfragen und mit neuen Erkenntnissen aus diesem Angriff hervorzugehen.
- Es wird wohl noch einige Zeit vergehen, bis für alle Mitarbeiter sämtliche IT-Dienste wieder im gewohnten Umfang zur Verfügung stehen.
- Der Zusammenhalt und das Miteinander der Menschen sowie der Wille, Probleme gemeinsam zu lösen, haben uns getragen.
- Unseren Kunden und Partnern, die uns im persönlichen Kontakt viel Verständnis entgegengebracht haben, sind wir sehr dankbar.

PILZ Security Services

Wie können wir unterstützen?

Security für die Automation-Zone
OT (Operational Technology) → PLCs, Visualisierung, ..
Vom Risk Assessment bis zur Verifikation nach IEC 62443

Schulungsangebot „Certified Security Expert“
Einstieg in das Themengebiet Industrial Security

Industrial Firewall „SecurityBridge“
Paketfilter, Rollenbasiertes VPN, sowohl Pilz als auch 3rd Party Geräte

Vielen Dank für Ihre Aufmerksamkeit!