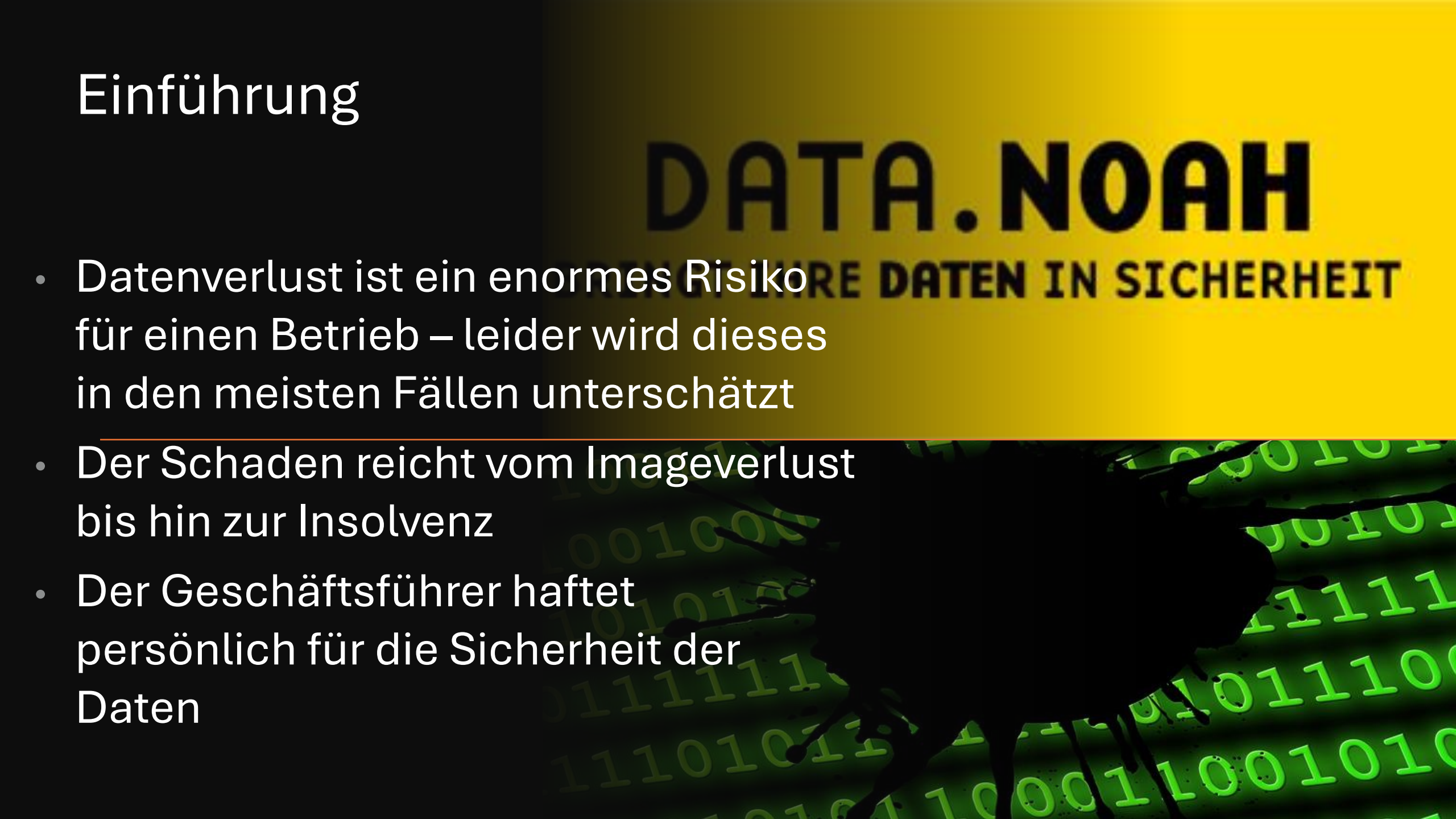
Alarmstufe Datenverlust.....

DATA.NOAH
BRINGT IHRE DATEN IN SICHERHEIT

Christoph Woisetschläger

TAXPO 25

Einführung



- Datenverlust ist ein enormes Risiko für einen Betrieb – leider wird dieses in den meisten Fällen unterschätzt
- Der Schaden reicht vom Imageverlust bis hin zur Insolvenz
- Der Geschäftsführer haftet persönlich für die Sicherheit der Daten

Datenverlust – die häufigsten Ursachen

- Unbeabsichtigtes Löschen
- Unbeabsichtigtes Überschreiben
- Technischer Defekt
- Brand
- Wassereintritt
- Diebstahl
- Viren
- Cyberangriffe / Cyberangriffe as a Service

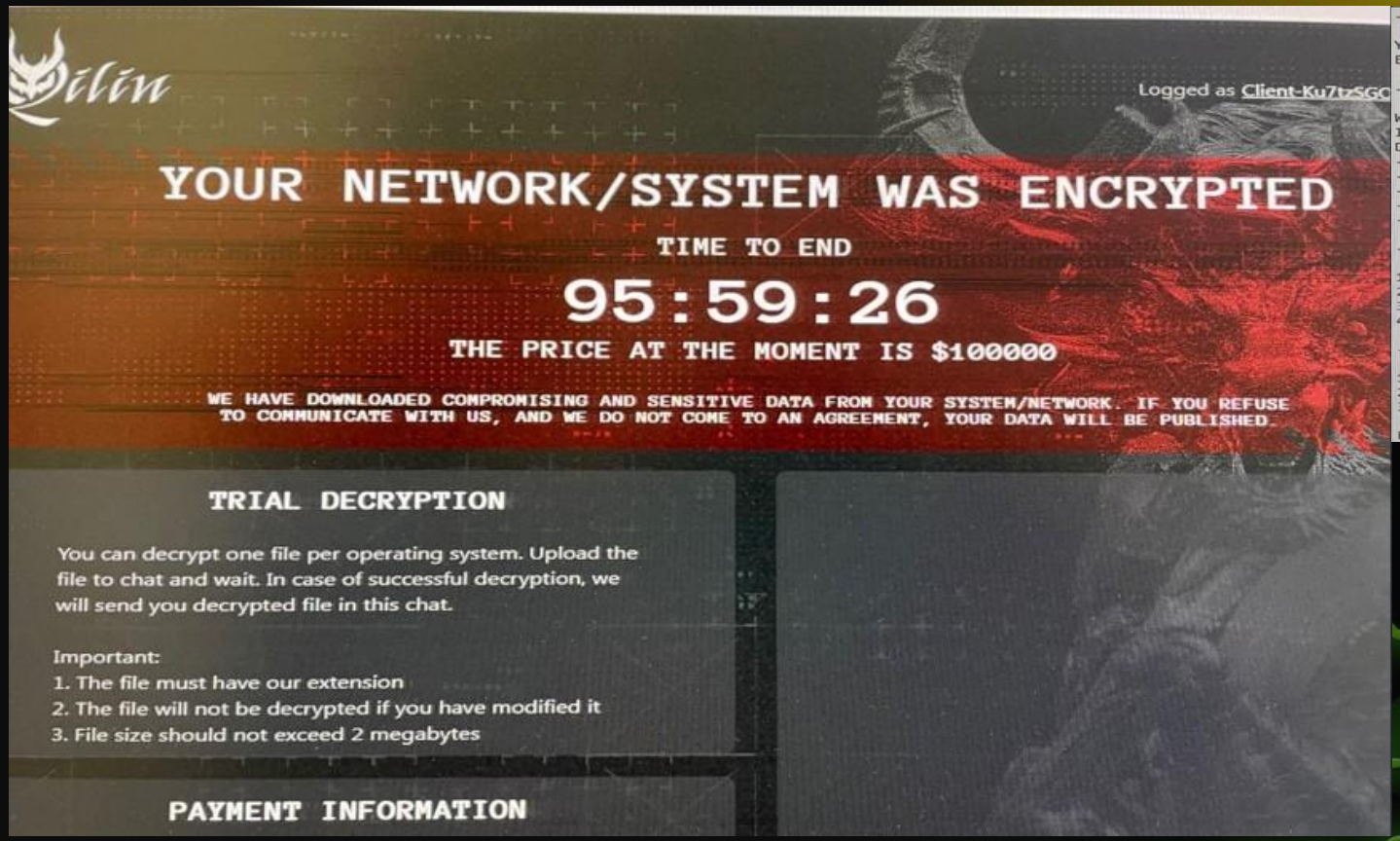
Cyberangriffe

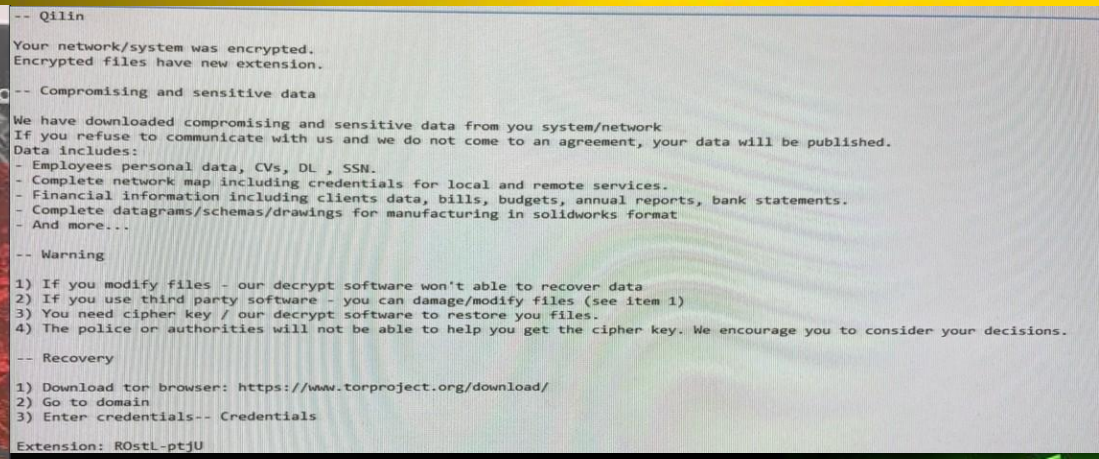
- Erste nennenswerte Angriffe ca. im Jahr 2011 (damals auf Infrastruktur von Telekommunikationsanbietern)
- Im österreichischen KMU Sektor stiegen die Zahlen seit 2015 langsam an
- Massiver Anstieg im Jahr 2020
- 80% der KMUs waren schon Opfer eines Cyberangriffes, ca. 16% sind erfolgreich

Cyberangriffe

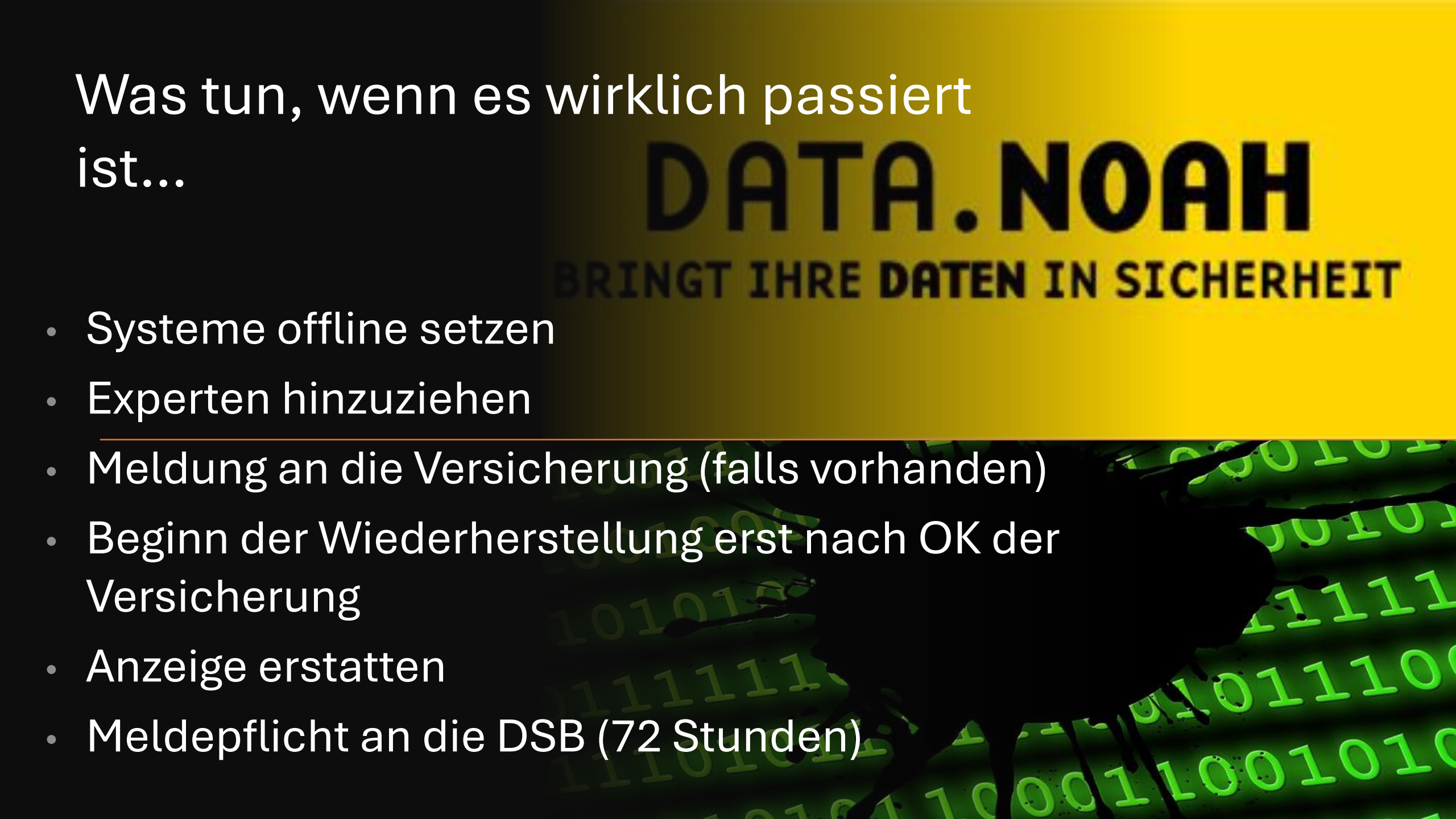
DATA.NOAH

BRINGT IHRE DATEN IN SICHERHEIT



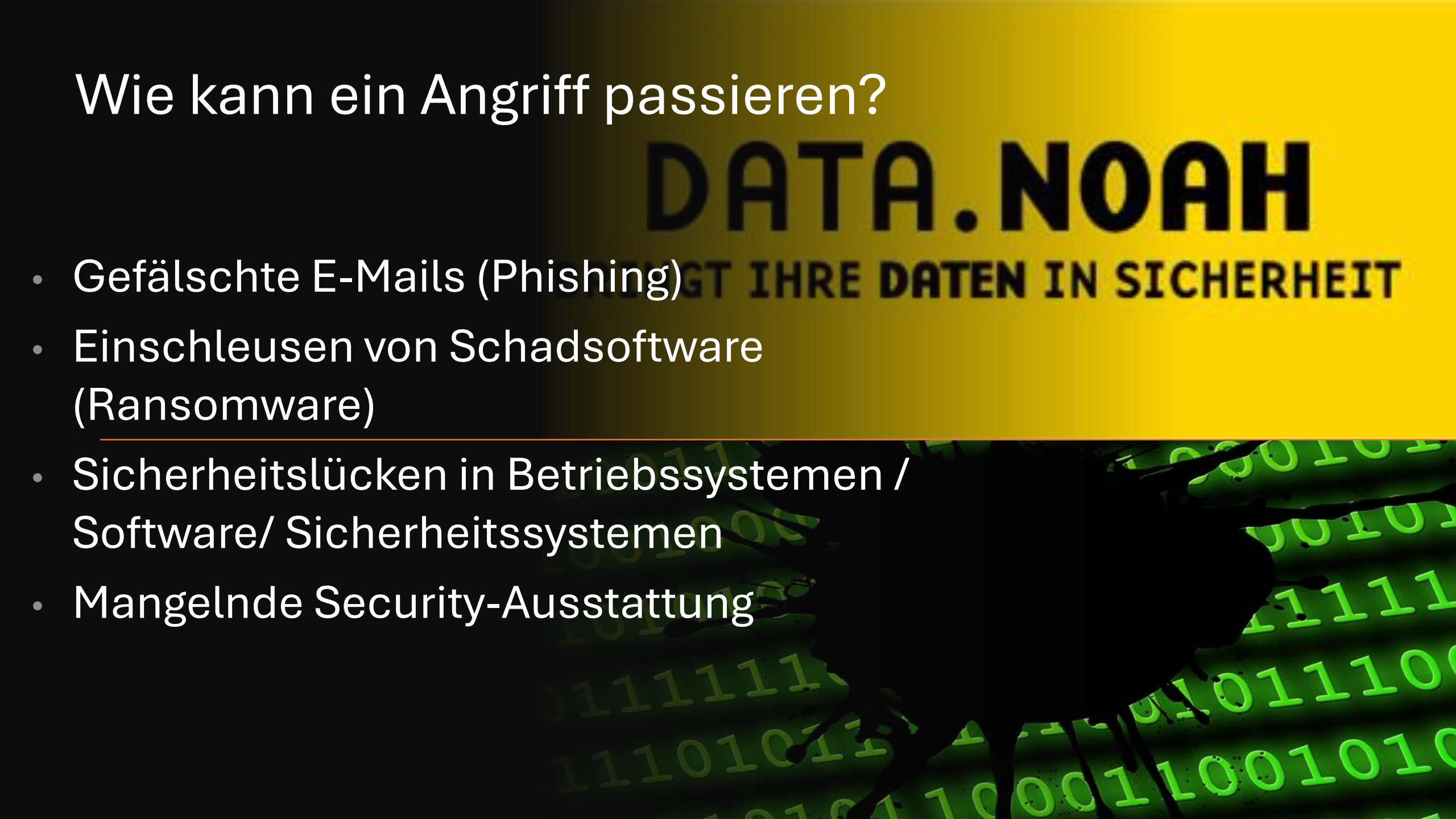


Was tun, wenn es wirklich passiert ist…



- Systeme offline setzen
- Experten hinzuziehen
- Meldung an die Versicherung (falls vorhanden)
- Beginn der Wiederherstellung erst nach OK der Versicherung
- Anzeige erstatten
- Meldepflicht an die DSB (72 Stunden)

Wie kann ein Angriff passieren?



- Gefälschte E-Mails (Phishing)
- Einschleusen von Schadsoftware (Ransomware)
- Sicherheitslücken in Betriebssystemen / Software/ Sicherheitssystemen
- Mangelnde Security-Ausstattung

Log Details

General

Absolute Date/Time	2025-10-20
Last Access Time	11:53:59
VDOM	root
Log Description	SSL VPN login fail

Source

Source Country/Region	Singapore
User	ashleys
Group	N/A

Destination

Destination Host	N/A

Action

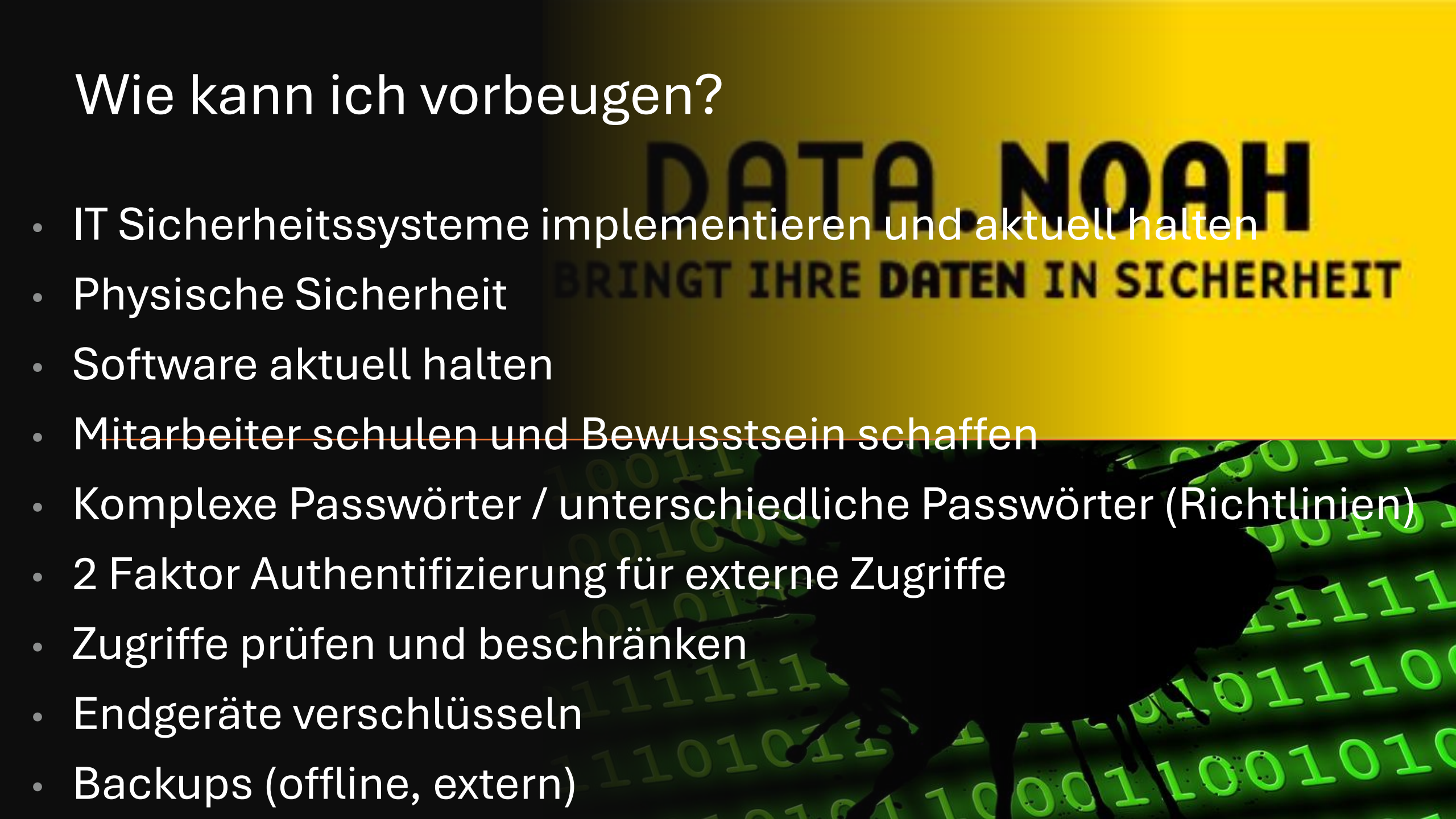
Action	ssl-login-fail
Reason	sslvpn_login_unknown_user

Security

Level	Alert Notification

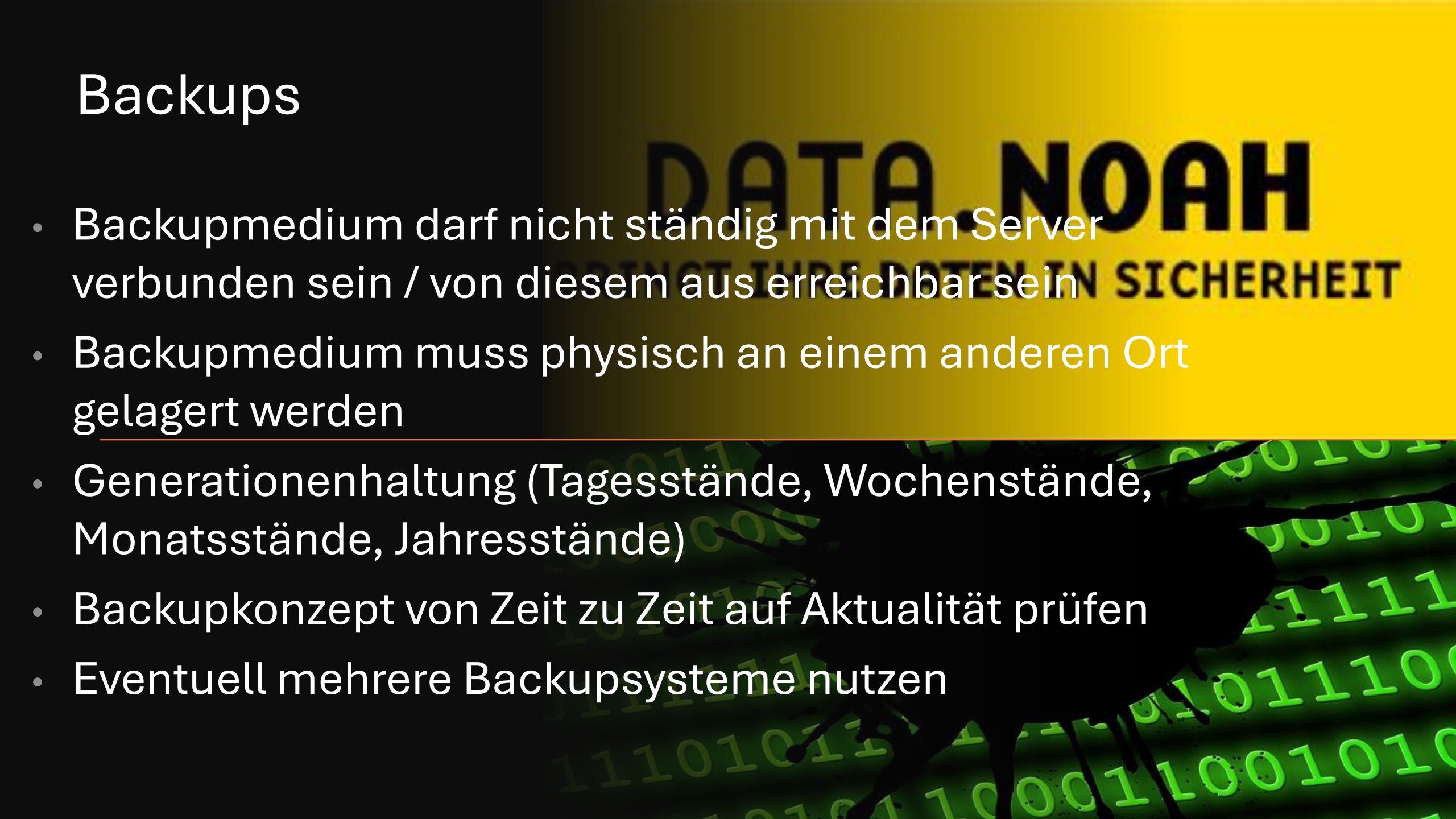
2025/10/20 11:52:32	Alert Notification	admin	Administrator admin login failed from https(178.22.24.15) because of blocked IP	Admin login failed
2025/10/20 11:52:29	Alert Notification	lohadmin	Administrator lohadmin login failed from https(217.119.139.52) because of invalid u...	Admin login failed
2025/10/20 11:52:23	Alert Notification	unknown	Administrator unknown login failed from https(217.119.139.51) because of an inter...	Admin login failed
2025/10/20 11:52:15	Alert Notification	unknown	Administrator unknown login failed from https(217.119.139.48) because of an inter...	Admin login failed
2025/10/20 11:51:42	Alert Notification	adminlve	Administrator adminlve login failed from https(217.119.139.49) because of invalid u...	Admin login failed
2025/10/20 11:51:32	Alert Notification	ruadmin	Administrator ruadmin login failed from https(217.119.139.41) because of invalid us...	Admin login failed
2025/10/20 11:51:19	Notice		Performance statistics: average CPU: 0, memory: 55, concurrent sessions: 130, setup...	System performance statistics
2025/10/20 11:50:32	Alert Notification	admin	Administrator admin login failed from https(178.22.24.29) because of blocked IP	Admin login failed
2025/10/20 11:50:16	Alert Notification	adminu	Administrator adminu login failed from https(217.119.139.40) because of invalid use...	Admin login failed
2025/10/20 11:49:54	Alert Notification	admin	Administrator admin login failed from https(77.90.185.143) because of blocked IP	Admin login failed
2025/10/20 11:49:43	Alert Notification	unknown	Administrator unknown login failed from https(217.119.139.51) because of an inter...	Admin login failed
2025/10/20 11:49:41	Alert Notification	unknown	Administrator unknown login failed from https(217.119.139.48) because of an inter...	Admin login failed
2025/10/20 11:49:37	Alert Notification	admin	Administrator admin login failed from https(178.22.24.30) because of blocked IP	Admin login failed
2025/10/20 11:49:24	Alert Notification	logadmin	Administrator logadmin login failed from https(217.119.139.52) because of invalid u...	Admin login failed
2025/10/20 11:48:56	Alert Notification	admin	Administrator admin login failed from https(178.22.24.15) because of blocked IP	Admin login failed
2025/10/20 11:48:40	Alert Notification	adminlve	Administrator adminlve login failed from https(217.119.139.49) because of invalid u...	Admin login failed
2025/10/20 11:47:21	Alert Notification	admin	Administrator admin login failed from https(178.22.24.61) because of blocked IP	Admin login failed
2025/10/20 11:46:56	Alert Notification	unknown	Administrator unknown login failed from https(217.119.139.51) because of an inter...	Admin login failed
2025/10/20 11:46:46	Alert Notification	unknown	Administrator unknown login failed from https(217.119.139.48) because of an inter...	Admin login failed

Wie kann ich vorbeugen?



- IT Sicherheitssysteme implementieren und aktuell halten
- Physische Sicherheit
- Software aktuell halten
- Mitarbeiter schulen und Bewusstsein schaffen
- Komplexe Passwörter / unterschiedliche Passwörter (Richtlinien)
- 2 Faktor Authentifizierung für externe Zugriffe
- Zugriffe prüfen und beschränken
- Endgeräte verschlüsseln
- Backups (offline, extern)

Backups



- Backupmedium darf nicht ständig mit dem Server verbunden sein / von diesem aus erreichbar sein
- Backupmedium muss physisch an einem anderen Ort gelagert werden
- Generationenhaltung (Tagesstände, Wochenstände, Monatsstände, Jahresstände)
- Backupkonzept von Zeit zu Zeit auf Aktualität prüfen
- Eventuell mehrere Backupsysteme nutzen

Nützliche Plattformen:

- cert.at (Computer Emergency Response Team Austria) - Warningliste sehr empfehlenswert!
- haveibeenpwned.com
- bundeskanzleramt.gv.at/themen/cybersicherheit.html

DATA.NOAH

BRINGT IHRE DATEN IN SICHERHEIT

Einen 100%igen Schutz gibt es nicht!

Danke!