Secutec

Cybersecurity Intelligence

Prevent now, secure tomorrow

Aktuelle Bedrohungslage

Vier MEGA Trends prägen die Bedrohungslandschaft 2026

1. KI beschleunigt Angriffe und eröffnet neue Angriffsvektoren

Bei den schnellsten 25 % der Angriffe erfolgte der Datenabfluss bereits nach rund 72 Minuten. (Vorjahr = 288 Minuten)

2. Identitäten sind der wichtigste Angriffsweg durch gestohlene Credentials und Tokens.

Schwachstellen bei Identitäten spielen in fast 90 % der Attacken eine wesentliche Rolle.

3. Neue Risiken in der Software Supply Chain

Angreifer missbrauchen häufig vertrauenswürdige SaaS-Integrationen, Drittanbieter Tools und Abhängigkeiten. Sie sind immer öfter eingebettet in Arbeitsabläufe.

4. Staatliche Akteure agieren verdeckter und persistenter, teils mit KI-Methoden.

Sie setzen verstärkt auf gefälschte Identitäten, Fake-Bewerbungen und die tiefe Kompromittierung zentraler Infrastrukturen.

Identität und vertrauenswürdige Verbindungen sind der neue Hauptangriffsweg
Angreifer brechen nicht mehr ein – sie loggen sich ein!

65 % des Initial Access waren über Identität.

Infostealer-Ökosystem liefert große Mengen kompromittierter Zugangsdaten oft schon wenige Stunden nach der Infektion an kriminelle Marktplätze.

87 % der Vorfälle betrafen mehrere Angriffsflächen gleichzeitig

z. B. Endpoint, Netzwerk, Cloud, SaaS und Identität.

48 % der Attacken enthielten browserbasierte Aktivität

Angriffe sind stark in normale Arbeitsabläufe wie E-Mail, Web und SaaS eingebettet.

MFA- und der Diebstahl von Tokens nehmen stark zu.

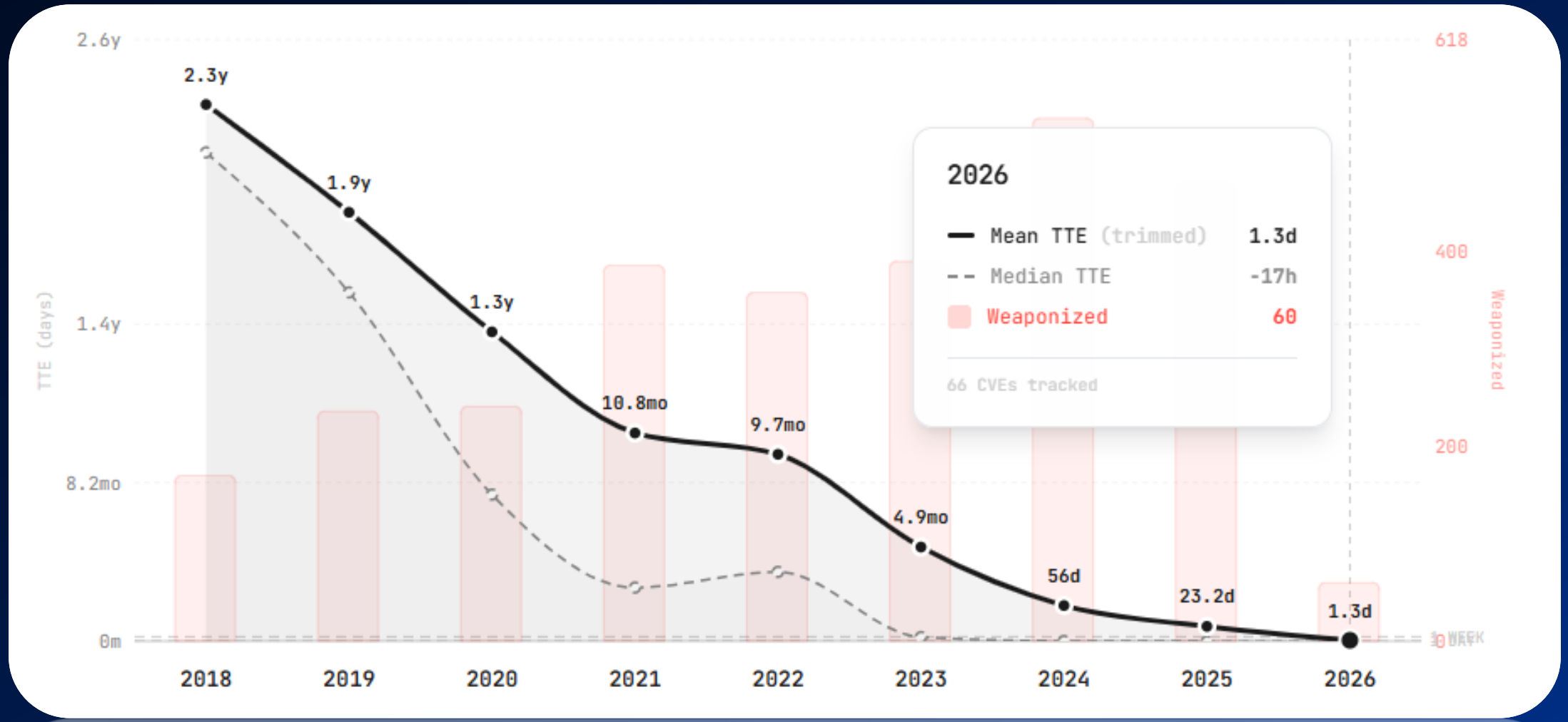
Daten aus SaaS-Anwendungen waren 2025 bereits in 23 % der Fälle relevant

Daten aus Cloud-Diensten wie Microsoft 365, Google Workspace, Salesforce, Slack, usw. spielen eine wichtige Rolle.

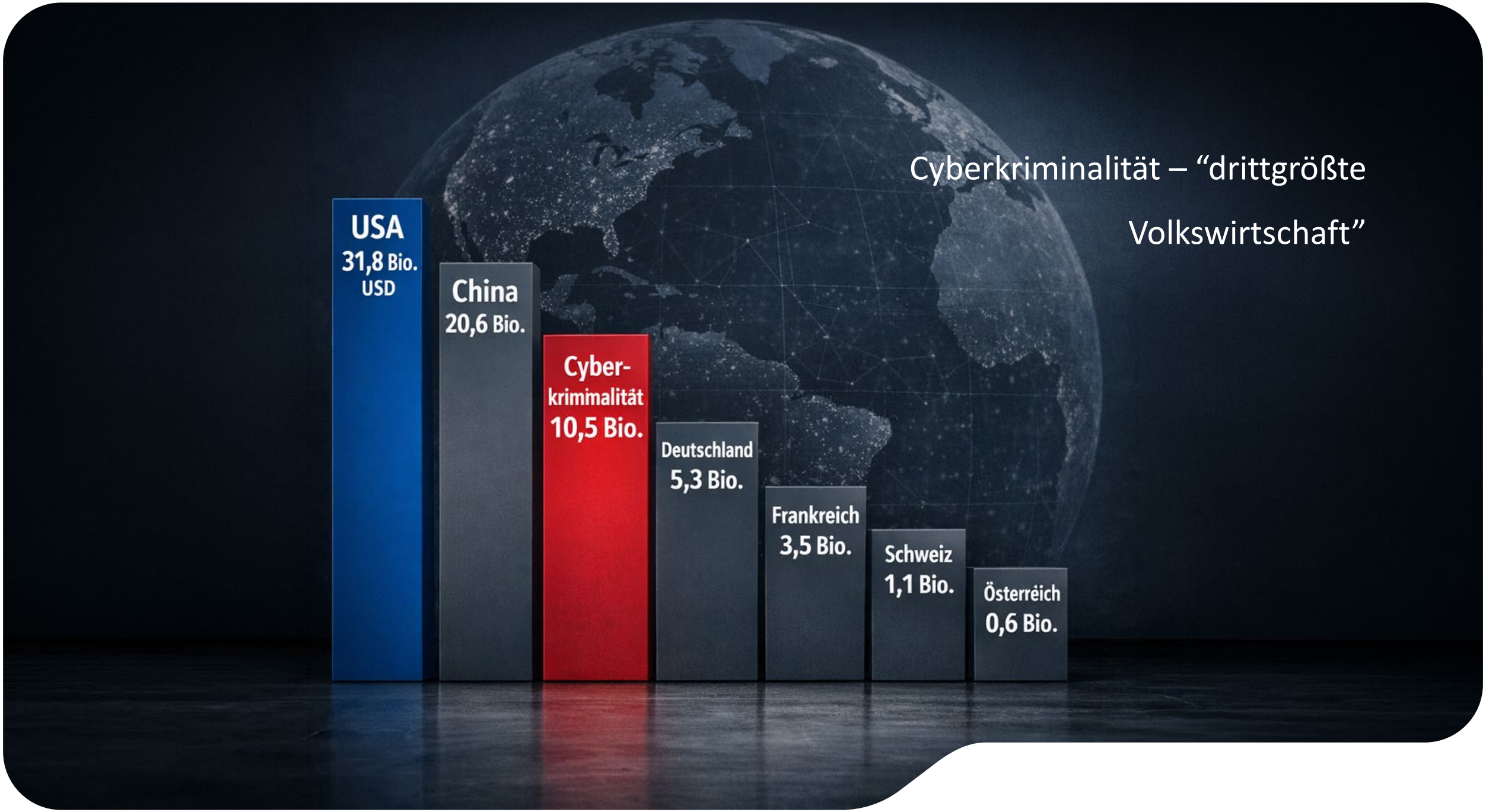
Von 6% auf 23% gestiegen.

Fünfter MEGA Trend – Speed bei Exploits!

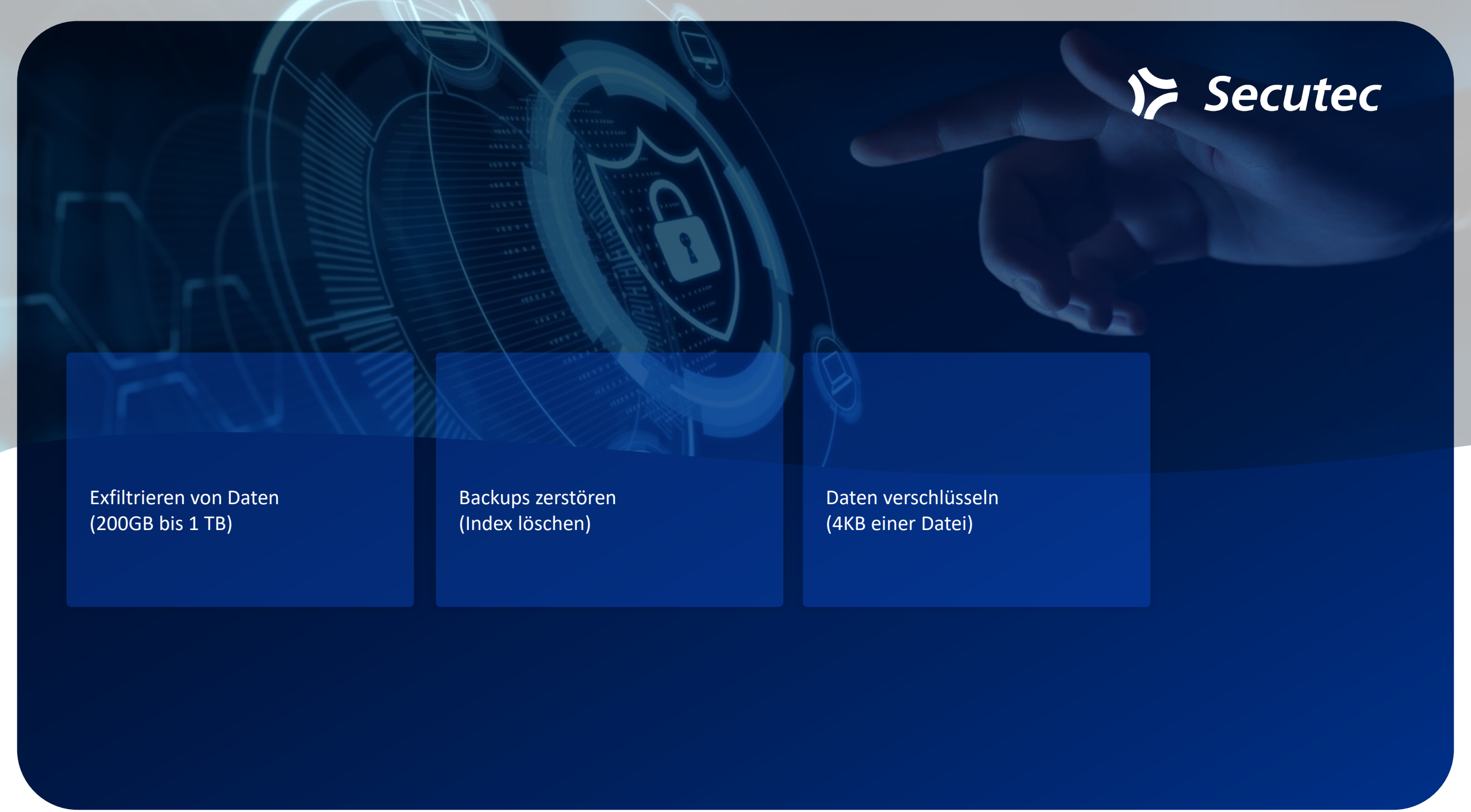
Zeit bis zum Exploit – vom CVE zum funktionierenden Exploit:



Cyberkriminalität – “drittgrößte Volkswirtschaft”



Die Ransomware Attacke



Secutec

Exfiltrieren von Daten
(200GB bis 1 TB)

Backups zerstören
(Index löschen)

Daten verschlüsseln
(4KB einer Datei)

Secutec

Speed of Ransomware Deployment

Durchschnittliches Zeitfenster, vom ersten Zugriff bis zur Aktivierung der Ransomware

~ 66 Tage	~ 9,5 Tage	~ 3,8 Tage	X Stunden	X Minuten
2019	2020	2021	2025	2026/27


Angriffsvektoren
Phishing
(Fokus New Domains)
Lösung: SecureDNS
Brute-Force Attacken
(Wellen bei größeren Leaks)
Lösung: Darknet Monitoring
Passwort Stealer/Keylogger
(Private- und Firmengeräte)
Lösung: Darknet Monitoring
Exploit Vulnerability
(Platzierung von Backdoors)
Lösung: Attack Surface Management
Supply Chain Attacken
(Dienstleister, Lieferanten Service Accounts, usw)
Lösung: ASM und Darknet Monitoring
Man in the Middle
(Fokus Rechnungsbelege)
Lösung: SecureDNS, Threat Hunting, M365 Kit
Social Engineering
Deep Fake
(Online, Audio, Video)
M365 Phishing
(Proxy/Cache - Logindaten/MFA)
Lösung: M365 Security Kit


Secutec
Ransomware Playbook

Secutec

Ausbruchsphase

- Cyberversicherung und Rest informieren
- Internet trennen (Wi-Fi, usw.)
- Backups sichern (Trennen vom Netzwerk)
- Infizierte Geräte nicht herunterfahren (Isolieren)

Secutec

Bewertungsphase

- Incident Tools (SecureDNS – XDR – Velociraptor)
- Logs sichern, autom. Tasks deaktivieren
- Prioritäten definieren (Applikationen)
- Redesign Netzwerk (Segmentierung)

Secutec

Wiederaufbauphase

- Kommunikation (Mail) – evtl. „Dark Site“
- Domaincontroller (**red** VLAN > **green** VLAN)
- ALLE Passwörter zurücksetzen
  (Kerberos Golden Ticket zweimal zurücksetzen)
- Application Server (**red** VLAN > **green** VLAN)
- Daten Restore (**red** -> **orange** -> **green**)
- Backup Planung und Aktivierung
- Endpoints im eigenen VLAN > XDR


Secutec
Playbook Geschäftsleitung

Secutec

Primäres Ziel: Schaden für Unternehmen, Kunden und Eigentümer minimieren

Rolle der Geschäftsleitung im Incident

- Cyber-Incidents sind kein IT-Problem, sondern Management-Thema

- Geschäftsleitung entscheidet über:
  -Risikoakzeptanz und Prioritäten
  -Kommunikation und Transparenz
  -Lösegeld und Wiederanlaufstrategie

Typische Schadensarten

- Operative/Finanzielle Schäden (Stillstand)

  Wie hoch ist der Schaden pro Tag?

- Daten- und Vertrauensschäden (Exfiltration)

  Dürfen die Daten an die Öffentlichkeit gelangen?

- Langfristige Folgen (Kundenabwanderung)

  Wie lange darf die Unterbrechung dauern?

Schwachstelle Kommunikation

- Häufige Situation:
  - E-Mail, Fileserver, Kollaborationstools sind verschlüsselt oder kompromittiert
  - Spontane, unkoordinierte Kommunikation verschärft die Krise
- Risiko:
  - Widersprüchliche Botschaften
  - Informationslecks
  - Vertrauensverlust bei Mitarbeitenden und Partnern

Kommunikation im Incident

- Tipps (vorab etablieren):

- Alternative Kommunikationskanäle
  (z. B. Signal/WhatsApp, externe Notfall-Maildomain)

- Abgestimmte Optionen mit dem Betriebsrat
  (z. B. „Betriebsurlaub“ in Extremszenarien)

- Dark Site / Notfall-Webseite
  für Krisenkommunikation vorbereitenext

Lösegeld entscheidungen ist Chefsache

- Entscheidung liegt immer bei Geschäftsleitung/Eigentümern

- Basis sind harte Fakten, nicht Emotionen:

  - Zustand & Verfügbarkeit der Backups
  - Zeitfaktor / Dauer des Stillstands
  - Art und Brisanz der gestohlenen Daten
  - Rechtlicher Rahmen (Sanktionen, DSGVO)

- Realität: In vielen Fällen ist Lösegeldzahlung wirtschaftlich der geringere Schaden –rechtliche und ethische Risiken bleiben!

Lösegeld und Sanktionsrechtext

- Gefahr:

  Lösegeldempfänger auf Sanktionslisten (Terrorismus, Russland-Sanktionen etc.)

- Vorbereitung:

  - Klare Abstimmung mit Rechtsanwälten und Versicherern

- Standardprozess:

  - Prüfung gegen Sanktionslisten
  - Dokumentation der Entscheidungsgrundlagen
  - Rückendeckung der Eigentümer sichern


Secutec
Lösegeldverhandlungen

Secutec

Lösegeld-forderungen

- Decken sich oft mit den liquiden Mitteln.

  Bilanzen sind in vielen Fällen bekannt.

  Start Forderung meist 5-8% vom Umsatz.

- Argumente über nicht liquide Mittel warden

  oftmals mit aktuellen Bankauszügen widerlegt.

Sarcoma group

1513	7623	6663	8522
Victim	Söllner	B&J Rocket Sales	Paul Hildebrandt
Site: victimransomware.org Industry: Victim GEO: Germany	Site: bedachungen-soellner.de Industry: Commercial & Residential Construction GEO: Germany	Site: bj-rocket.com Industry: Manufacturing GEO: Switzerland	Industry: Manufacturing GEO: Germany
Timer Paused			
More Info	More Info	More Info	More Info

Timer pausiert bei Verhandlungen

13629	13666	15232	16669

Sarcoma group

620

Victim

Site: victimransomware.org
Industry: Victim
GEO: Italy

3 days 18 hours 40 minutes

More Info

14874

Söllner

Site: bedachungen-soellner.de
Industry: Commercial & Residential Construction
GEO: Germany

More Info

13212

B&J Rocket Sales

Site: bj-rocket.com
Industry: Manufacturing
GEO: Switzerland

More Info

14822

Paul Hildebrandt

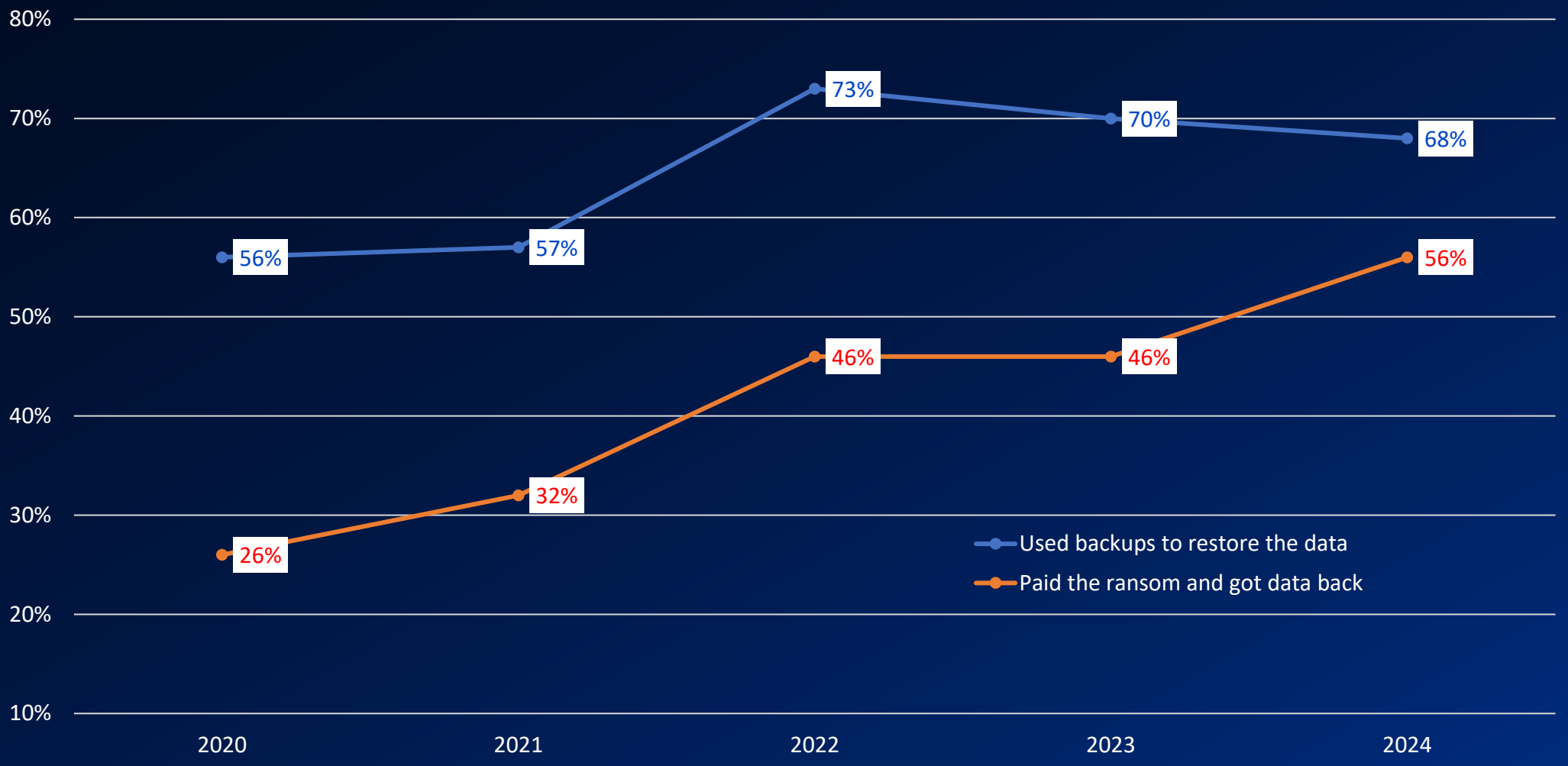
Site: hildebrandt.de
Industry: Manufacturing
GEO: Germany

More Info

Das Opfer fehlt nach der Lösegeldzahlung

Secutec

Verfahren zur Wiederherstellung verschlüsselter Daten



Sophos - State of Ransomware 2024 report.

Hello!

Visit our Blog:

Tor Browser Links:
    http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion/

Links for normal browser:
    http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion.ly/

>>> Your data is stolen and encrypted.

- If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

>>> If you have an external or cloud backup; what happens if you don’t agree with us?

- All countries have their own PDPL (Personal Data Protection Law) regulations. In the event that you do not agree with us, information pertaining to your companies and the data of your company’s customers will be published on the internet, and the respective country’s personal data usage authority will be informed. Moreover, confidential data related to your company will be shared with potential competitors through email and social media. You can be sure that you will incur damages far exceeding the amount we are requesting from you should you decide not to agree with us.

>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.

- Seeking their help will only make the situation worse,They will try to prevent you from negotiating with us, because the negotiations will make them look incompetent,After the incident report is handed over to the government department, you will be fined <This will be a huge amount,Read more about the GDRP legislation:https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>,The government uses your fine to reward them.And you will not get anything, and except you and your company, the rest of the people will forget what happened!!!!!

>>> How to contact with us?

- Install and run 'Tor Browser' from https://www.torproject.org/download/
- Go to http://an2ce4pqpf2ipvba2djurxi5pnxxhu3uo7ackul6eafcundqtly7bhid.onion/
- Log in using the Client ID:


[AKIRA]
AKIRA
Well, you are here. It means that you're suffering from cyber incident right now. Think of our actio
ns as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a
fair price to make it all go away.
Do not rush to assess what is happening - we did it to you. The best thing you can do is to follow o
ur instructions to get back to your daily routine, by cooperating with us you will minimize the dama
ge that might be done.
Those who choose different path will be shamed here publicly. The functionality of this blog is extr
emely simple - enter the desired command in the input line and enjoy the juiciest information that c
orporations around the world wanted to stay confidential.
Remember. You are unable to recover without our help. Your data is already gone and cannot be traced
to the place of final storage nor deleted by anyone besides us.
guest@akira:~$ help
List of all commands:
leaks – hacked companies
news – news about upcoming data releases
contact – send us a message and we will contact you
help – available commands
clear – clear screen
guest@akira:~$

Hi friends,

Unabhängig davon, wer Sie sind und welchen Titel Sie tragen, wenn Sie dies lesen, bedeutet dies, dass die interne Infrastruktur Ihres Unternehmens ganz oder teilweise tot ist, alle Ihre Backups - virtuell, physisch - alles, was wir erreichen konnten, ist vollständig entfernt. Außerdem haben wir einen großen Teil Ihrer Unternehmensdaten vor der Verschlüsselung entwendet.

Nun, lassen Sie uns die Tränen und den Groll erst einmal für uns behalten und versuchen, einen konstruktiven Dialog aufzubauen. Wir sind uns voll und ganz bewusst, welchen Schaden wir mit der Sperrung Ihrer internen Quellen angerichtet haben.
Im Moment müssen Sie das wissen:

1. Wenn Sie mit uns zusammenarbeiten, werden Sie VIEL sparen, denn wir sind nicht daran interessiert, Sie finanziell zu ruinieren. Wir werden Ihre Finanzen, Bank- und Einkommensauszüge, Ihre Ersparnisse, Investitionen usw. gründlich studieren und Ihnen einen angemessenen Vorschlag unterbreiten. Wenn Sie eine aktive Cyber-Versicherung haben, lassen Sie es uns wissen, und wir werden Ihnen zeigen, wie Sie diese richtig nutzen können. Wenn Sie den Verhandlungsprozess in die Länge ziehen, wird das Geschäft nicht zustande kommen.

2. Wenn Sie uns bezahlen, sparen Sie Ihre ZEIT, Ihr GELD, Ihren Aufwand und sind innerhalb von 24 Stunden wieder auf dem richtigen Weg. Unser Entschlüsselungsprogramm funktioniert bei allen Dateien und Systemen einwandfrei, so dass Sie es überprüfen können, indem Sie zu Beginn unseres Gesprächs einen Test-Entschlüsselungsdienst anfordern. Wenn Sie sich für eine Wiederherstellung auf eigene Faust entscheiden, bedenken Sie, dass Sie den Zugriff auf einige Dateien dauerhaft verlieren oder sie versehentlich beschädigen können - in diesem Fall können wir Ihnen nicht helfen.

3. Der Sicherheitsbericht oder die exklusiven Informationen aus erster Hand, die Sie bei Abschluss einer Vereinbarung erhalten, sind von großem Wert, da KEINE vollständige Prüfung Ihres Netzwerks Ihnen die Schwachstellen aufzeigt, die wir aufdecken und nutzen konnten, um in Ihr Netzwerk einzudringen, Backup-Lösungen zu finden und Ihre Daten hochzuladen.

4. Was Ihre Daten betrifft, so werden wir, wenn wir uns nicht einigen können, versuchen, persönliche Informationen/Geschäftsgeheimnisse/Datenbanken/Quellcodes - allgemein gesagt, alles, was auf dem Schwarzmarkt einen Wert hat - an mehrere Bedrohungsakteure auf einmal zu verkaufen. All dies wird dann in unserem Blog veröffentlicht - https://linkprotect.cuda.com/url?a=https%3a%2f%2fakiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion&c=E,1,dJXYIYKI-r4ni_emkQ2CG1rW-DGjxYVPWw4O_MIQQokmy_gdVwkUBvfzCg3NqAJ6C8exu647llHIiABBHWQFCJCXZUfqNc8BbVLM_7t1b-J2FADO&typo=1

5. Wir sind mehr als verhandlungsbereit und werden mit Sicherheit einen Weg finden, die Angelegenheit schnell zu regeln und eine Einigung zu erzielen, die uns beide zufrieden stellt.

Wenn Sie tatsächlich an unserer Hilfe und den von uns angebotenen Dienstleistungen interessiert sind, können Sie sich mit uns in Verbindung setzen, indem Sie die folgenden einfachen Anweisungen befolgen:

1. Installieren Sie den TOR-Browser, um Zugang zu unserem Chatroom zu erhalten - https://linkprotect.cuda.com/url?a=https%3a%2f%2fwww.torproject.org%2fdownload%2f&c=E,1,J0kXbGjEb6C9clIaVzAU-pSdhuYDg8m7aileLbNrCdp-ZeZT_jDLp4VmSDZtvjoYtOTZKpD5K60aZOYAytRkK5SVRECtoCaC0GJCKgNqfLQtx1Q,&typo=1.

2. Fügen Sie diesen Link ein - https://linkprotect.cuda.com/url?a=https%3a%2f%2fakiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.onion&c=E,1,eUm7ptlW0C6Z6Rt8eY4x-cKl9Mb-KjJU6Jcxk-waKKRA3RRi4VHdaUhoEDA-Ez1cOCXf2Qd2N5vhBl_-60w45DSozru3VeHCzfrKbJA7QpA,&typo=1

3. Verwenden Sie diesen Code - 5391-OY-PYET-ZUOF - um sich in unseren Chat einzuloggen.
Denken Sie daran, dass je schneller Sie sich melden, desto weniger Schaden entsteht.

Your current file limit You can upload 2 more file(s)

Upload new file Browse... No file selected. max file size = 20 MB Upload

Chat

[support, 2021-11-04 11:28:53] : got it?
[client, 2021-11-04 11:29:17] : yes
[support, 2021-11-04 11:30:38] : entered password?
[client, 2021-11-04 11:30:57] : Voila I'm in
[support, 2021-11-04 11:33:08] : bitcoin wallet 3Nf9MJsQToPnRkyTcA5CxC3e21AHvZ9KVP
[client, 2021-11-04 11:34:03] : OK I send you 0,1 bitcoin you confirm me and then I send you 15,65 Bitcoins
[support, 2021-11-04 11:36:11] : ok
[client, 2021-11-04 11:36:20] : OK?
[client, 2021-11-04 11:38:10] : have you received the 0,1?
[support, 2021-11-04 11:44:57] : yes
[client, 2021-11-04 11:46:05] : ok I send you now 15,65 bitcoin
[support, 2021-11-04 11:46:47] : ok
[client, 2021-11-04 11:48:52] : they are send!

Note You can send no more than 1 message per minute.

Message

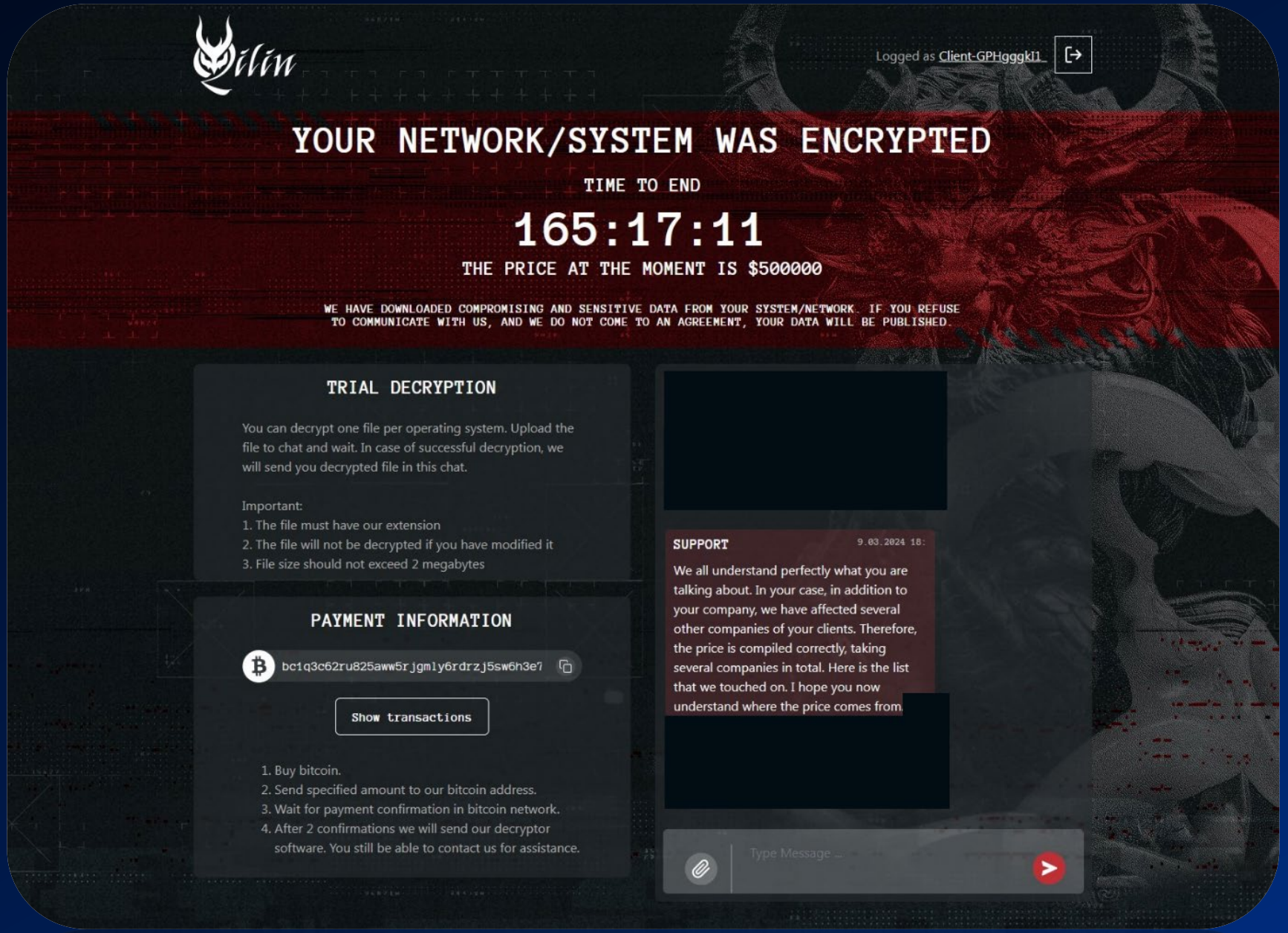
Chat

[client, 2021-11-02 11:02:06] : I received a go for 900.000 USD from the customer, this is already much more than the emount they could spent when we start the negotiation.
[client, 2021-11-02 11:04:28] : amount
[support, 2021-11-02 14:08:11] : it must be 999
[client, 2021-11-03 19:04:10] : ok I received a go from the customer, I'm waiting for the money on my account and than I can prepare the last steps, can you send me your bitcoian adres so that I can send you first 0,5 bitcoin, ones you confirm that you received this I will send the rest.
[client, 2021-11-04 06:30:27] : The money is on my account, can you give me your bitcoin address please. Thanks
[support, 2021-11-04 08:48:25] : before I give you bitcoin address I have to password protect our conversation. Please tell me when you are here and confirm you are ready to write down the password.
[client, 2021-11-04 11:22:34] : ok I'm there
[support, 2021-11-04 11:28:12] : password is Besix2277

Note You can send no more than 1 message per minute.

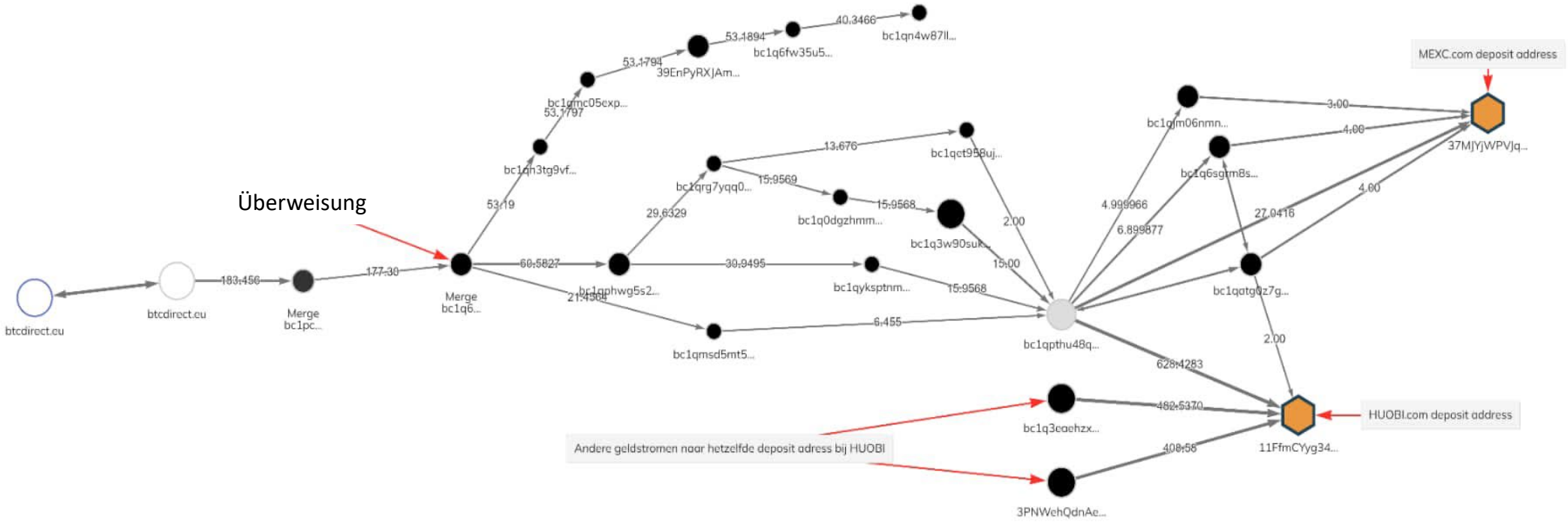
Message

Send


Logged as Client-GPHgggkI1
YOUR NETWORK/SYSTEM WAS ENCRYPTED
TIME TO END
165:17:11
THE PRICE AT THE MOMENT IS $500000
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
bc1q3c62ru825aww5rjgmly6rdrzj5sw6h3e7
Show transactions
1. Buy bitcoin.
2. Send specified amount to our bitcoin address.
3. Wait for payment confirmation in bitcoin network.
4. After 2 confirmations we will send our decryptor software. You still be able to contact us for assistance.
SUPPORT
9.03.2024 18:
We all understand perfectly what you are talking about. In your case, in addition to your company, we have affected several other companies of your clients. Therefore, the price is compiled correctly, taking several companies in total. Here is the list that we touched on. I hope you now understand where the price comes from.
Type Message ...

Lösegeldverhandlungen

Initiale Forderung	Bezahltes Lösegeld	Discount %	Discount	Verhandlungsschritte
900.000,00	325.000,00	63,9	575.000,00	15
1.500.000,00	350.000,00	76,7	1.150.000,00	10
400.000,00	200.000,00	50,0	200.000,00	9
999.000,00	512.000,00	48,7	487.000,00	8
980.000,00	300.000,00	69,4	680.000,00	7
200.000,00	100.000,00	50,0	100.000,00	7
5.000.000,00	746.500,00	85,1	4.253.500,00	6
3.000.000,00	800.000,00	73,3	2.200.000,00	6
900.000,00	450.000,00	50,0	450.000,00	6
300.000,00	150.000,00	50,0	150.000,00	5
150.000,00	100.000,00	33,3	50.000,00	3
1.250.000,00	1.000.000,00	20,0	250.000,00	1
1.329.153,85	396.423,08	58,7	932.730,77	7


Overweisung
btcdirect.cu
183.456
btcdirect.cu
177.30
Merge
bc1pc...
Merge
bc1q6...
53.19
bc1qh3tg9vf...
53.1797
bc1qmc05exp...
53.1794
39EnPyRXJAm...
53.1894
bc1q6fw35u5...
40.3466
bc1qn4w87ll...
60.5827
bc1qphwg5s2...
21.4368
29.6329
bc1qrg7yqq0...
13.676
bc1qct958uj...
15.9569
bc1q0dgzhmm...
15.9568
bc1q3w90suk...
30.9495
bc1qyksptnm...
15.9568
2.00
15.00
6.455
bc1qmsd5mt5...
bc1qpthu48q...
4.999966
6.899877
bc1qjm06nmn...
3.00
4.00
bc1q6sgrm8s...
27.0416
4.00
37MJYjWPVJq...
MEXC.com deposit address
bc1qatg0z7g...
2.00
628.4283
bc1q3eaehzx...
482.5370
HUOBI.com deposit address
11FfmCYyg34...
Andere geldstromen naar hetzelfde deposit adress bij HUOBI
408.58
3PNWehQdnAe...

Empfehlungen für Unternehmen

Secutec

DNS Monitoring Auch IoT Devices beachten!	**Externe Scans Schwachstellen** Aus Sicht eines Cyberkriminellen	**Blacklist Scanner IPs** Externe Vul-Scanner IP Adressen blocken	**Darknet Monitoring** Leaked Credential und Keywords	**Incident Vorbereitung** Playbook Geschäftsleitung nicht vergessen!
Multifaktor Authentifizierung Nicht nur mit Bestätigung!	**EDR/XDR Virenscanner** Anomalie-erkennung	**Backup Konzept und Recovery** Testen nicht vergessen!	**Server Logs Backup** Rund 90 Tage für Forensik	**Netzwerk Segmentierung** Firewall nicht vergessen!
Keine lokalen Admin Rechte Nur temporäre Rechte zulassen	**Active Directory Tiering Struktur** Eigene User für Server und DC	**Cyber Risiken Sichtbar machen** Messbare Cyber Risiken auf den Punkt bringen	**Passwort Manager** Verwaltung und sichere Passwörter (+Privatnutzung)	**Cyberversicherung Polizze** Die Polizze sollte auf keinen Fall digital abgelegt werden!