

Alarmstufe Datenverlust....

Christoph Woisetschläger

DATA.NOAH
BRINGT IHRE DATEN IN SICHERHEIT

TAXPO
25



Einführung

DATA.NOAH

BRING YOUR DATEN IN SICHERHEIT

- 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

DATA.NOAH

BRINGT IHRE DATEN IN SICHERHEIT

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

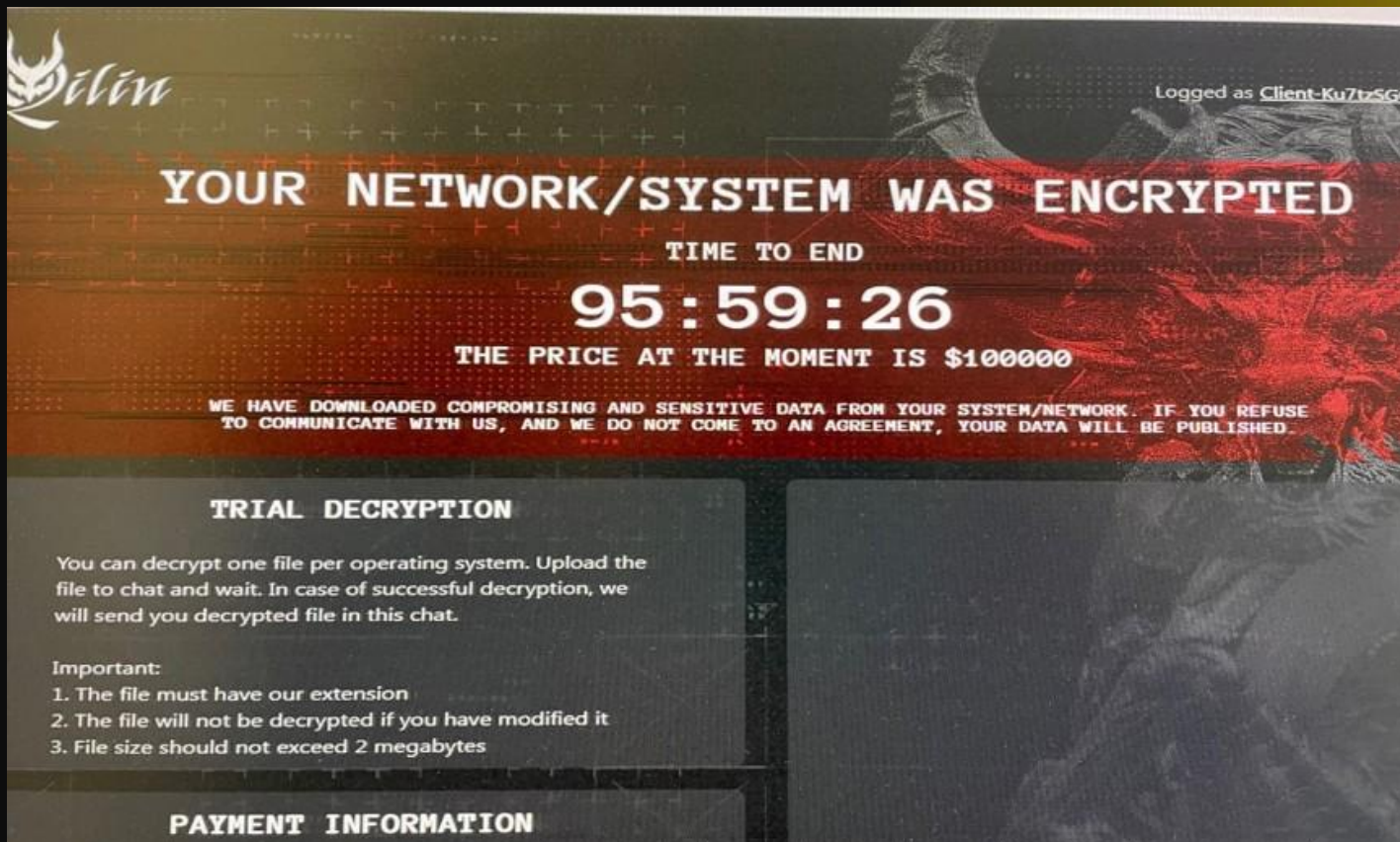


Cyberangriffe

- 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



Qilin

Logged as Client-Ku7bSG0

YOUR NETWORK/SYSTEM WAS ENCRYPTED

TIME TO END
95:59:26
THE PRICE AT THE MOMENT IS \$100000

WE HAVE DOWNLOADED COMPROMISING AND SENSITIVE DATA FROM YOUR SYSTEM/NETWORK. IF YOU REFUSE TO COMMUNICATE WITH US, AND WE DO NOT COME TO AN AGREEMENT, YOUR DATA WILL BE PUBLISHED.

TRIAL DECRYPTION

You can decrypt one file per operating system. Upload the file to chat and wait. In case of successful decryption, we will send you decrypted file in this chat.

Important:

1. The file must have our extension
2. The file will not be decrypted if you have modified it
3. File size should not exceed 2 megabytes

PAYMENT INFORMATION

```
-- Qilin
Your network/system was encrypted.
Encrypted files have new extension.

-- Compromising and sensitive data

We have downloaded compromising and sensitive data from you system/network
If you refuse to communicate with us and we do not come to an agreement, your data will be published.
Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...

-- Warning

1) If you modify files - our decrypt software won't able to recover data
2) If you use third party software - you can damage/modify files (see item 1)
3) You need cipher key / our decrypt software to restore you files.
4) The police or authorities will not be able to help you get the cipher key. We encourage you to consider your decisions.

-- Recovery

1) Download tor browser: https://www.torproject.org/download/
2) Go to domain
3) Enter credentials-- Credentials

Extension: R0stl-ptfJU
```



Was tun, wenn es wirklich passiert
ist...

DATA.NOAH

BRINGT IHRE DATEN IN SICHERHEIT

- 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?

DATA.NOAH

- 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

DATA.NOAH

BRINGT IHRE DATEN IN SICHERHEIT

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)

DATA.NOAH

BRINGT IHRE DATEN IN SICHERHEIT

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:

DATA.NOAH
BRINGT IHRE DATEN IN SICHERHEIT

- 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!