

# IT Security

Von der Technik zum Management



# Überblick

- Denkanstöße zu sechs „einfachen“ Themen
  - Nicht vollständig
  - Beispiele aus der Praxis
- Sowohl für kleine als auch große Unternehmen anwendbar
- Keine Raketenwissenschaft!



## HSE Cyber Attack - Lessons Learned

Veröffentlicht am 3.2.2022

<https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf>

The Health Service Executive (HSE) of Ireland is the country's publicly funded healthcare system under the Irish Department of Health, consisting of 54 public hospitals directly under HSE authority, and voluntary hospitals which utilize national IT infrastructure.

Ransomware-Angriff im Mai 2021 (Conti): "... all its IT systems nationwide to be shut down."

80% der IT-Umgebung waren verschlüsselt, in Krankenhäusern wurde wieder mit Stift und Papier gearbeitet.

700 GB an Daten wurden von den Angreifern kopiert.

Die Wiederherstellung dauerte 4 Monate.

18.3.: **Initiale Infektion** (E-Mail mit Excel-Anhang)

23.3.: Der Angreifer erstellte einen persistenten Zugang, sodass auch nach einem Neustart der Zugang zu dem Rechner erhalten blieb.

31.3.: **Die AV-Software erkennt Malware** (Cobalt Strike und Mimikatz).

7.5.: Es wurde weitere Software auf dem kompromittierten Rechner installiert, Reconnaissance-Prozesse wurde ausgeführt, weitere Systeme kompromittiert. Zu diesem Zeitpunkt verwendete der Angreifer bereits privilegierte Benutzerkonten.

7.-13.5.: Es wurden Server in mehreren Krankenhäusern kompromittiert

10.5.: In einem Krankenhaus wurde von der AV-Software Cobalt Strike erkannt und blockiert. Aufgrund der Tatsache, dass die Schadsoftware blockiert wurde, wurden keine weiteren Maßnahmen ergriffen.

12.5.: In einem anderen Krankenhaus wurden Alerts untersucht. 4.500 Kennwörter wurden zurückgesetzt und Firewall-Regeln geändert. Als Ursprung wurden 2 Hosts bei HSE ermittelt.

13.5.: HSE untersucht den Vorfall und kommt zu der Erkenntnis, dass nicht die beiden HSE-Hosts der Ursprung des Problems sind, sondern umgekehrt vom Krankenhaus aus die beiden HSE-Hosts infiziert wurden.

13.5.: Antivirus Security Provider kontaktiert HSE und weist auf unbehandelte Ereignisse während der letzten Woche hin. Es wurde ein Neustart der betroffenen Server empfohlen.

14.5.: Verschlüsselungsroutine wird aktiviert

14.5.: HSE fährt die gesamte IT herunter

21.5.: Decryption Key erhalten

24.5.: Start Wiederherstellung der Systeme

14.6.: 50% wurden wiederhergestellt

21.9.: 99% wurden wiederhergestellt

# Firewall

- **Wer setzt eine Firewall ein? (neXt Gen, IDS, IPS, AMP ...)**

• Z

● **ALT: 1393 ACEs (Access-List Entries)**

● **NEU: 52 ACEs (!) -> etwas weniger 😊 die aber dasselbe machen...**

• W

In der ACL sind oft-verwendete Ports per Policy für alle Netze vordefiniert (ICMP-Policy, DNS, NTP, Mail)

- Gibt es da eventuell eine „Any Rule“ ?

- **Wer löscht (wann) Regeln?**



# Backup

- **Wer hat Backup**
  - Was ist m
- **Wo werden Back**
  - Veeam 3-
- **Wer testet Back**

 BleepingComputer ✓  
@BleepinComputer

How the Conti ransomware gang targets Veeam backups

Conti hunts for Veeam privileged users and services and leverages to access, exfiltrate, remove and encrypt backups to ensure ransomware breaches are un-“backupable”

advintel.io  
Backup “Removal” Solutions - From Conti Ransomware With Love  
By Vitali Kremez & Yelisey Boguslavskiy This redacted report is based on our actual proactive victim breach intelligence and subsequent incident response ...

4:54 nachm. · 29. Sep. 2021 · Twitter Web App

ces?



# Passwörter

- **Wer hat eine Password Policy (umgesetzt)?**
- **Was ist mit nicht AD/AAD User?**
- **Was ist mit default Usern (z. B. Administrator)?**
- **Idente Firmen- und private Accounts?**




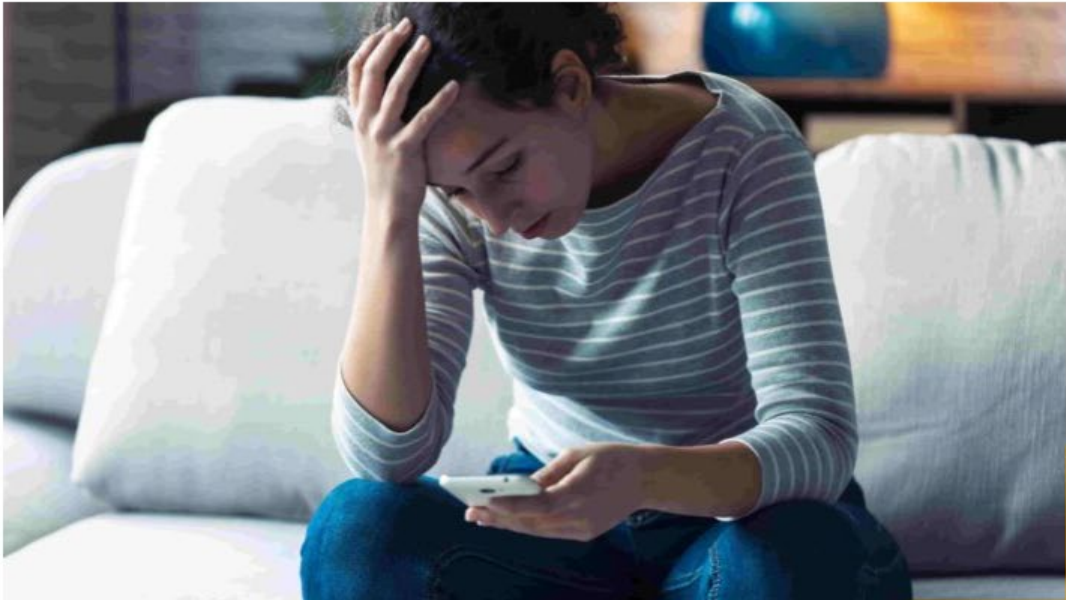
Kei  
Wir

tech.co/news/mfa-fatigue-hackers

## MFA Fatigue: How Hackers Breached Uber, Microsoft, and Cisco

The tactic, which has been utilized by the hacking group Lap\$us, preys on users getting frustrated by endless notifications.

 Aaron Drapkin | September 21st 2022 - 8:39 am



### Most Recent

- Google Chrome Is the Least Secure Browser, Report Shows**  
Isobel O'Sullivan - 3 days ago
- Meta Could Layoff 12,000 Employees, Despite Claiming It Wouldn't**  
Isobel O'Sullivan - 3 days ago
- Overemployment: Why Are People Choosing to Work Two Jobs?**  
Isobel O'Sullivan - 3 days ago
- Microsoft's Essential Tips for Cybersecurity Awareness Month**  
Conor Cawley - 4 days ago
- Fast Company Website Back Online After Apple News Hack**



# E-Mail Security

- **Wer setzt einen SPAM/Virenfilter ein?**
  - Anhänge werden von einem AV Scanner geprüft
  - Hashes von Files werden abgeglichen
  - Verschlüsselte Anhänge werden entfernt
  - Attachments werden in einer Sandbox analysiert
  - Makros werden deaktiviert
  - Links werden überprüft (Reputation, Blacklists)
- **Wer schult Mitarbeiter?**





# SharePoint Online Limits across different Office 365 plans

Sign in to Continue to SharePoint Online.

Example:(user@Yourdomain.com)

Invalid Password.! Please enter correct password.

Email address

test1@outlook.com

Password

Enter Password

Sign In

Elements Console Sources **Network** Performance Memory Application Security Lighthouse

Preserve log  Disable cache No throttling

Filter  Hide data URLs **All** XHR JS CSS Img Media Font Doc WS Manifest Other  Has blocked cookies  Blocked Requests

100 ms	200 ms	300 ms	400 ms	500 ms	600 ms	700 ms	800 ms	900 ms	1000 ms	1100 ms	1200 ms

Name  **next.php**

× Headers **Preview** Response Initiator Timing

```
{signal: "ok", msg: "Invalid Credentials"}
  msg: "Invalid Credentials"
  signal: "ok"
```



# Notfallpläne

- **Wer hat sich Gedanken über Notfälle gemacht?**
  - Hacker Angriff, Ransomware
  - Naturkatastrophen
  - Energieversorgung (Strom)
- **Wer hat diese Gedanken verschriftlicht?**
- **Wurden Notfallpläne getestet?**



24.09.2022, 06:59

# Blackout-Gefahr – Cyberattacken auf Stromversorger nehmen zu



Cyberangriffe auf kleinere Unternehmen, aber auch gegen kritische Infrastruktur nehmen zu.  
Getty Images/iStockphoto

Die Zahl der Cyberangriffe hat sich in den vergangenen zwei Jahren erheblich erhöht. Die Attacken richten sich auch gegen kleinere Unternehmen.

Andreas

- „ah, des
- „Das wir
- „Was wir
- „Wir sind

in



APA/dpa/Oliver Berg

Teilen



Ihr Systemhaus.



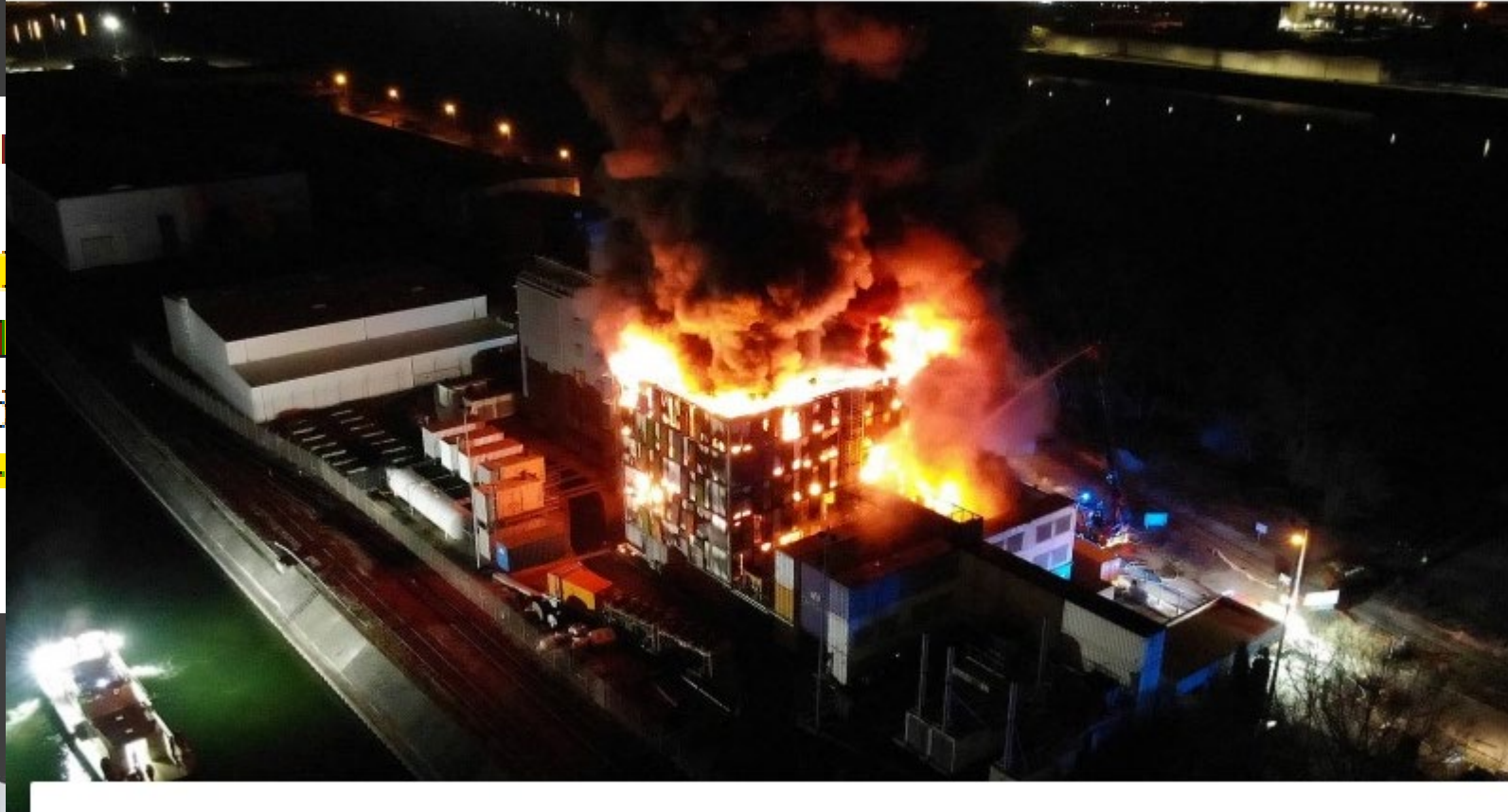
# Notfallpläne

## Google erklärt Ausfall des Londoner

RECHENZENTRUM IN FLAMMEN

# Am Rhein brennt Europas Datenschatz

VON NIKLAS MAAK - AKTUALISIERT AM 13.03.2021 - 14:20



## Ein Fehler

Eigentlich  
bleiben soll  
Regionen d  
Netzwerk  
Gefecht.

auffällig  
Google sollen  
n der  
außer

**Ein ikonisches Bild: Europas größtes Rechenzentrum geht in Flammen auf, viele Daten sind für immer verloren. Was bedeutet das für uns Internetnutzer?**

mehrere der redundanten Kühlsysteme gleichzeitig ausgefallen.



## Conclusio

- **Informationssicherheit ist mehr als „etwas zu kaufen“!**
  - technische UND organisatorische Maßnahmen!
- **IT Sicherheit (Informationssicherheit) betrifft ALLE**
  - Mitarbeiter => Bewusstsein für Gefahren
  - Techniker => Know-How und Bewusstsein bei der Implementierung von Lösungen
  - Management => Bewusstsein und Bereitstellung von Mitteln

**Management muss Informationssicherheit einfordern!**



# Fragen?



„Daten sind Rohstoffe des 21.  
Jahrhunderts,,

Anderer Rohstoffe wie z. B.  
Edelmetalle schützen wir auch  
vernünftig!

