



IT-Solutions AG

# Super-GAU Cyberattacke

Was kann ich im Vorfeld tun?

**Zur Person**

**Jens Hildenbeutel**  
 Fachinformatiker Fachrichtung Systemintegration  
 Leiter IT-Service-Management

**IT-Werdegang:** Als Hobby C64 → PC → DOS →  
 Produktiv seit NT4 und Windows 95

**Security-Schwerpunkte:** Microsoft → Barracuda Networks  
 Firewalls (Netz und WAF), E-Mail, ZTNA, Backup



Unbequeme Tatsachen

Tätermotivation

Chronik eines Cyberangriffs

**Sonntag, 29.12.24 – 01:23:45**

- Nach 209 Tagen unbemerkt im Netz und 219 Tagen seit der Entdeckung des schlecht gepatchten Webserver, erfolgt der finale Angriff.
- Wie ein Flächenbrand raubt die Angriffswelle durch das Netzwerk alle Datenlogger, E-Mail-Systeme, SAP-Computer - selbst die Steuerung der Produktionsmaschine - und alle Datenstrukturen der letzten Monate sind ergrascht worden.



# Zur Person



## Jens Hildenbeutel

Fachinformatiker Fachrichtung Systemintegration

Leiter IT-Service-Management

IT-Werdegang: Als Hobby C64 → PC → DOS →  
Produktiv seit NT4 und Windows 95

Security: Microsoft → Barracuda Networks  
Schwerpunkte: Firewalls (Netz und WAF), E-Mail, ZTNA, Backup

# Chronik eines Cyberangriffs

- Wir beginnen mit der Tat – und bewegen uns durch die Zeit, um den Angriff zu verfolgen

- Wir lernen ausgenutzte Lücken und die Motivation der Angreifer kennen

- Tipps zur Prävention

**COLUMBO**



# Sonntag, 29.12.24 – 01:23:45

- Nach 203 Tagen unbemerkt im Netz und 219 Tagen seit der Entdeckung des schlecht gepflegten Webserver, erfolgt der finale Angriff.
- Wie ein Flächenbrand rast die Angriffswelle durch das Netzwerk
- Alle Dateiserver, E-Mail-Systeme, SAP, Computer - selbst die Steuerung der Produktionsmaschinen - und alle Datensicherungen der letzten Monate sind erfolgreich verschlüsselt worden.

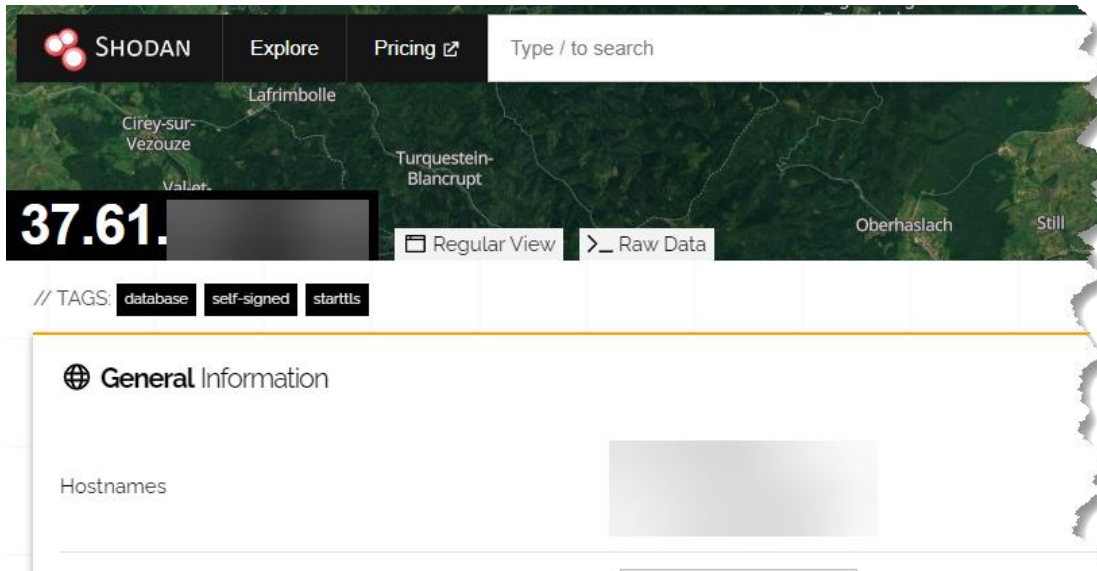
**75% aller SMB sind nach einem erfolgreichen Verschlüsselungsangriff nicht mehr in der Lage den Betrieb fortzusetzen\***

**\*Cybercatch Small Business and Medium Sized Businesses Ransomware Survey 2022 (Unternehmen <1000 AN)**

# 26.05.2024 – Tag 0

- Bei der Auswertung automatisierter Schwachstellensuchen entdeckt ein Unbekannter einen schlecht abgesicherten Webserver
- Wenige Minuten später weiß der Unbekannte, dass es sich beim Besitzer des Servers um einen „hidden champion“ handelt
- Der Unbekannte beschließt, den Fund genauer zu untersuchen

# Viele Informationen sind öffentlich!



SHODAN Explore Pricing Type / to search


37.61. [redacted]

Regular View Raw Data

// TAGS: database self-signed starttls

### General Information

Hostnames [redacted]



Open Ports

21	25	53	80	443	465	587	993	995	3306	3333	8443	8880
----	----	----	----	-----	-----	-----	-----	-----	------	------	------	------

// 21 / TCP



## Critical

**CVE-2008-3844**

**9.3** Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

## Medium

**CVE-2020-15778**

**6.8** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because

target systems where users are in use. NOTE: the discoverer states a "side effect" of the OpenSSH development process do not want to classify such a username enumeration (or "oracle") as a vulnerability.

**CVE-2021-41617**

**4.4** sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

**CVE-2007-2768**

**4.3** OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user

**CVE-2016-20012**

**4.3** OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an

# 28.05.2024 – Tag 2

- Der Unbekannte wird zum Angreifer, denn der Serverbesitzer – von jetzt an das Opfer – scheint ein lohnendes Angriffsziel zu sein

# 09.06.2024 – Tag 14

- Nachdem ein Mitarbeiter der Buchhaltung die .pdf-Datei eines nicht existenten Lieferanten geöffnet hat, stürzt sein Computer ab.
- Er startet den Rechner neu – „nichts passiert“
- Recherche zur Herkunft der Mail unterbleibt, da offenbar „schlechter Scherz“
- Ein umfassender E-Mail-Scan hätte die Bedrohung entdeckt...

# Exkurs:

- Durch den „Systemabsturz“ hat der Angreifer dafür gesorgt, dass sein Backdoor im System fest verankert ist.
- Der Angriff ist jetzt persistent, es besteht jederzeit Fernzugriff auf das Netzwerk des Opfers



# 11.06.2024 – Tag 16

- Der Angreifer hat das Netzwerk ausgekundschaftet und kartiert
- Er hat längst eine Anzahl Schwachstellen ausgemacht
- Er weitet nun Stück für Stück seine Präsenz im Netz aus

# Exkurs:

- Der Angreifer nutzt zuerst die Rechte des angemeldeten Nutzers
- Auf dem angegriffenen Rechner hat er längst nicht nur Administrator- sondern Systemberechtigungen
- Sobald sich ein Administrator auf dem Rechner anmeldet, um den Rechner zu warten, kann auch dessen Identität gestohlen und übernommen werden



# 17.06.24 – Tag 22

- In den Systemlogs der Verzeichnisdienstserver häufen sich ungültige Anmeldeversuche
- Die Logs werden leider weder händisch noch automatisch überwacht

# Exkurs

- Verzeichnisdienste wie Active Directory sind ein lohnendes Ziel, da in der Datenbank die Identitäten und Berechtigungen der Nutzer gespeichert sind
- Weil viele Anwendungen die Nutzeranmeldung über AD integrieren (SSO), bedeutet dies auch viele Zugriffe von und in andere Netzbereiche





# 20.06.24 – Tag 25

- Der Angreifer hat einen alten Server gefunden, der nur zum Austausch von Daten zwischen SAP und Produktionsmaschinen dient
- Jetzt kennt er auch die Maschinensteuerungen, deren Version – und damit deren Schwachpunkte...

# Exkurs

- Gerade für alte Systeme ist es besonders leicht, Sicherheitslücken zu ermitteln. Datenbanken wie CVE sind öffentlich einsehbar
- Dies gilt für Linux / UNIX genauso wie für Windows





# 21.06.24 – Tag 26

- Ein Glückstag – leider für den Angreifer
- Er findet auf einem Dateiserver eine Passwortliste. Diese ist zwar schon älter, aber auf dieser ist erkennbar, dass einfache Passwörter oft mehrfach und für verschiedene Zwecke genutzt werden
- Leider gibt es keine unternehmensweite Passworttresor-Lösung

# Exkurs

- Passwortlisten, Post-Its leisten Ihnen einen Bärendienst
- Passwort-Recycling auch – egal wie lange das Kennwort ist
- Gehen Sie immer davon aus, dass nicht Sie Ihr Passwort verlieren, sondern jemand anderes Ihr Passwort verliert!
- Grundregel: Eine Anmeldung = ein Passwort



# 02.07.24 – Tag 37

- Der Angreifer beginnt mit der Exfiltration von Daten der Konstruktion und Buchhaltung
- Über eine verschlüsselte Verbindung werden im Hintergrund fortwährend Daten auf die Virgin Islands übertragen
- Leider existieren weder Geo-Fencing noch IDP/IDS oder eine automatische Auswertung der Firewall-Logs

# Exkurs

- In Zeiten üppiger Bandbreiten fällt eine Belastung durch einen andauernden Upload kaum auf, wenn dieser nur einen Teil der Bandbreite belegt
- Geofencing, also die Filterung nach Ländern, allein ist auch kein Allheilmittel (Stichwort VPN-Anbieter)



# 17.07.24 – Tag 52

- Der Angreifer hat über Rechner in Buchhaltung, Konstruktion und Lager, sowie verschiedene Server Zugriff auf das Firmennetz, wann und wie es ihm beliebt.
- Er hat Vertraulichkeitsvereinbarungen mit verschiedenen Kunden entdeckt und macht sich zielstrebig auf die Suche nach den zugehörigen, gewinnversprechenden Daten.



# Zwischenstand

Spätestens an dieser Stelle hat das Opfer die Hoheit über sein Netzwerk und seine Daten verloren



# 30.07.24 – Tag 65

- Ein Mitarbeiter aus dem Marketing erhält einen Anruf von der IT. Er wird gebeten, ein Update zu installieren, und im Rahmen der Installation Benutzernamen und Kennwort neu einzugeben
- Leider kennt man die Mitarbeiter der IT nicht persönlich. Es gibt auch keine Verfahren zur Legitimitätsprüfung...
- Der Angreifer kann nun, beginnend mit diesen Daten, den E-Mail-Verkehr durchsuchen

# Exkurs

- Die Rolle von Social Engineering Angriffen wird oft völlig unterschätzt
- Oft ist ein solcher Angriff in strikten und anonymen Hierarchien erfolgreicher als in Organisationen, die einen offenen Umgang pflegen
- Dienst nach Vorschrift oder innerliche Kündigung begünstigen diese Angriffsform besonders



# 02.08.24 – Tag 68

- Der Angreifer hat erkannt, dass das Opfer Zulieferer für die Rüstungsindustrie ist.
- Er wendet sich an *sein* Netzwerk

# Exkurs

- Auch in der „Schattenwelt“ gibt es längst eine Wertschöpfungskette und Arbeitsteilung



# 04.08.24 – Tag 70

- Der Angreifer hat seine Erkenntnisse an einen Nachrichtendienst verkauft.
- Für umgerechnet 15.000 € wird er es sich eine Weile lang gut gehen lassen, bevor er wieder aktiv wird.
- Der Nachrichtendienst setzt gleich eine ganze Gruppe von Hackern auf das Opfer an

# Exkurs

- In Zeiten weltweiter Konflikte gibt es – nicht nur im Osten – zahlreiche staatliche Akteure
- Cyberangriffe durch staatliche Akteure sind nicht von Cyberversicherungen gedeckt



# Süddeutsche Zeitung (30.10.2013)

☰ Menü 🔍 SZ | Meine SZ | SZ Plus | Israel US-Wahl Ukraine | Politik Wirtschaft Meinung Panorama Sport Münch

Schon 2001 veröffentlichte die EU einen [Bericht zur Wirtschaftsspionage](#). Auch hier kommen die Franzosen nicht gut weg. Aufgelistet sind zwei Verdachtsfälle aus dem Jahr 1993. Es geht dabei um die Lieferung von Hochgeschwindigkeitszügen nach Südkorea, bei der sich der französische Hersteller Alstom (TGV) durch Spionage einen Wettbewerbsvorteil gegenüber dem deutschen Konkurrenten Siemens (ICE) verschafft haben soll. In einem der Fälle ist der französische Auslandsgeheimdienst Direction Générale de la Sécurité Extérieure (DGSE) als Quelle der Informationen benannt.





# 12.08.24 – Tag 78

Das Opfer wendet sich an den Hersteller seiner Maschinen, da er in den letzten Tagen immer wieder Probleme mit den Fertigungstoleranzen hat, die zu Ausschuss an sehr teuren Baugruppen führen

Einstweilen wird die Produktion der Baugruppe ausgesetzt

# Exkurs

- Es muss nicht immer Datendiebstahl sein
- Stellen Sie sich vor, man würde nur jede 157. Triebwerksschaufel eines Jettriebwerks sabotieren...



# 03.09.24 – Tag 100

- Nach fast 3-wöchigem Ausfall der Produktion und kompletter Überprüfung aller Komponenten durch den Hersteller wird die Produktion für die Baugruppe wieder angefahren.
- Innerhalb weniger Tage tritt das Problem erneut auf

# Exkurs

- In diesem Katz-und-Maus-Spiel sind der Perfidität des Angreifers leider keine Grenzen gesetzt



# 09.09.24 – Tag 106

- Experten des Nachrichtendienstes bewerten die Baugruppe, deren Funktion und Auswirkung auf das zugehörige Waffensystem
- Beim Opfer werden seit Wochen alle E-Mails als Kopie in Echtzeit abgegriffen

# Die gute Nachricht zur Halbzeit

Einer Sophos-Studie zu Folge liegt die Dwell-Time im Jahr 2023 bei nur noch 8 Tagen



# 12.09.24 – Tag 109

- Anwender erhalten von der IT die Bitte, eine Handyapp von einer Webseite herunterzuladen, die die Endgerätesicherheit verbessern soll
- Ein MDM (Mobile Device Management) würde solche Bitten überflüssig machen – falls sie von der IT stammen würden...

# Exkurs

- Ein MDM sorgt für Sicherheit und vereinfacht die Bereitstellung von Software erheblich
- Setzen Sie dienstlich Mobilgeräte ein, sollten Sie dringend ein MDM nutzen
- Wie authentifizieren sich Ihre IT-Mitarbeiter oder Dienstleister?





# 18.09.24 – Tag 115

- Beim Opfer melden sich Geschäftskontakte, die behaupten, sein Unternehmen hätte einen Virus verschickt.
- Die IT weist glaubhaft nach, dass der Absender am fraglichen Tag keine Mail zum Geschäftspartner geschickt hat.
- Damit ist die Sache für das Opfer erledigt

# Exkurs

- Diese Angriffsart nennt sich Conversation Hijacking.
- Der Angreifer erbeutet Mails und knüpft dann an diese an
- Durch den Mailverlauf erscheinen diese Mails dann vertrauenswürdig und werden unbewusst als harmlos bewertet
- Schutzmechanismen existieren!



# 19.09.24 – Tag 116

Der Nachrichtendienst beginnt mit der Auswertung seiner Phishing- und Conversation-Hijacking-Attacke **gegen die Geschäftspartner des Opfers**

# Exkurs

- Selbstverständlich sind Zulieferer und Kunden des Opfers weitere, interessante Ziele



# 23.09.24 – Tag 120

- Die Angreifer beschließen, zwischen Weihnachten und Neujahr zuzuschlagen, und alles wie eine Verschlüsselungsattacke aussehen zu lassen – um ihre Spuren zu verwischen
- Zahlt das Opfer, ist dies nur das „Sahnehäubchen“ – es ist nicht vorgesehen, die Daten jemals wieder zu entschlüsseln

# Exkurs

- Zahlung von Lösegeldern stärkt die Angreifer und sind keine Garantie, dass Sie Ihre Daten wiederbekommen
- Was bereits geleakt ist, wird auch durch Zahlung von Lösegeld nicht ungeschehen werden



# 26.09.24 - Tag 123

- Durch die Handyapps erbeutete Sprachdaten erlauben den Angreifern die Erstellung von Deep Fakes der Geschäftsleitung und verschiedener anderer Schlüsselpositionen

# Exkurs

Nein, wir sind nicht bei James Bond – mehr dazu gleich





# 04.10.24 – Tag 192

- Die Sekretärin eines anderen Unternehmens, in denen einer der Geschäftsführer ebenfalls beteiligt ist, überweist nach einem Telefonat dringend 25.000 € nach China, um dort festgefahrene Verhandlungen wieder in Gang zu bringen
- Die Arme wurde nie geschult – sonst hätte sie den **CEO-Fraud** erkannt oder reagieren können...

## Ferrari CEO impersonated by AI in deepfake scam attempt – report

NEWS

A Ferrari executive has stopped an elaborate scam in its tracks – but the incident is a warning to the automotive industry to be cautious.



Ben Zachariah

12:59 30 July 2024

5 comments

34 shares



Zitate: Bloomberg

"Sorry, Benedetto, but I need to identify you," the executive said, before asking what the book was that Mr Vigna had recommended to him just days earlier.

The call ended abruptly, and inquiries quickly determined it had been scammers imitating the Ferrari CEO's voice using artificial intelligence (AI).



Scammers pretending to be **Ferrari's CEO Benedetto Vigna** have been stopped in their tracks, thanks to a quick-thinking executive.

# 19.12.24 – Tag 207

- Auf einer Weihnachtsfeier ist die Geschäftsführung des Opfers froh, dass dieses seltsame Jahr, mit all den Problemen zum Glück so gut wie vorbei ist...
- Sein Alptraum wird im Skiurlaub erst richtig beginnen...

# Niemand glaubt an die Wahrscheinlichkeit eines Vorfalls, bis er passiert

Windows Sicherheit

Microsoft Press

2. Auflage, 2005

# Tätermotivation

# Was kostet es, einen Staat zu hacken?



World ▾ Business ▾ Markets ▾ Sustainability ▾ Legal ▾ Breakingviews ▾ Technology ▾ Investigations

## Exclusive: Chinese hackers attacked Kenyan government as debt strains grew

By Aaron Ross, James Pearson and Christopher Bing

May 24, 2023 11:28 PM GMT+2 · Updated a year ago



50.000,- €

[2/9] A view shows the Jomo Kenyatta International Airport toll station on the Nairobi Expressway undertaken by the China Road and Bridge Corporation (CRBC) on a public-private partnership (PPP) basis, along Mombasa road in Embakasi district of Nairobi, Kenya May 7, 2023. REUTERS/Thomas Mukoya/File Photo [Purchase Licensing Rights](#)

### Summary

- Cyber spies infiltrated Kenyan networks from 2019
- Hit finance ministry, president's office, spy agency and others
- Sources believe Beijing was seeking info on debt

NAIROBI, May 24 (Reuters) - Chinese hackers targeted Kenya's government in a widespread, years-long series of digital intrusions against key ministries and state institutions, according to three sources,

# Hacking als Einnahmequelle für Staaten

North Korea was floundering under sanctions. Now it's making billions from stolen cryptocurrency

By Matt Bevan and Yasmin Parry for If You're Listening

Cryptocurrency

Fri 17 Nov



Es gibt kein „zu klein, um gehackt zu werden“ mehr!



# Zitat eines IT-Verantwortlichen:

Nein, einen täglichen Schwachstellenscan **will ich nicht**.  
Ich habe sowieso kein Personal, und wenn wir Kenntnis von  
einer Schwachstelle haben, und die ignorieren...

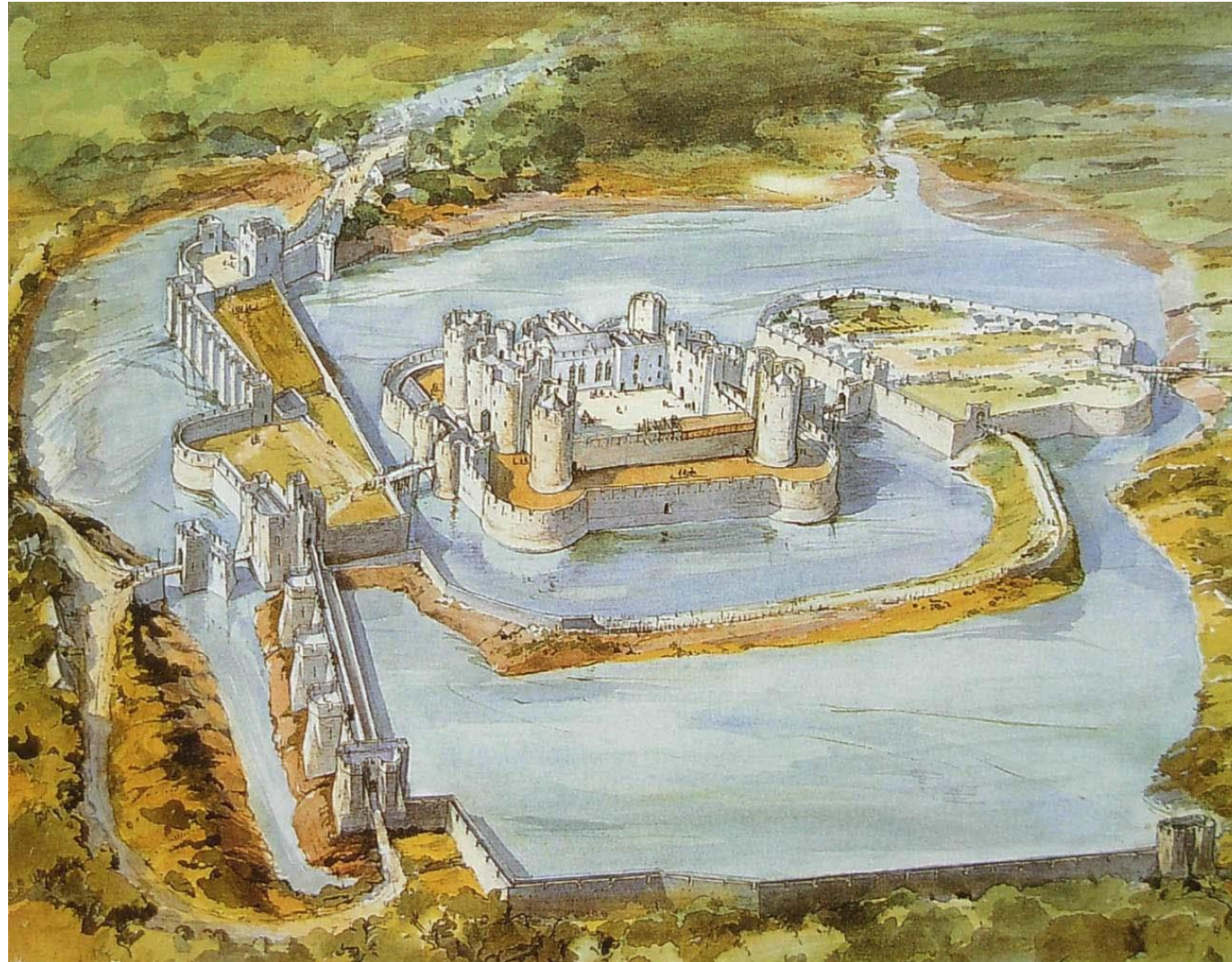
Ich meine, wenn es uns erwischt, und wir wussten nicht,  
dass diese Schwachstelle existierte, **das ist ja was  
anderes...**



# Was also tun? Mindset ändern!



# One Size fits all? Nicht mal im Mittelalter!



Man muss nicht alte Grundsätze  
über Bord werfen – aber man  
sollte sie hinterfragen!

Unbequeme Tatsachen

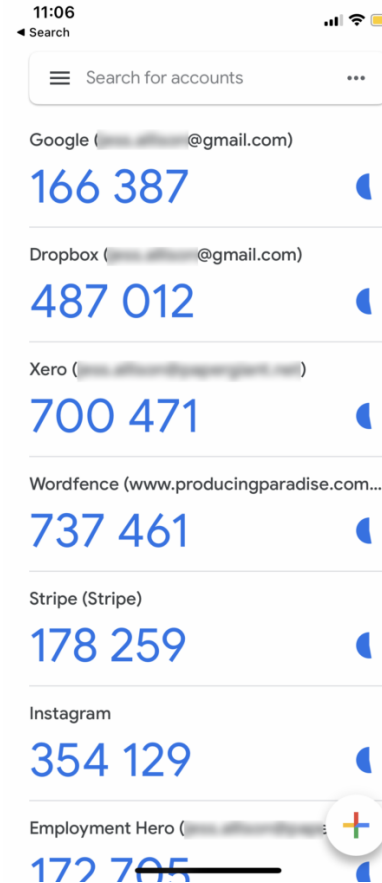
# 1. Ein Cyberangriff ist unausweichlich

- 12% aller Mitarbeiter klicken Phishing-Links an – Ihre auch!
- Schulen Sie sie! Kontinuierlich, nicht 1x im Jahr!
- Binden Sie Ihre Mitarbeiter in die Verteidigung ein!



## 2. Sicherheit funktioniert nur, wenn sie einfach ist

- Einfacher Lösungen = bessere Compliance
- 2FA
- Passworttresore





# 3. Kein Mensch liest alle Logs

- Selbst ein kleines Netzwerk erzeugt leicht mehrere Millionen Logeinträge täglich
- Manuelle Kontrolle ist nicht leistbar
- Automatisierung wird benötigt, i.d.R. von KI unterstützt

# 4. Ohne Backup können Sie zusperrten

- Die Daten sollten mindestens
  - 3 Sicherungen der gleichen Daten umfassen
  - auf 2 verschiedenen Medien
  - mit 1 Kopie an einem anderen Ort
- Erhält ein Angreifer Zugriff auf Ihr Backup, ist es nicht mehr Ihr Backup
  - → Integrität ?
  - → Funktionsfähigkeit?

# 5. Sie benötigen einen getesteten Notfallplan

- Wann? Wenn Sie keinen haben: jetzt!
- Testen Sie den Notfallplan und staunen Sie
- Machen sie ihn offline verfügbar und drucken Sie ihn aus – man weiß ja nie...



# Kontakt

Mail: [jens.hildenbeutel@4s-ag.de](mailto:jens.hildenbeutel@4s-ag.de)

Tel: 01761 13033632

[www.4s-ag.de](http://www.4s-ag.de)