

Erfahrungen aus Security Audits



Sandro Müller
CEO



Mein erstes Audit



Mein erstes Audit

Die Ursache für den Millionenschaden



05. August 2022

**Angriffsziel deutsche
Wirtschaft: mehr als 220
Milliarden Euro Schaden
pro Jahr**

Quellen: <https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr>

Unser Alltag

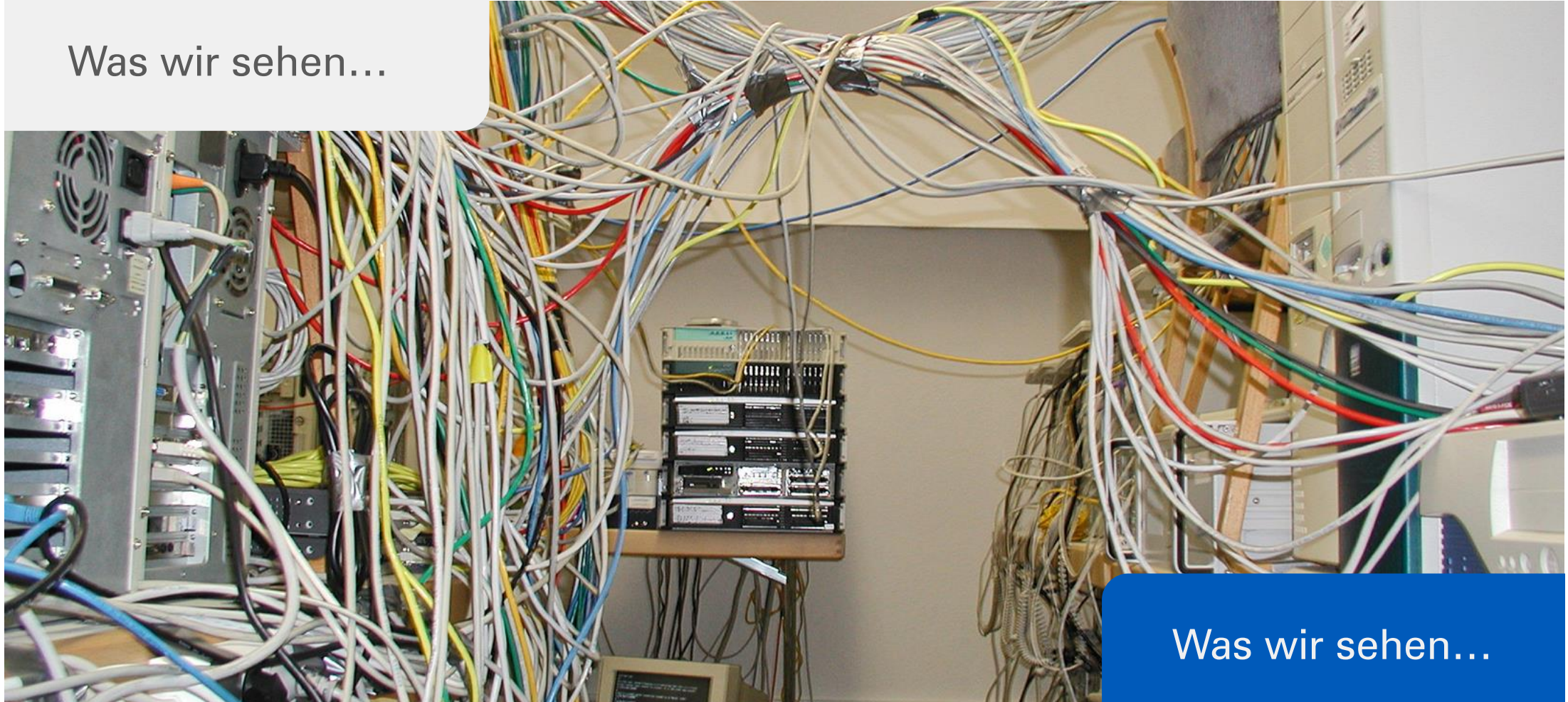
Was man uns erzählt...



Was man uns erzählt...

Unser Alltag

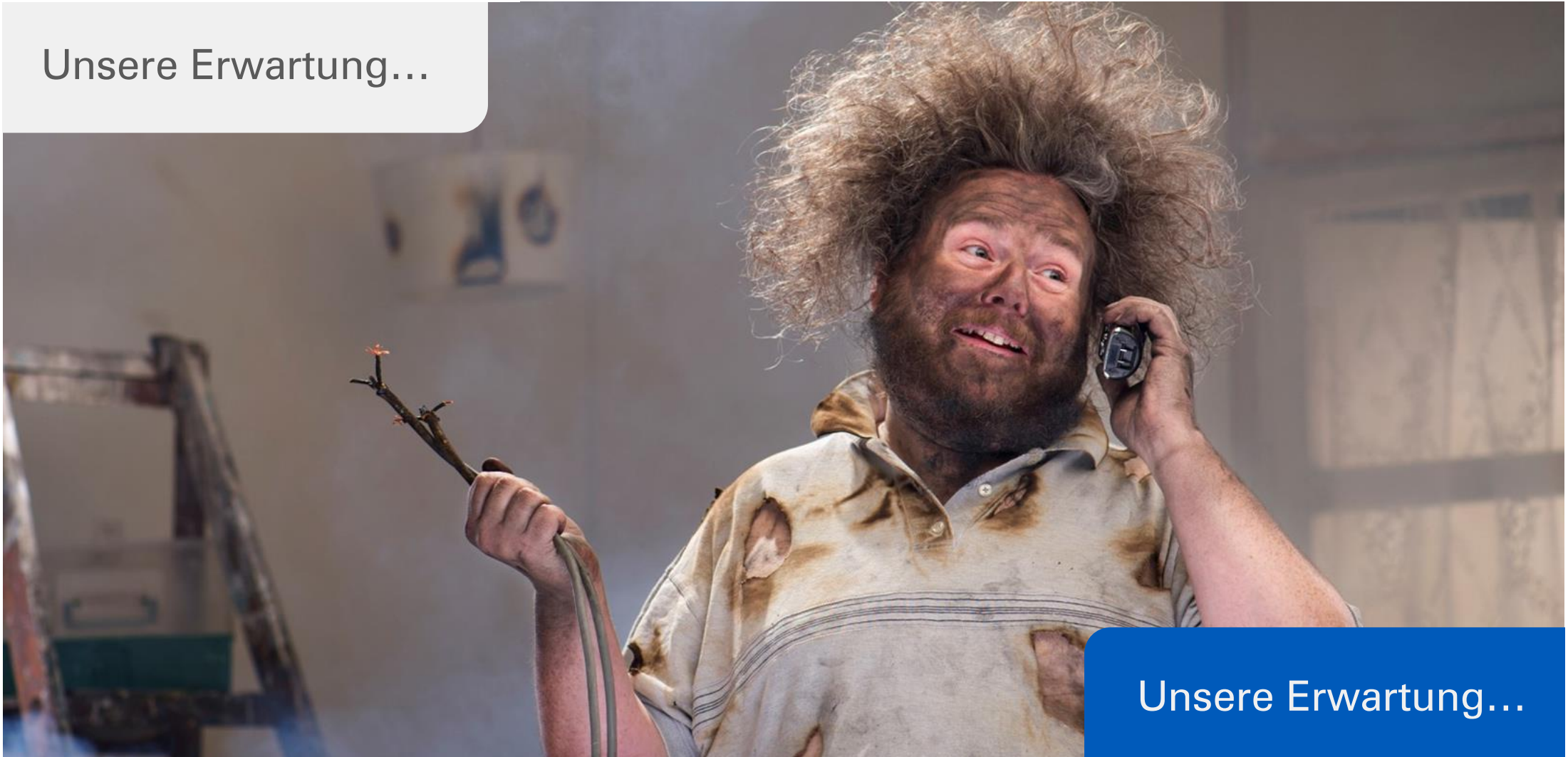
Was wir sehen...



Was wir sehen...

Unser Alltag

Unsere Erwartung...



Unsere Erwartung...

- ☐ 20% der Serverräume sind per se ungeeignet
- ☐ 20% haben Antivirus nicht im Griff
- ☐ 50% haben Patchen nicht im Griff
- ☐ 80% haben die USV nie adäquat getestet
- ☐ 60% haben die Systeme nicht richtig gehärtet (sicher konfiguriert)
- ☐ 70% der User wurden noch nie geschult
- ☐ 80% vergeben zu hohe Berechtigungen (z.B. Service Accounts)
- ☐ 90% Haben Ihr Backup nicht getestet (20% massive Fehler)

Geschätzte Zahlen auf Basis der durch goSecurity durchgeführten Audits

Im Dschungel...



Im Dschungel...

Dschungel – Expedition

Unerwartete Schwierigkeiten...



- ☐ 20% der Serverräume sind per se ungeeignet
- ☐ 20% haben Antivirus nicht im Griff
- ☐ 50% haben Patchen nicht im Griff
- ☐ 80% haben die USV nie adäquat getestet
- ☐ 60% haben die Systeme nicht richtig gehärtet (sicher konfiguriert)
- ☒ 70% der User wurden noch nie geschult
- ☒ 80% vergeben zu hohe Berechtigungen (z.B. Service Accounts)
- ☒ 90% Haben Ihr Backup nicht getestet (20% massive Fehler)

Geschätzte Zahlen auf Basis der durch goSecurity durchgeführten Audits

Warum die Schulung von Usern so schwierig ist...

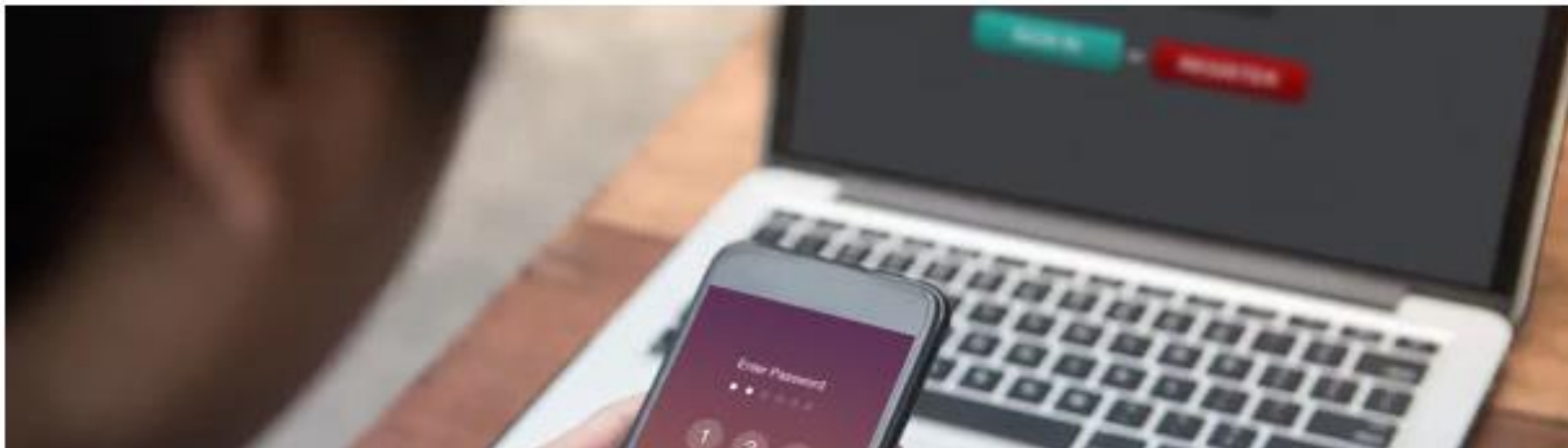


Passwörter: 64 Prozent der User verwenden Kennwörter mehrmals

Eine Umfrage unter 3750 Angestellten auch aus deutschen Organisationen fördert bedenkliche Passwortnutzung zutage. Und das trotz besseren Wissens.

Lesezeit: 3 Min.  In Pocket speichern

   69



Anzahl Stellen	Beispiel	Knacken
6	L-H2i)	< 1 Minute
7	:8B42tX	2 Minuten
8	mW*9=y%1	1-2 Stunden
9	<r+uF50/q	Mehrere Tage
10	9?s}2Kt6C4	Ca. 1-5 Jahre
11	-7\$gL@0Pat5	> 10 Jahre
12	8#h;71GeB/)2	> 100 Jahre

Passwörter Praxis - DEMO

Maximillian1999*

Beatboxer%12

8952_Schlieren

Schneeflocke2019:)

Drei Möglichkeiten zum Domänen-Administrator

Scheduled Task



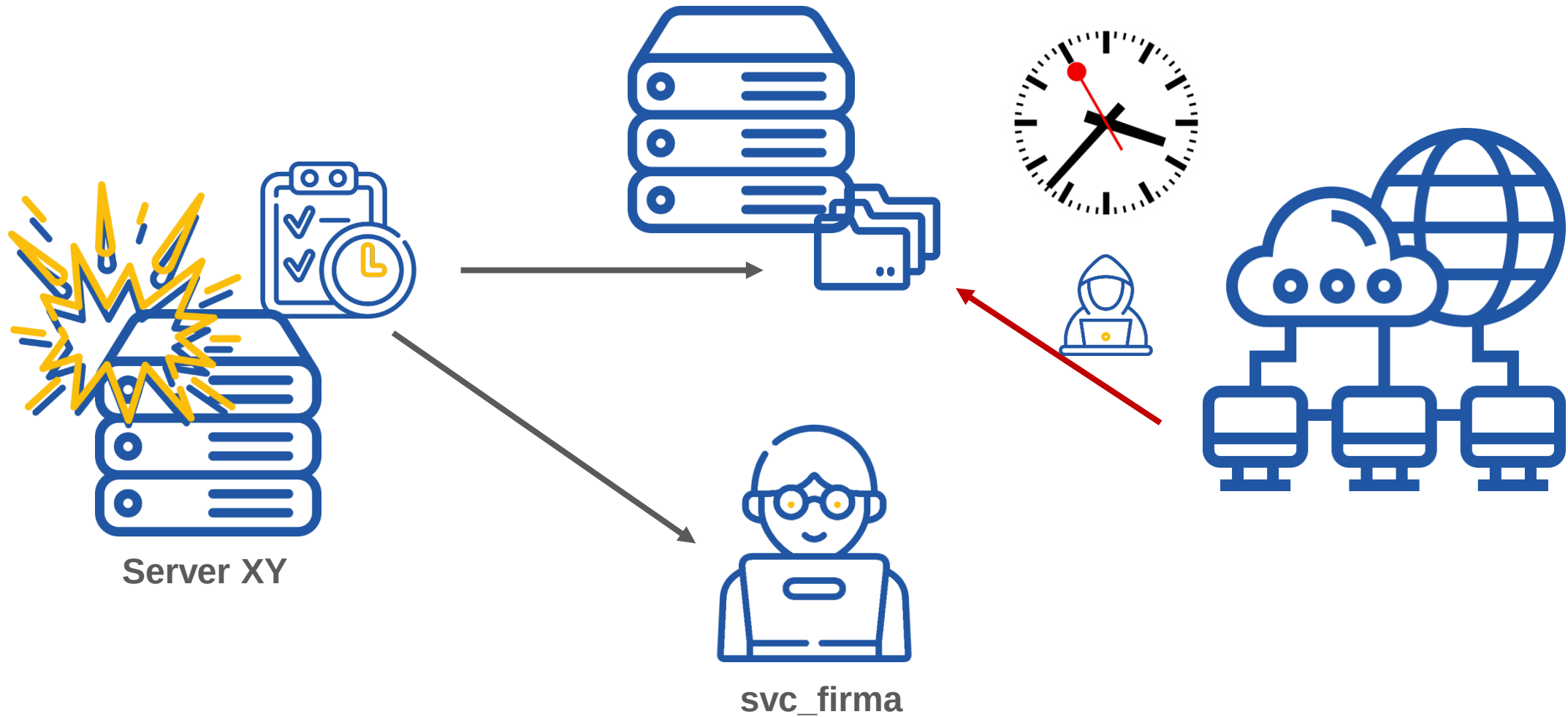
Passwörter in Scripts



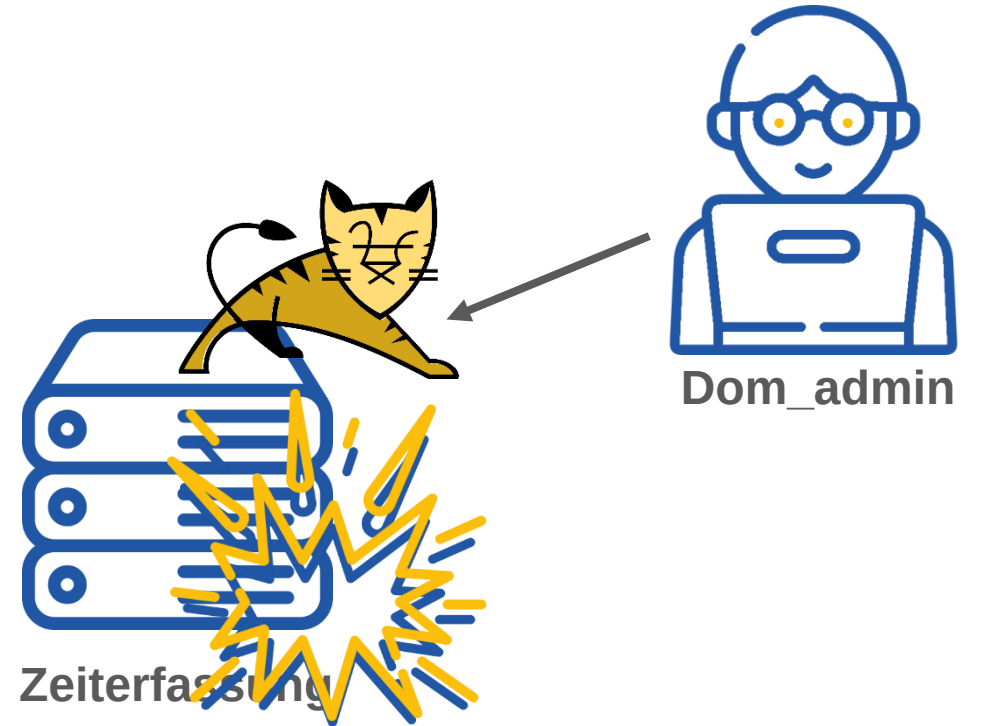
Patchen



Scheduled Tasks



Patchen



- ☐ Daten werden konzeptlos gesichert...
 - Muss ich wirklich ein Konzept erstellen?
- ☐ Auslagerung vs. Offline
 - Offline Backup ist doch von 1980
- ☐ Backups übers Kreuz (z.B. File-Systeme)
- ☐ Restore Test

Backup in der Cloud (SaaS)

- ☐ Der Tool-Anbieter macht auch die Backups
- ☐ Es gibt ein ausführliches SLA
- ☐ Was ist wenn im Fall der Fälle
 - Die Daten inkonsistent sind? / Der Restore nicht funktioniert?
 - Das Backup nicht vorhanden ist (z.B. Brand)?
 - Die Backups auch verschlüsselt sind?
 - Eine Behörde den Cloudanbieter blockiert?
 - Der Cloud-Anbieter insolvent ist?



Mit der IT-Security ist es wie mit der Gesundheit. Sie wird erst dann wichtig, wenn ich sie verloren habe. Und habe ich sie zurück, dann wird Sie jeden Tag wieder etwas weniger wichtig...

Sandro Müller
CEO, goSecurity AG

Danke für Ihre
Aufmerksamkeit



Sandro Müller
CEO



Angriffslustig

IT-Sicherheit für Dein Unternehmen



Ein kostenloser Service
der goSecurity AG

www.angriffslustig.ch

- ☐ **Spotify:** <https://open.spotify.com/show/2IDdpQ5y6Z7zCd7qiSxgT0>
- ☐ **Apple:** <https://podcasts.apple.com/podcast/id1503181480>
- ☐ **Google:** <https://www.youtube.com/user/anwi9/videos>