

# Cyberbedrohungen für Ihr Unternehmen

und wie Sie sich schützen können



**Hans-Otto Mohr**

Leiter Competence Center Security  
IT-HAUS  
E-Mail: [hmohr@it-haus.com](mailto:hmohr@it-haus.com)

# Agenda

1. Cybercrime aktuell
2. Was hilft?  
Handlungsempfehlungen

Agenda



## Hackerangriff auf Bafin-Website

Die Finanzaufsicht Bafin hat mit den Folgen eines Hackerangriffs auf ihre öffentliche Website zu kämpfen.



## Deutsche Leasing stellt Datendiebstahl fest

Die Deutsche Leasing AG wurde vor drei Monaten gehackt. Nun hat

Frankfurter Uniklinikum: Hackerangriff hat Folgen für Patienten und Studenten

Julia M.

## Immer mehr Attacken aus Russland und China auf deutsche Wirtschaft

Russland und China sind wichtigste Basis für Angriffe



DATENABFLUSS WIRD GEPRÜFT

## Cyberangriff auf Maternus-Kliniken AG

Die Maternus-Kliniken AG ist Opfer eines Cyberangriffs geworden. nervor, die am Freitag in Berlin veröffentlicht...

den  
ommen  
m



## Cloud Nordic verliert fast alle Daten nach Angriff

Der dänische Cloud-Anbieter Cloud Nordic wurde von einer Ransomware-Attacke getroffen. Dabei gingen fast sämtliche Daten der Kunden verloren.

Aufgrund einer Cyber-Attacke ist das Bürgerbüro am **Samstag, 02.09.2023, geschlossen.** Leider müssen auch sämtliche Termine bis einschließlich **Montag, 04.09.2023** storniert werden. Wir bitten um Verständnis und arbeiten daran, so bald wie möglich

DDoS-Attacken

## Hackerangriff legt deutsche Städte-Webseiten lahm

Hacker haben in den vergangenen Tagen mehrere Webseiten deutscher Städte, darunter Köln, Dortmund, Frankfurt und Nürnberg, lahmgelegt.



Das größte Risiko für Unternehmen –

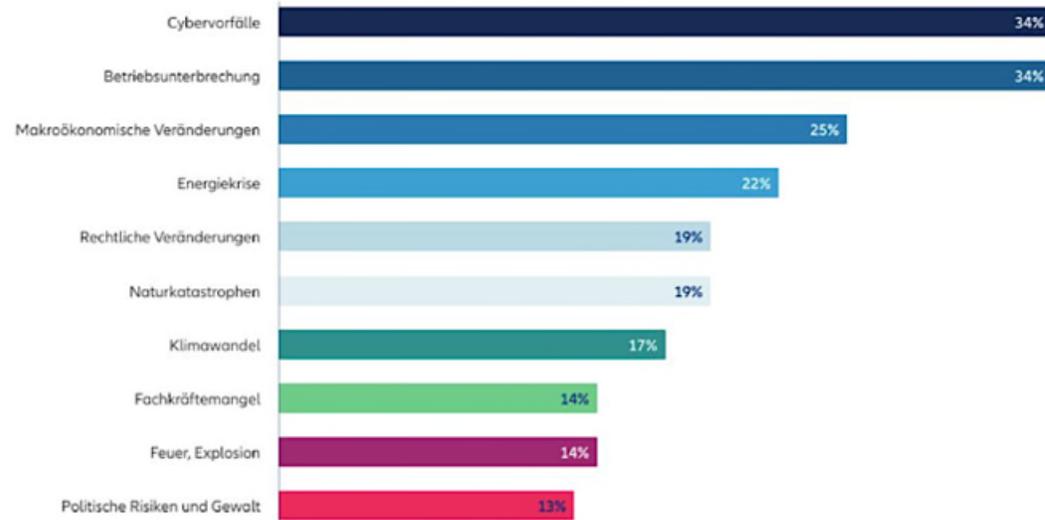
# Cyberfälle



## Top 10 Geschäftsrisiken weltweit in 2023

Allianz Risk Barometer 2023

Basierend auf den Antworten von 2.712 Risikomanagement-Experten aus 94 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.



AGCS News & Insights

Source: Allianz Global Corporate & Specialty

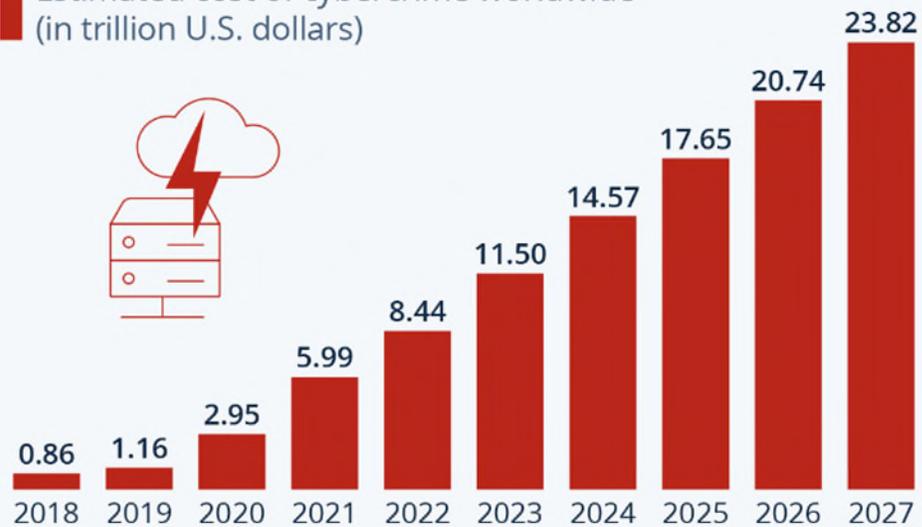
# 84%

aller von BITKOM befragten Unternehmen waren 2022 von Cyberangriffen betroffen

# Die Kosten aus Cybercrime explodieren

## Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide  
(in trillion U.S. dollars)



As of November 2022. Data shown is using current exchange rates.

Sources: Statista Technology Market Outlook,  
National Cyber Security Organizations, FBI, IMF

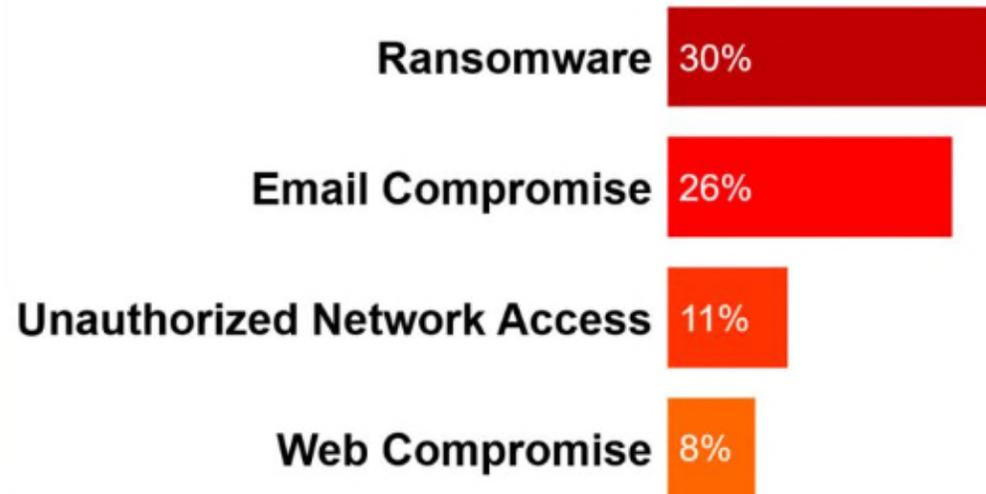


# Ransomware und Phishing dominant



## Threat Incident Frequency

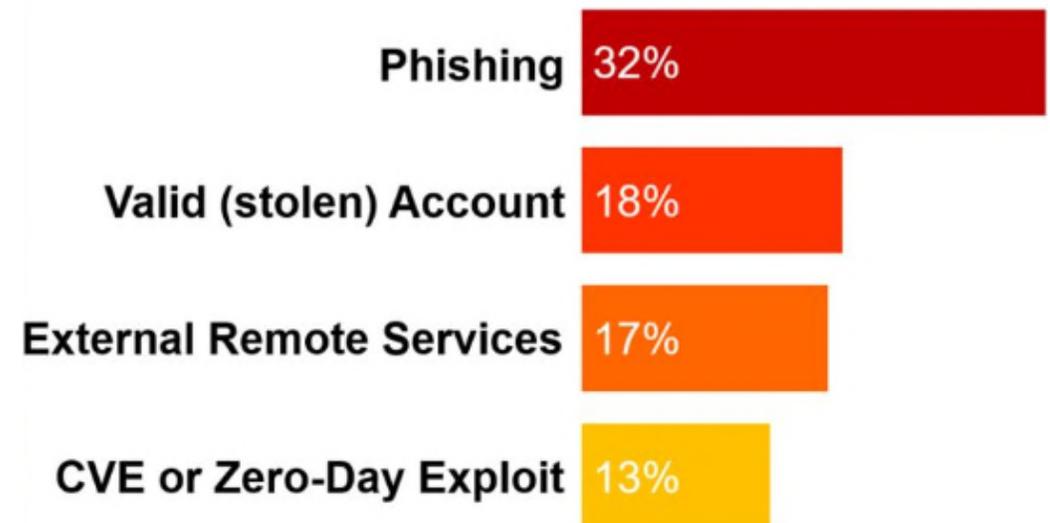
30% of cyber incidents are Ransomware attacks



Q1 2023 Threat Landscape Report  
Published May 2023

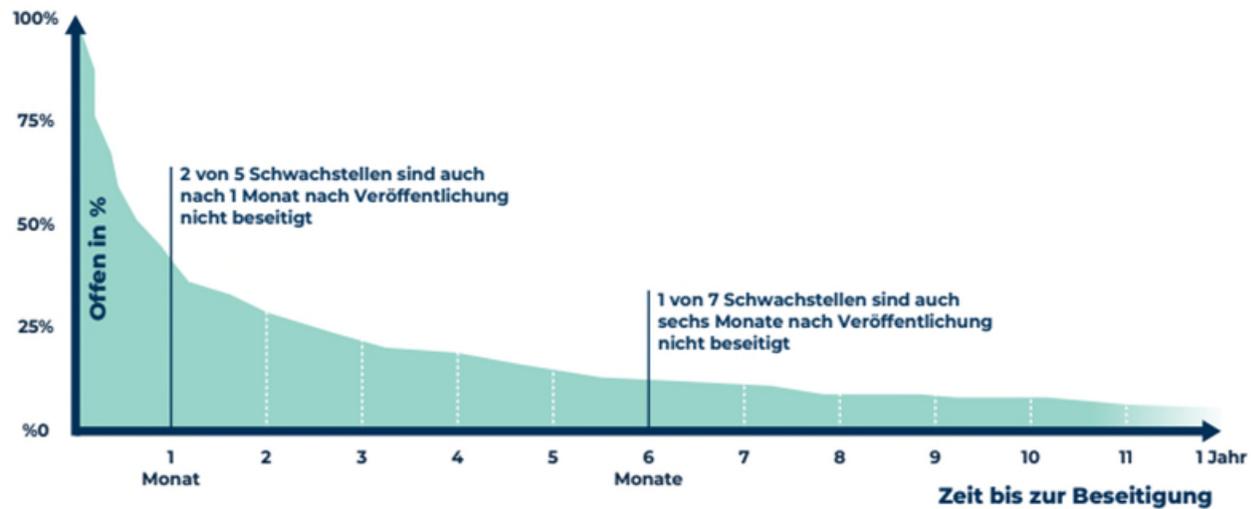
## Cyber Threat Access Method

32% of Cybercrime uses Phishing for initial access



Q1 2023 Threat Landscape Report  
Published May 2023

# 11.000 Schwachstellen je Unternehmen



Quelle: Cybersecurity Report Schwarz Gruppe 2023

# Nicht nur IT-HAUS setzt auf „as a Service“



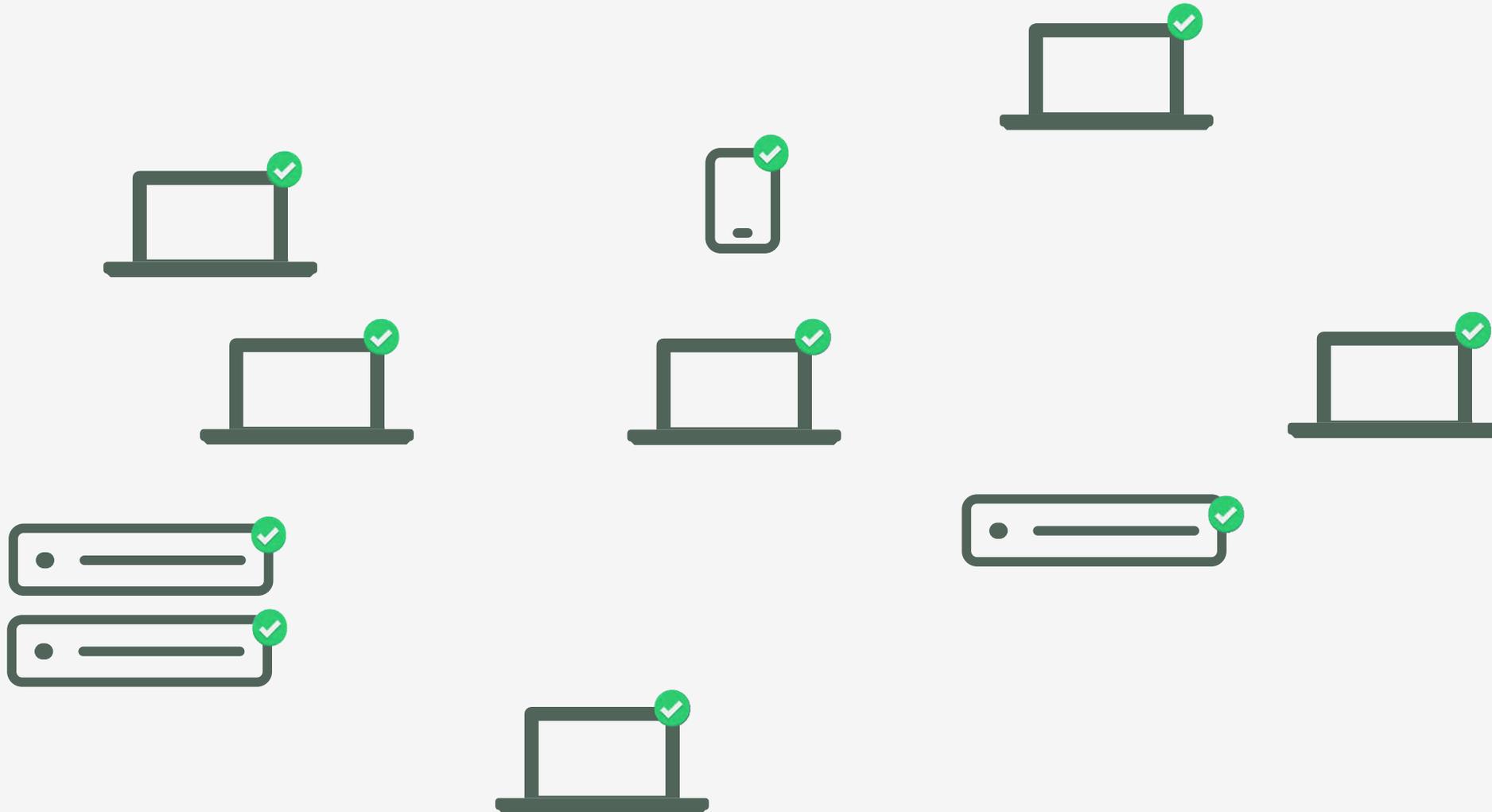
## Cybercrime as a Service

DDoS	ab 9 EUR/Std.
Botnetz	ab 75 EUR/Monat
Phishing-Kampagne	ab 499 EUR/Monat
Keylogging-Kampagne	ab 180 EUR/Monat
Ransomware und RAT	ab 1.000 EUR/Monat
Malware Angriff	ab 40 EUR
Social Media Account	ab 9 EUR
Netflix Account	ab 90 Cent
Kreditkarten-Klon	ab 7 EUR
E-Mail mit Passwort	ab 60 Cent
Admin Account	500 - 140.000 Euro

**-50%**

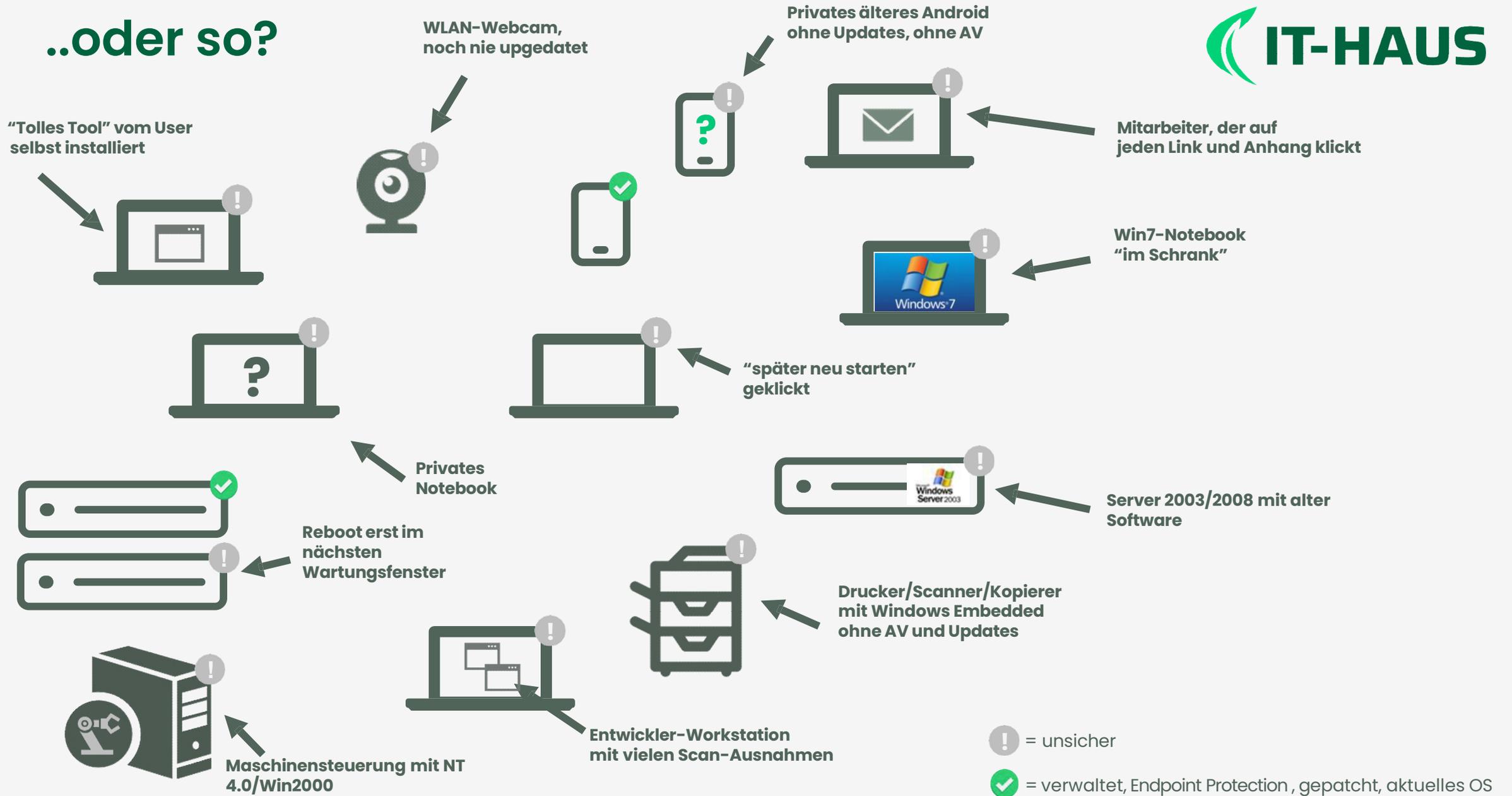


# Sieht Ihr Netzwerk so aus?



 = verwaltet, Endpoint Protection , gepatcht, aktuelles OS

# ..oder so?



..oder so?

"Tolles Tool" vom User selbst installiert

WLAN-Webcam, noch nie upgedatet

Privates älteres Android ohne Updates, ohne AV

Mitarbeiter, der auf jeden Link und Anhang klickt

..dann brauchen Sie Unterstützung

Win7-Notebook "im Schrank"

"später neu starten" geklickt

Privates Notebook

Server 2003/2008 mit alter Software

Reboot erst im nächsten Wartungstermin

Drucker/Scanner/Kopierer mit Linux Embedded ohne AV und Updates

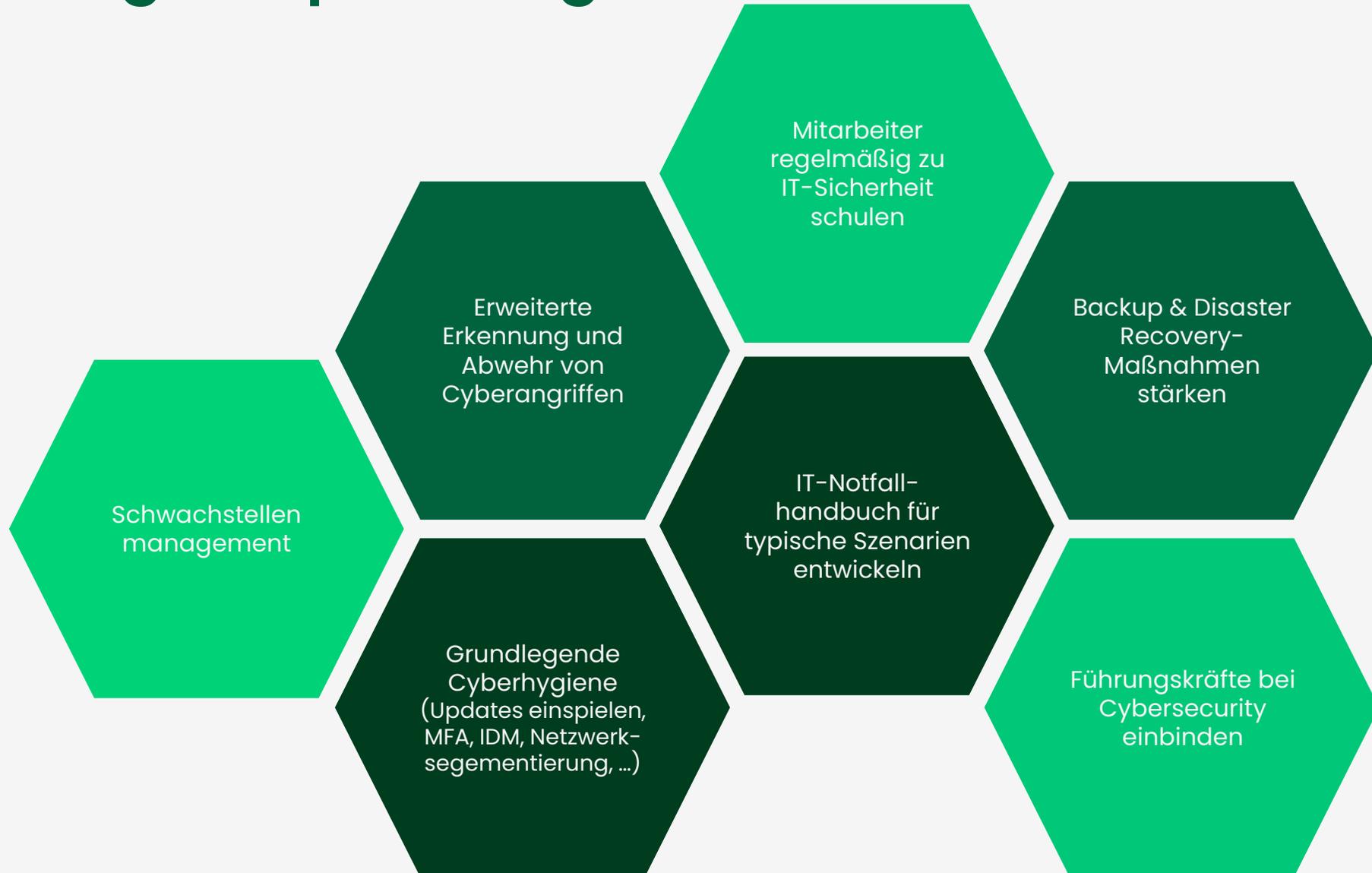
Entwickler-Workstation mit vielen Scan-Ausnahmen

Maschinensteuerung mit NT 4.0/Win2000

! = unsicher

✓ = verwaltet, Endpoint Protection, gepatcht, aktuelles OS

# Handlungsempfehlungen



# Schwachstellen finden und Patchen

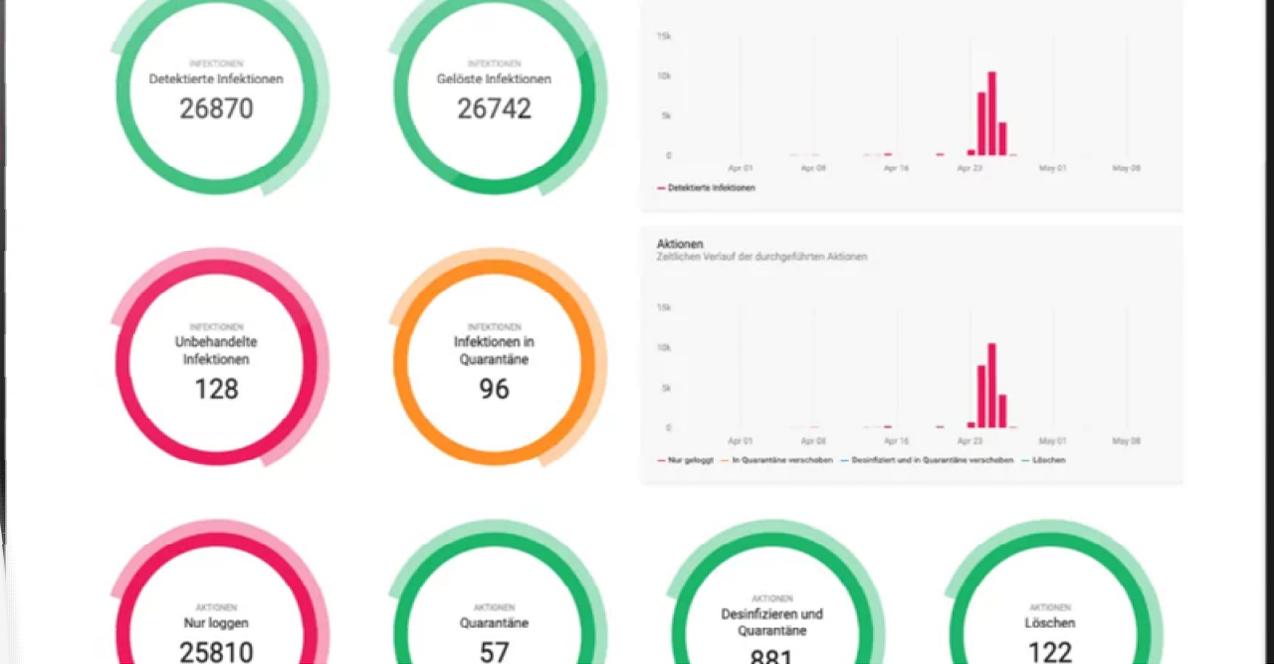
Inventarisieren ihrer IT Assets -> automatisch binnen Minuten

Ermittlung der Softwarestände

Permanenter Abgleich mit aufkommenden Vulnerabilities (CVE)

Klassifizierung / Priorisierung nach Kritikalität

**PATCHEN!**



Suchen...

IP: 123.456.789.10

Subnetz: 123.456.789.0/24

MAC: ab.cd.ef.gh.12

Zuletzt gesehen am: 04.03.22, 14:42:21

Watchdog: watchdog-01

Betriebssystem: windows

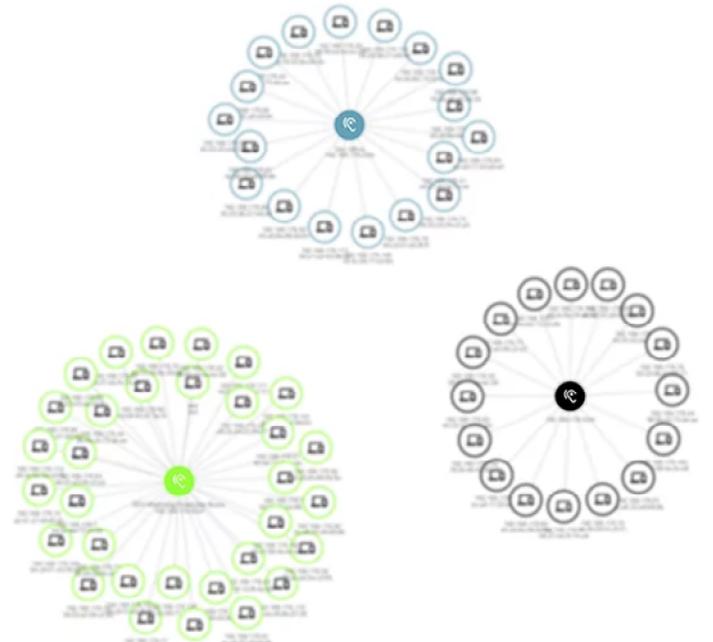
Hersteller: Micro-Star INTL CO., LTD.

Technischer Verantwortlicher: Max Mustermann (max.mustermann@domain.com)

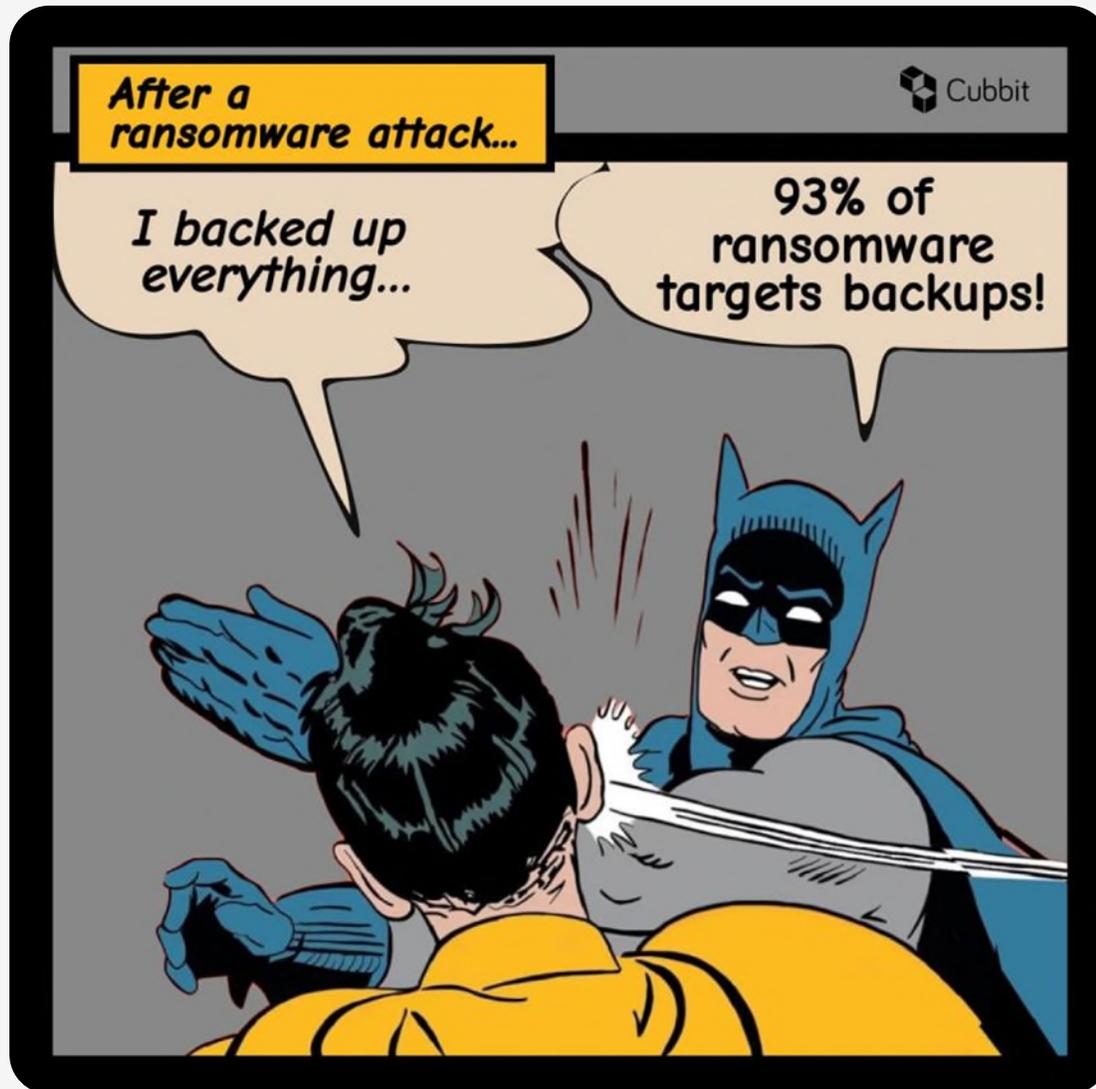
Fürthlicher Verantwortlicher: Peter Müller (peter.mueller@domain.com)

Hostnames: client-03

Details: Microsoft HTTPAPI/2.0



# Kernmassnahme Backup



## 3-2-1-1-0 Regel:

- 3 Kopien
- 2 Medien
- 1 Kopie offsite
- 1 Kopie entweder offline oder unveränderbar (immutable)
- 0 Fehler im Backup



## 3-2-1-1-0 Regel:

- 3 Kopien inkl. Produktion
- 2 Medien
- 1 Kopie offsite
- 1 Kopie entweder offline oder unveränderbar (immutable)
- 0 Fehler im Backup

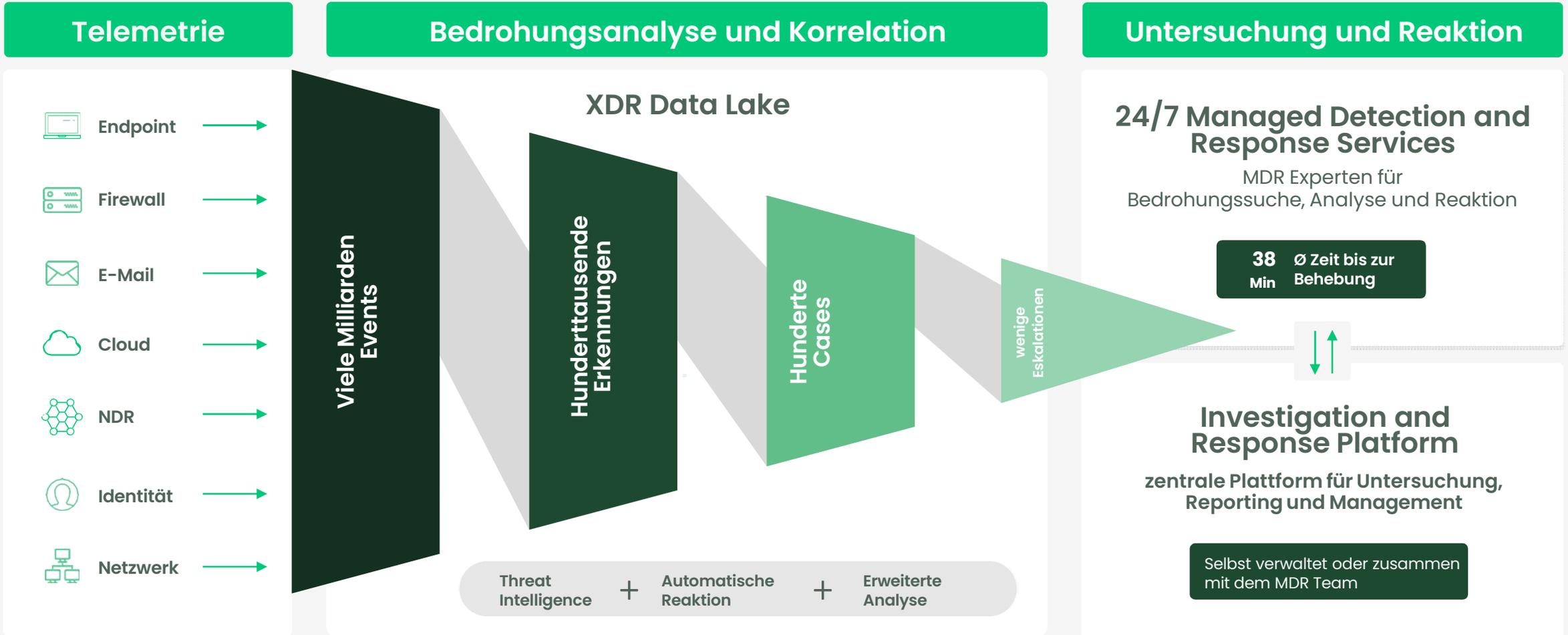
Angriffserkennung: Team zu klein für 24/7? Zu wenig Erfahrung?

# Managed Detection and Response



Erkennung und Reaktion:

# Gemeinsam oder durch Anbieter



# Das Ergebnis zählt: Rundum sicher durch Cybersecurity as a Service

- ✓ Ihr ausgelagertes Security Operations Center (SOC)
- ✓ Nutzung vorhandener Systeme -> Logs, Telemetrie
- ✓ 24/7 Bedrohungserkennung und Reaktion
- ✓ Bedrohungssuche durch Experten
- ✓ Vollständiges Incident Response bei Angriffen
- ✓ Bestmögliches Ergebnis für Ihre IT-Sicherheit



Aktuell Sonderpreis -25% für KMU möglich!

Rundum geschützt

# IT-Sicherheit by IT-HAUS

Die 360-Grad-Lösung für Ihre IT-Security



# Vielen Dank für Ihre Aufmerksamkeit

Ihre Herausforderungen sind unser tägliches Geschäft