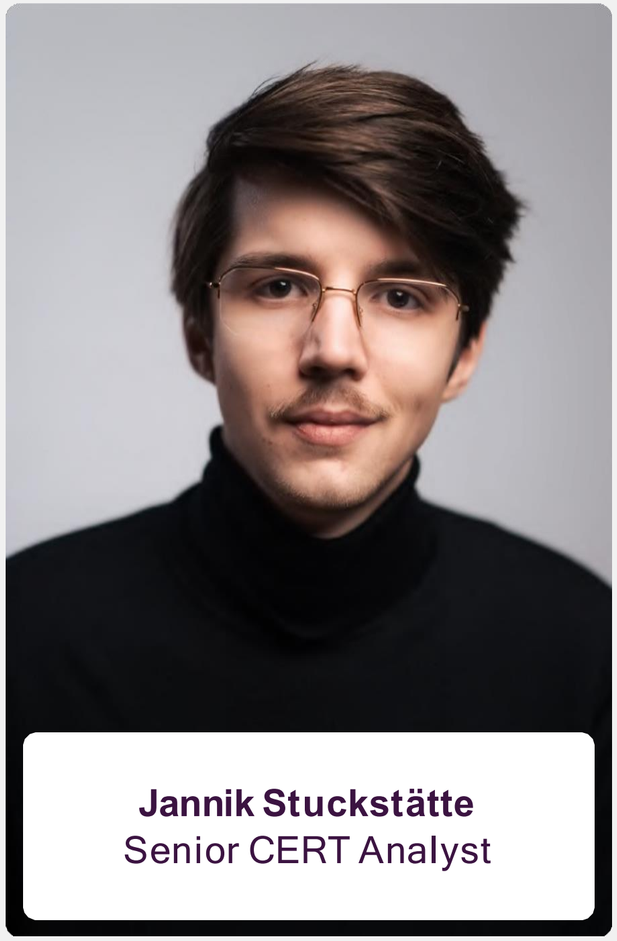
stoïk

Cyber-Krisenmanagement

Schadenkonferenz 2025

19 / 09 / 2025

Ihr Referent heute



Jannik Stuckstätte
Senior CERT Analyst

Führender Cyberassekuradeur für Gewerbe- und Industrieunternehmen

Starkes Wachstum seit 2021

+8000

Unternehmen
versichertundgeschützt

+2000

Partnermakler

7

europäische Länder
eröffnet

+110

Mitarbeitende
in Deutschland, Österreich und Europa

110 Experten, unterstützt von starken institutionellen Partnern

Munich RE

Größter Cyberversicherer der Welt (A+)
Stoïk-Investor seit 2022

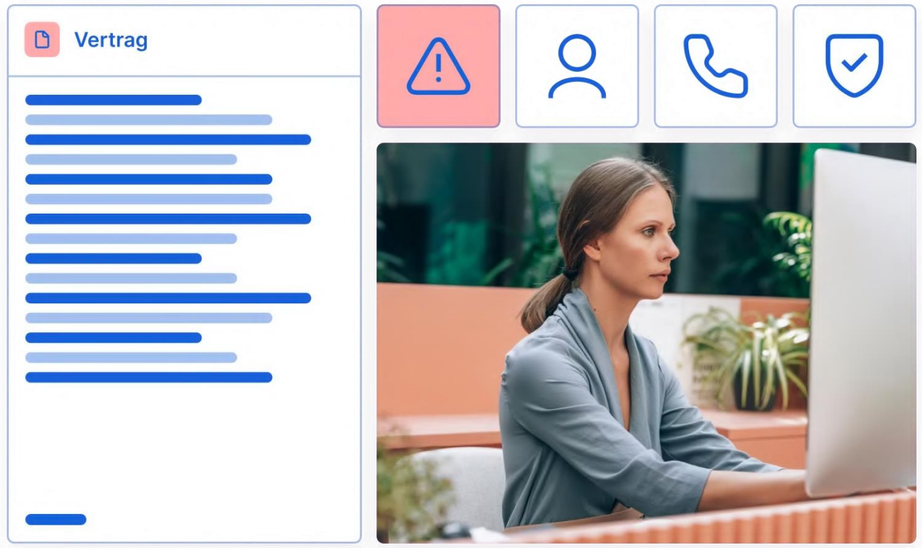
Swiss Re

Zweitgrößter Cyberversicherer der Welt (A+)
Stoïk-Risikoträger seit 2021

TOKIO MARINE HCC

Einer der größten Versicherer der Welt (AA+)
Stoïk-Risikoträger und Investor seit 2023

Ein aktiver Ansatz für ganzheitliches Risikomanagement



1. **Der umfassendste Versicherungsschutz am Markt**
   um Versicherungsnehmer im Angriffsfall zu begleiten und zu entschädigen

2. **Stark vereinfachte Antragsstrecke**
   um Makler zu befähigen alle ihre Kunden optimal abzusichern

3. **Online-Plattform für aktive Prävention**
   kostenlos für alle Versicherungsnehmer

4. **24/7 verfügbare Cyberexperten**
   gewährleisten zu jedem Zeitpunkt effiziente und sofortige Schadenshilfe

5. **Zusätzliche Lösungen für mehr Cybersicherheit**
   um Unternehmen noch effektivere Kontrolle über ihre Risiken zu ermöglichen

Das Stoïk CERT: 100% hausinterne Cyberexpertise

Bei Stoïk stehen IT-Forensiker und Cyberexperten jeden Tag rund um die Uhr zur sofortigen Schadenshilfe bereit.

- **Schnelles und effektives Eingreifen**
  Unsere Experten reagieren durchschnittlich in weniger als 3 Minuten auf Ihre Anfrage.
- **Schnelle und sichere Wiederaufnahme des Geschäftsbetriebs**
  75% unserer Versicherungsnehmer konnten binnen einer Woche nach einem Ransomwareangriff ihre Geschäftstätigkeit wieder aufnehmen.
- **Enge technische Begleitung**
  auch bei Zweifel und kleineren Fällen.
- **Keine versteckten Kosten**
  Transparenter Service ohne zusätzliche Kosten.

Unser ganzheitlicher Ansatz zum Schutz vor Cyberrisiken

Cybersicherheit | **Versicherung**

Stoïk Protect

verringert das Risiko des Eindringens eines potentiellen Angreifers in das Informationssystem.

Stoïk MDR

erkennt automatisch verdächtige Aktivitäten auf den überwachten Endpunkten und macht sie unschädlich.

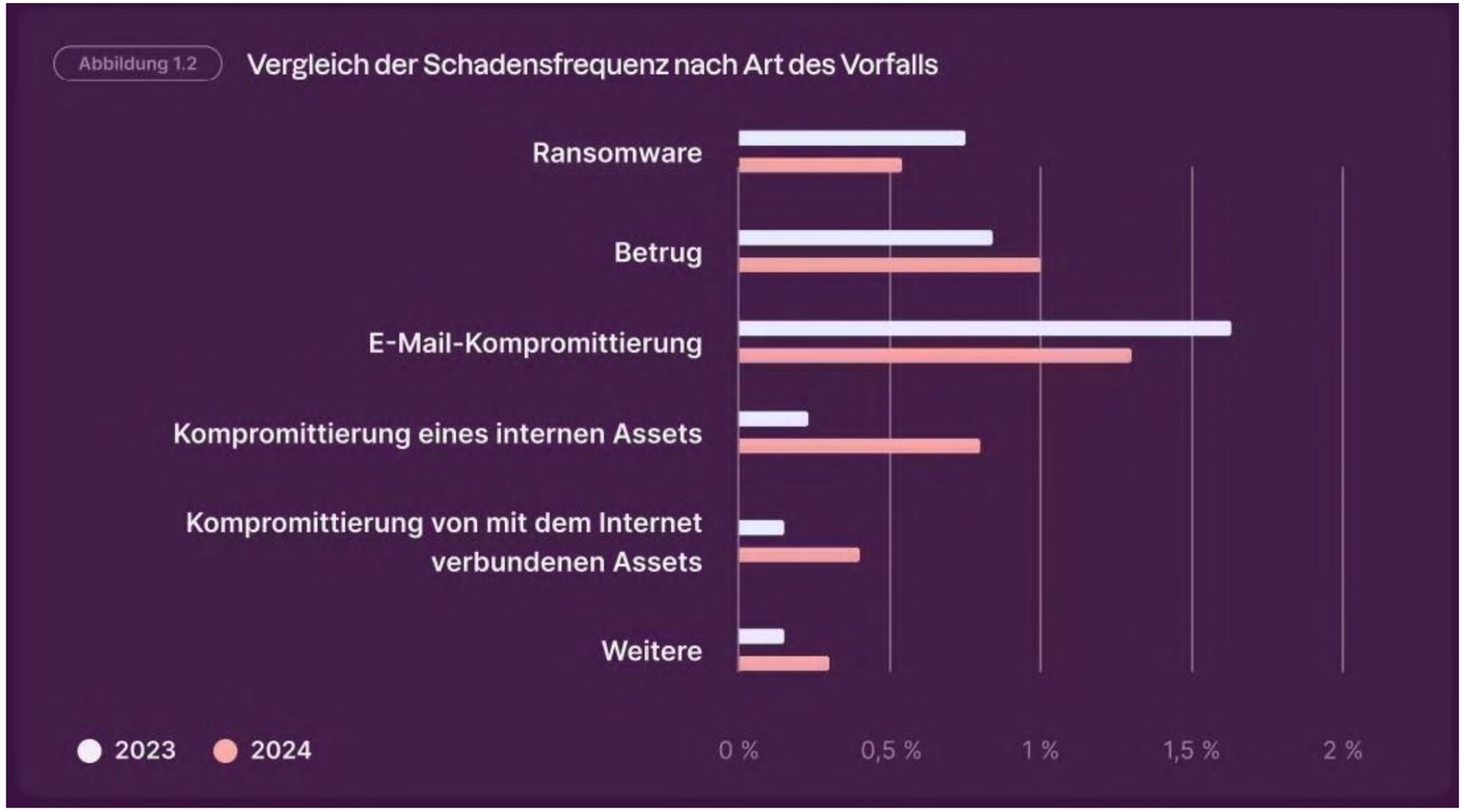
Stoïk CERT

leistet sofortige Schadenshilfe um schnellstmögliche Wiederaufnahme des Betriebs zu gewährleisten.

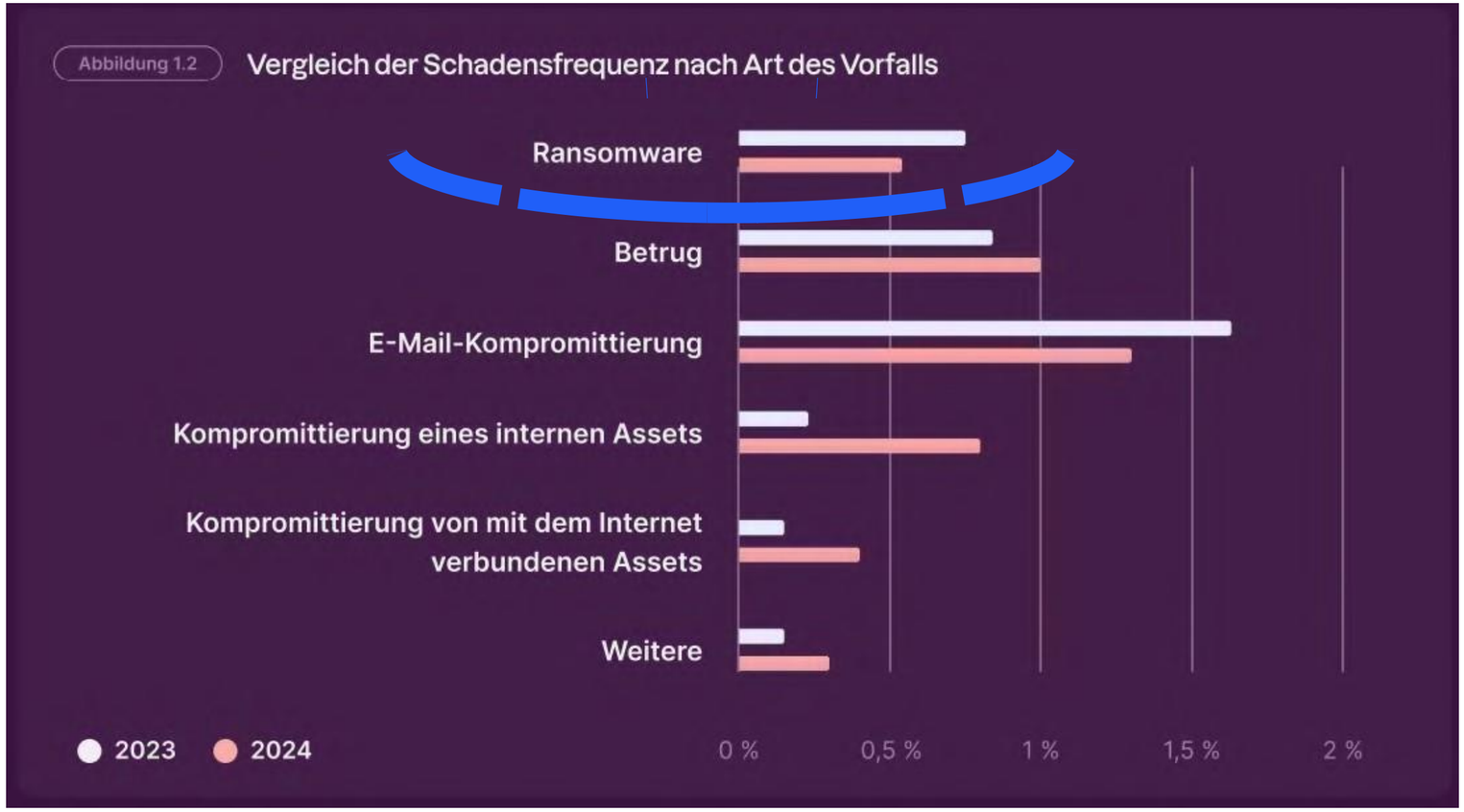
Stoïk Versicherung

deckt Schäden ab, die bei einem Cyberangriff enstehen.

Cyber-Schadensbericht 2024



Cyber-Schadensbericht 2024

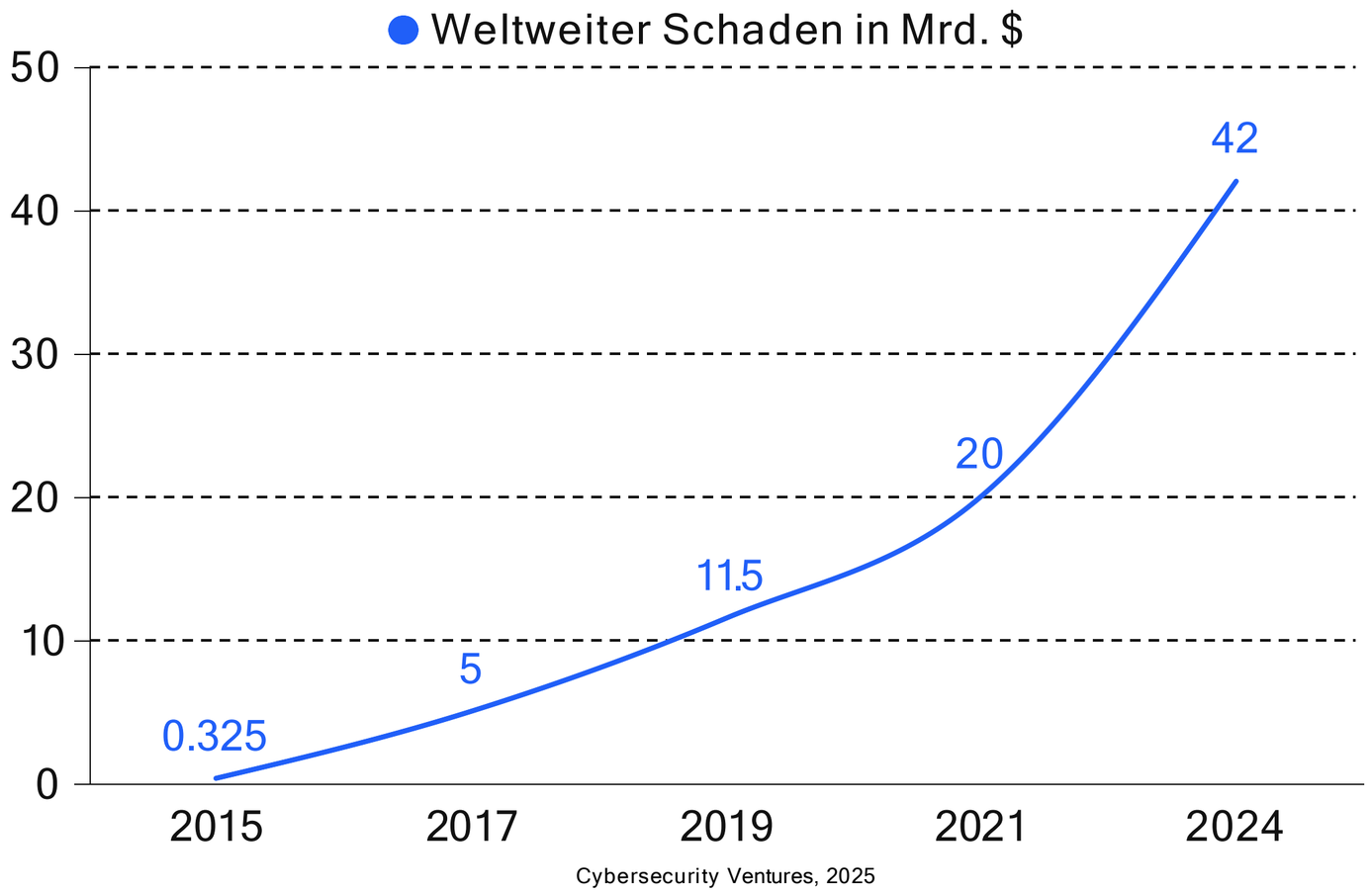


stoïk

Ransomware, die "[...] eine Art von Schadprogrammen, die den Zugriff auf Daten und Systeme einschränken oder unterbinden. Für die Freigabe wird dann ein Lösegeld (englisch: Ransom) verlangt."

BSI, Ransomware - Vorsicht vor Erpressersoftware

Wie Ransomware die Welt veränderte



Cybersecurity Ventures, 2025

178,6 Mrd. € Schaden durch Cyberkriminalität allein in der Deutschen Wirtschaft

Bitkom e.V., Wirtschaftsschutz 2024

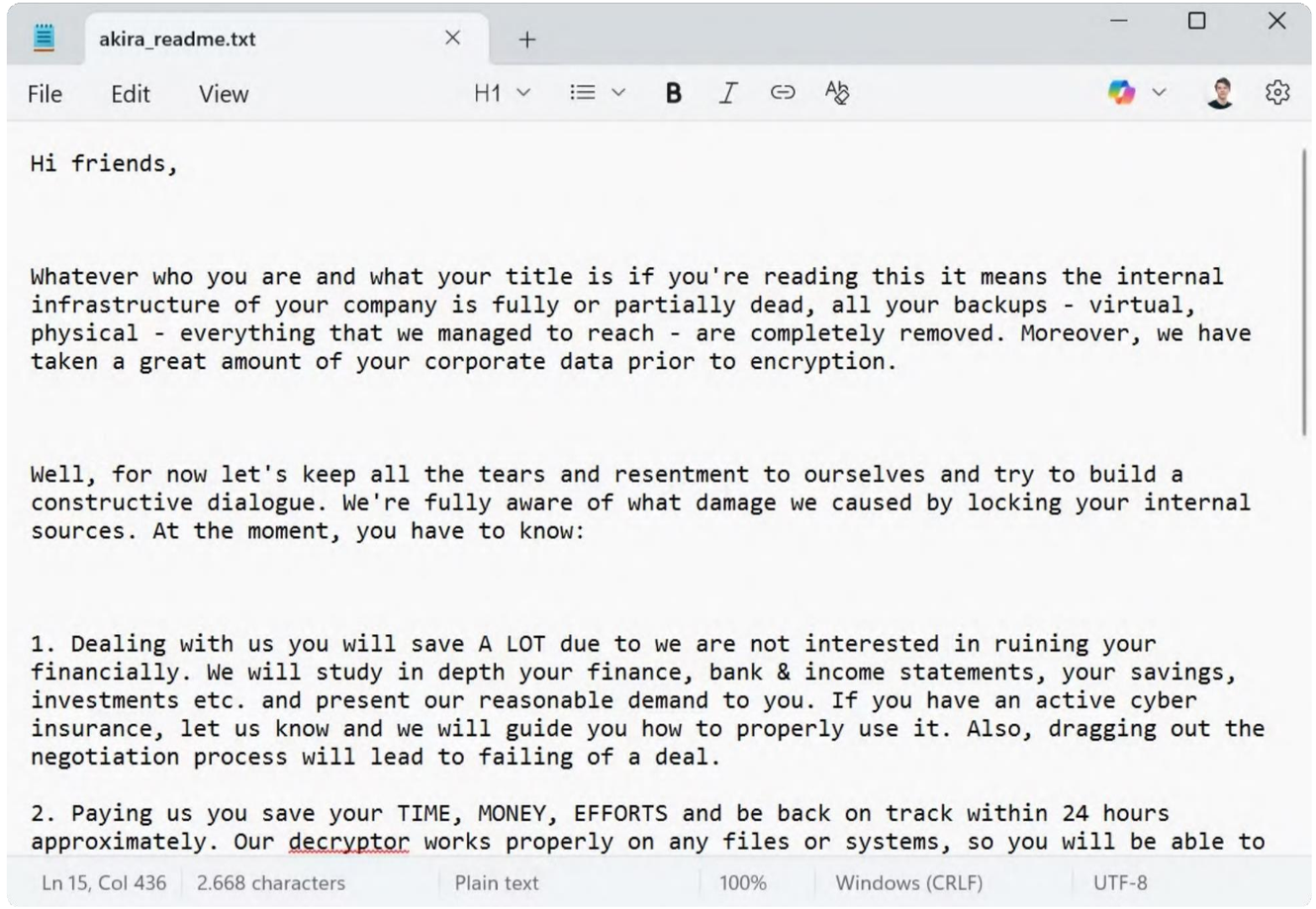
alle 2-3 Tage wurde ein Ransomwarevorfall durch ein österreichisches Unternehmen *angezeigt*

BMI AT, Cybercrime-Report 2023

Der typische Ablauf bei Ransomware

Das Erpresserschreiben am Beispiel "Akira"

akira_readme.txt



akira_readme.txt

File Edit View H1

Hi friends,

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover, we have taken a great amount of your corporate data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal.

2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to

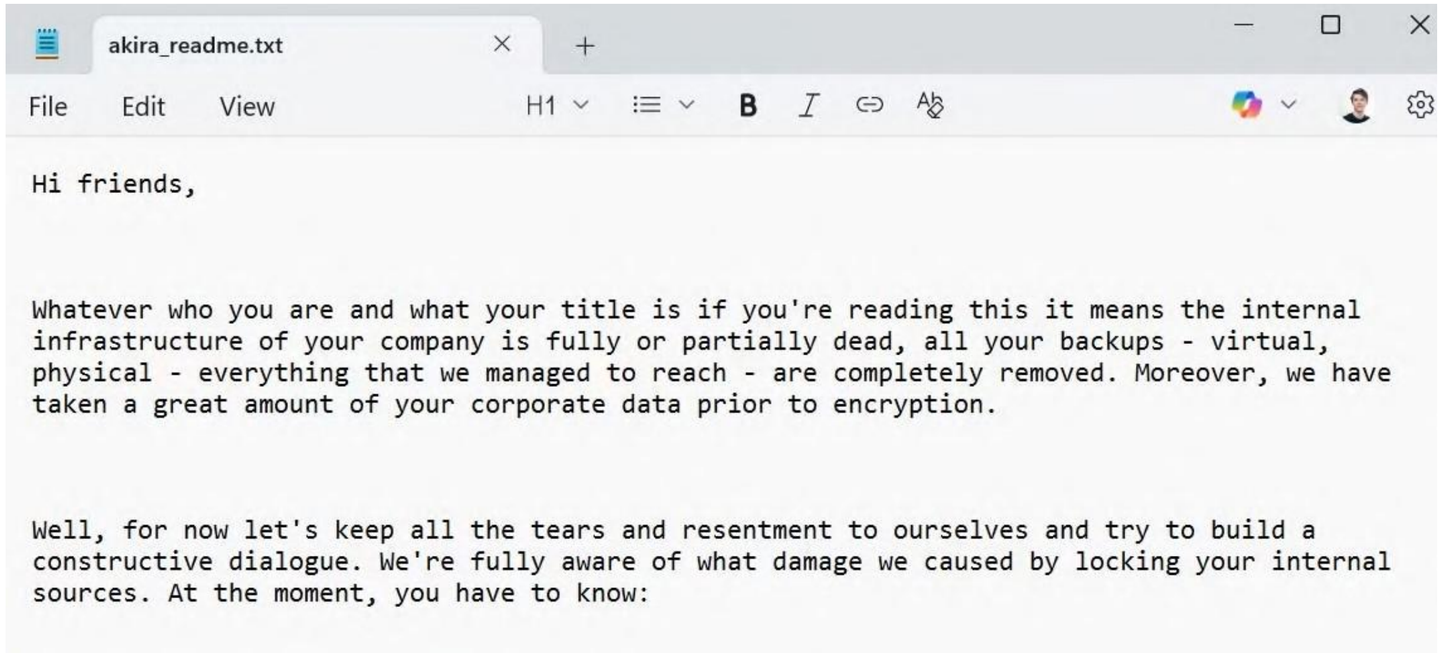
Ln 15, Col 436 | 2.668 characters | Plain text | 100% | Windows (CRLF) | UTF-8

Der typische Ablauf bei Ransomware

Das Erpresserschreiben am Beispiel "Akira"

Markenbildung →

Drohkulisse →



Der typische Ablauf bei Ransomware

Das Erpresserschreiben am Beispiel "Akira"

Vertrauen aufbauen →

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal.

2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to some files or accidently corrupt them - in this case we won't be able to help.

3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload your data.

4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of this will be published in our blog - https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion.

5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

Der typische Ablauf bei Ransomware

Das Erpresserschreiben am Beispiel "Akira"

Kontaktinfos →

```
1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/.

2. Paste this link - https://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.onion.

3. Use this code - [ENTFERNT] - to log into our chat.
```

Die Drohkulisse

- **Verschlüsselung kritischer Daten**
- **Datenabftuss sensibler Daten**
- **Verfügbarkeitsverlust von Diensten (sog. DoS/DDoS)**
- **Nachricht an Kunden, Mitarbeiter oder Behörden**

Die Vorbereitung

Kenne dein Gegenüber

Wer erpresst uns überhaupt?

- Name der Gruppe
- Reputation
- Ort & Art der Datenveröffentlichung
- Wir haben idR. mit sog. "Affiliates" zu tun!
- Typisches Vorgehen ("modus operandi")
  - "TTPs" - Tactics, Techniques & Procedures

Die Angreifertypen

Mitarbeiter

Hacktivists

Organisierte Kriminalität

Staatliche Akteure

Persönliche Motive

Ideologie

Monetärer Gewinn

Spionage/ Destruktion

Nichts läuft mehr, und nu?

Wie entschlüssele ich ein Unternehmen? - Die Theorie

Identifizierung

- Betroffene Geräte / Ressourcen identifzieren

Eindämmung

- Weitere Ausbreitung verhindern

Beseitigung

- Angreifer aus dem Netzwerk aussperren (Zugangspunkte & TTPs!)

Wiederherstellung

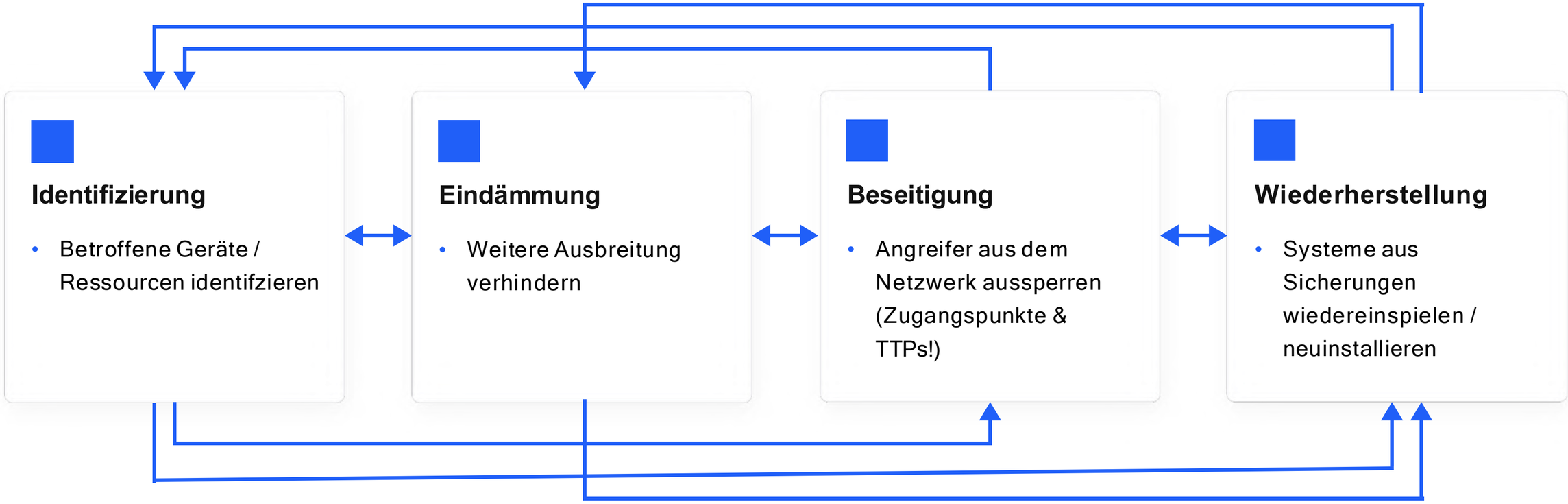
- Systeme aus Sicherungen wiedereinspielen / neuinstallieren

Nichts läuft mehr, und nu?

Wie entschlüssele ich ein Unternehmen? - Die Theorie

Nichts läuft mehr, und nu?

Wie entschlüssele ich ein Unternehmen? - Die Praxis



Nichts läuft mehr, und nu?

Ein Incident betrifft mehr als nur Technik

Weitere Aufgaben:

- Meldung an DS-Behörde (DSB AT) nach Art. 33 DSGVO
  - Binnen 72 Std. nach Erkennung
- Anzeige und Kommunikation mit Strafverfolgung
- Krisenkommunikation mit Kunden, Lieferanten und Geschäftspartnern
- Risikoabschätzung Datenveröffentlichung
  - Benachrichtigung an Betroffene? (Art. 34 DSGVO)
- Prozesse betriebswirtschaftlich priorisieren
  - Notfallhandbuch/Wiederanlaufplan/BCM?
  - Alternativprozesse

Die üblichen Verdächtigen

Wie kommen die Angreifer ins Unternehmen?

Schwache Zugangsdaten und fehlende 2FA/MFA
Angreifer übernehmen das Konto eines Mitarbeiters für die Anmeldung bei einer Fernzugriffslösung (z.B. Firmen-VPN).

Technische Schwachstelle (häufig 0-days)
Angreifer finden eine Schwachstelle in einem weit verbreiteten Produkt und übernehmen das darunter liegende System.

Schadsoftware + Social Engineering
Angreifer bringen einen Mitarbeiter dazu, eine vermeintlich harmlose/bekannte Software auszuführen, die dann aber Schadsoftware enthält (z.B. via Mail, Fake-Captcha oder Malvertising)

Auch Mitarbeiter aus der IT sind hierbei regelmäßig betroffen!

Einiges läuft wieder, und nu?

Nach dem Incident ist vor dem Incident

Nach der Wiederherstellung:

- Alle Passwörter und Secrets ändern
- Härtungsmaßnahmen
- Weitere ext. Kommunikation
- Weiteres Monitoring (min. 2-4 Wochen)
  - Langfristig: Stoïk MDR

Q&A

stoïk

Stoïk GmbH
Im Mediapark 8
50670 Köln

Stoïk GmbH - Zweigniederlassung Österreich
Kohlmarkt 8-10
1010 Wien

www.stoik.com

kontakt@stoik.io

Mehr als Cyberversicherung