COMMERZBANK

nviso

www.nviso.eu

ATHENS

BRUSSELS

FRANKFURT

MUNICH

VIENNA

Von Analyse bis Aktion

Ihr Fahrplan zur digitalen Absicherung

18.02.2025

Agenda

1. NVISO Vorstellung
2. Die aktuelle Bedrohungslage
3. Warum Sie sich mit Ransomware befassen sollten
4. Wie man Ransomware-Resilienz aufbaut

NVISO Vorstellung

Über NVISO

Unsere Company

NVISO ist ein führendes Cyber-security Beratungsunternehmen mit über 300 spezialisierten Sicherheits-experten.

Gegründet im Jahr 2013 in **Belgien**, sind wir seit 2019 auch in **Deutschland** sowie seit 2022 in **Griechenland** und **Österreich** tätig.

Unsere Mission: **Wir schützen die Grundlagen der europäischen Gesellschaft vor Cyberangriffen.**

Unsere DNA

We are proud: Wir sind stolz darauf, wer wir sind und was wir tun.

We care: Wir kümmern uns um unsere Kunden und Menschen.

We break barriers: Wir fordern den Status quo durch kontinuierliche Innovation heraus.

No BS: Wir halten unsere Versprechen und arbeiten pragmatisch.

Unser Research

Wir investieren **10 % unseres Jahresumsatzes in die Erforschung** neuer Sicherheitstechniken und die Entwicklung neuer Lösungen.

Blog

blog.nviso.eu

X

@NVISOsecurity

@NVISO_Labs

Unsere Services

Wo finden Sie uns…

Website
nviso.eu

Blog
blog.nviso.eu

E-Mail
info@nviso.eu

Linkedin
nviso-cyber

X
@NVISOsecurity
@NVISO_Labs

Sie wurden gehackt?

Emergency Response

Belgium
+32 (0)2 588 43 80
csirt@nviso.eu

Germany
+49 69 8088 3829
csirt@nviso.de

Austria
+43 720 228 337
csirt@nviso.at

Unsere Expertise

Wir übernehmen eine Vorreiterrolle und geben unser Wissen aktiv weiter. Ein Beweis dafür sind die SANS-Kurse, die wir (mit-)verfassen und unterrichten.

SEC575

Mobile Pen. Testing

Seit 2019 sind NVISO-Experten die Hauptautoren des SANS SEC575 Kurses „Mobile Penetration Testing & Ethical Hacking“.

NVISO-Experten pflegen 6 Tage Kursmaterial für diesen 6-tägigen Kurs.

SEC598

Security Automation

Im Laufe der Jahre 2021 und 2022 hat NVISO einen neuen SANS-Kurs entwickelt, der sich auf Security Automation konzentriert. Veröffentlicht im Jahr 2023.

NVISO-Experten pflegen und entwickeln 6 Tage Kursmaterial für diesen Kurs.

SEC599

Purple Team Tactics

Im Jahr 2018 waren NVISO-Experten die Hauptautoren eines der ersten Purple Teaming Kurse, „SEC599 – Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses“.

NVISO-Experten pflegen 5 Tage Kursmaterial für diesen Kurs. Wir unterrichten ihn auch aktiv weltweit.

SEC699

Advanced Purple Team

Im Jahr 2020 entwickelten NVISO-Experten einen Folgekurs zu SEC599, genannt SEC699, der sich mehr auf die automatisierte Nachahmung von Bedrohungen mit CALDERA konzentriert.

NVISO-Experten pflegen 5 Tage Kursmaterial für diesen 6-tägigen Kurs. Wir unterrichten ihn auch aktiv weltweit.

Wir teilen unser Know-How mit der Community

Talks & Konferenzen

Wir präsentieren unsrer Forschungsergebnisse auf renommierten Sicherheitsveranstaltungen und Konferenzen präsentiert, darunter die RSA Conference, Black Hat, BruCON, OWASP, FIRST und viele weitere.

Frau Plattner als Präsidentin des Bundesamtes für Sicherheit in der Informationstechnik eröffnet unsere Deutschen Hacking Meisterschaft.

Unsere Expertise

Unsere Fachexperten werden regelmäßig eingeladen, ihr Wissen und ihre Expertise in Print- und Fernsehnachrichten zu teilen, um komplexe Cybersecurity-Themen verständlich zu machen.

nVISO.eu

Handelsblatt

KÜNSTLICHE INTELLIGENZ

Wie neuartige Cyberattacken mit KI die Banken bedrohen

von: Andreas Kröner • Elisabeth Atzler
Datum: 28.06.2023 04:00 Uhr

Geldhäuser geraten besonders häufig ins Visier von Hackern. Mit KI werden die Angriffe zunehmen und ausgefeilter werden. Aufsichtsbehörden sind alarmiert.

Frankfurter Bankenviertel

Behörden warnen vor Cyberattacken unter dem Einsatz künstlicher Intelligenz.

(Foto: dpa)

BUNDESBANK-PROJEKT „TIBER"

„Wir greifen auf drei Wegen an": So lassen sich deutsche Banken fast immer hacken

Die Zahl von Cyberangriffen ist deutlich gestiegen. Um besser gerüstet zu sein, lassen sich Finanzkonzerne zu Testzwecken attackieren. Ein Angreifer erklärt, wie er dabei vorgeht.

19.10.2021 - 13:22 Uhr

Internetkriminalität

Die Zahl der Cyberattacken hat sich in der letzten Dekade verdreifacht, schätzt der Internationale Währungsfonds. Der Finanzsektor zählt dabei zu den am meisten attackierten Branchen.
(Foto: dpa)

Sendung verpasst?

Wirtschaft ▸ Finanzen ▸ "Virtueller Bankraub": Finanzaufsicht warnt vor Cyberangriffen

Cyberangriffe auf IT-Dienstleister

Finanzaufsicht warnt vor "virtuellem Bankraub"

Stand: 23.01.2024 18:25 Uhr

Customer Success Story

Read the story

KÖRBER

Our time-to-response and mean time-to-response have dropped enormously thanks to Microsoft Sentinel. This makes our IT infrastructure and us as a company much more resistant to cyberattacks.

Andreas Gaetje, Chief Information Security Officer, Körber

Source: https://www.microsoft.com/en/customers/story/20130-korber-microsoft-sentinel

100%

More **Detection**

50%

Fewer **Incidents**

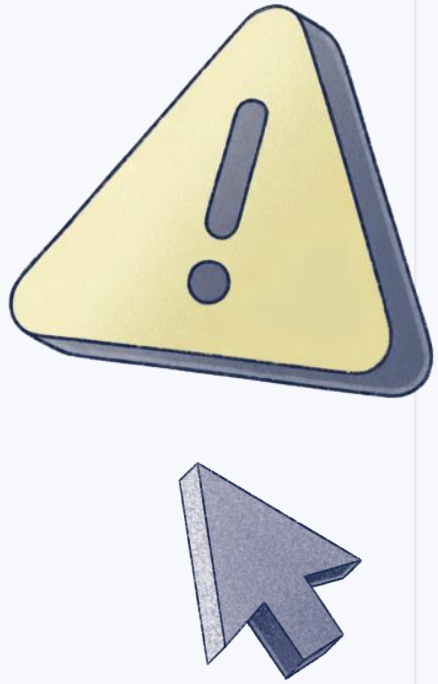
240%

Increase in

Security Coverage

Unsere Kunden

Aktuelle Bedrohungslage



Hackerangriff auf LUP-Kliniken

News

11 Februar 2025 • 2 Minuten

Cyberangriffe

"Prorussische" Cyberattacke auf Staatsregierung und Polizei

Nach BR-Informationen kam es vor Beginn der Sicherheitskonferenz zu einem stundenlangen Cyberangriff auf Webseiten von Staatsregierung und Polizei. Das Landesamt für Sicherheit in der Informationstechnik spricht von "prorussischem Hacktivismus".

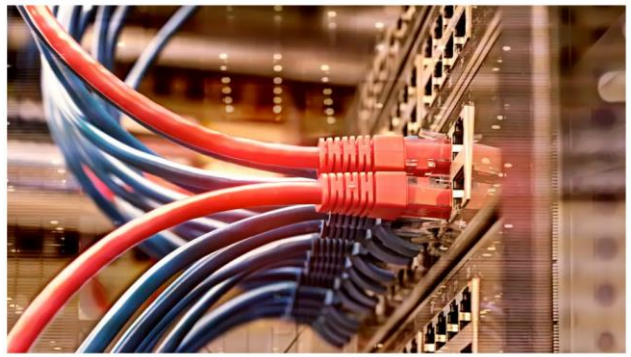
Massive Cyber Attack On Tata Company, All IT Services Suspended

Tata Technologies has confirmed experiencing a ransomware attack that led to the temporary suspension of certain IT services.

Massiver Cyberangriff auf US-Provider: Attacken gehen immer noch weiter

Im Herbst wurde der schlimmste Telekommunikationshack in der US-Geschichte entdeckt. Die Angreifer wurden noch nicht gestoppt, ganz im Gegenteil.

87



(Bild: asharkyu/Shutterstock.com)

13.02.2025, 15:18 Uhr Lesezeit: 2 Min. | Security

Von Martin Holland

MÜNCHEN

Cyberangriff trifft Universität der Bundeswehr

Angreifer sind wohl über geleakte Zugangsdaten in den Besitz persönlicher Daten von Soldaten und zukünftigen Offizieren der Bundeswehr gelangt.

in Pocket speichern | merken

14. Februar 2025, 9:09 Uhr, Marc Stöckel

(Bild: pixabay.com / DomPixabay)

Blick auf eine dunkle Tastatur (Symbolbild)

"Marposs under attack: servers encrypted"

Hackers targeted the company on Sunday night. A team of cybersecurity experts is working to unlock the system

Aktuelle Bedrohungslandschaft

Breaches werden immer schneller erkannt...

Anzahl unerkannter Tage (Median Dwell Time)

	2016	2021	2023
Global	99	21	10
EMEA	106	48	22

Quelle: Mandiant M-Trends 2024

...aufgrund von zwei Faktoren

- **Verbesserte Erkennungsfähigkeiten** (Technologie, Menschen & Prozesse)
- **Ransomware und Erpressungsangriffe** werden in ca. 5 Tagen abgeschlossen und machen ein Drittel aller Angriffe aus – schnelles Aufdecken ist notwendig!

54%
der Breaches werden von externen Parteien erkannt

Quelle: Verizon DBIR 2024; Mandiant M-Trends 2024

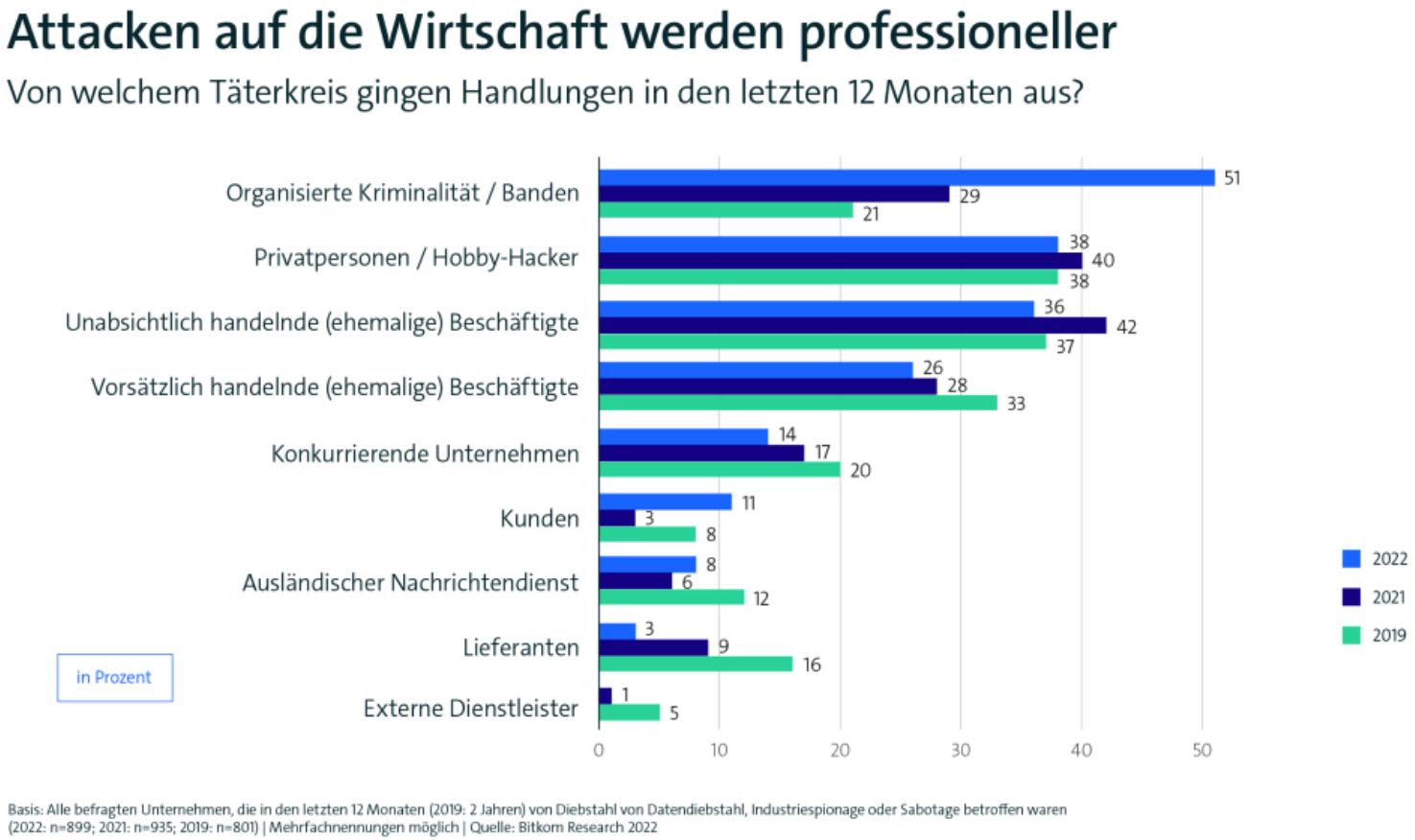
Wir erkennen Sicherheitsvorfälle zwar schneller, doch auch deren Häufigkeit nimmt zu.

Aktuelle Bedrohungslandschaft

Gemäß dem Digitalverband Bitkom kam es im letzten Jahr zu mehr als **203 Milliarden Euro an Schaden durch Cyber Angriffe** auf Unternehmen in Deutschland.

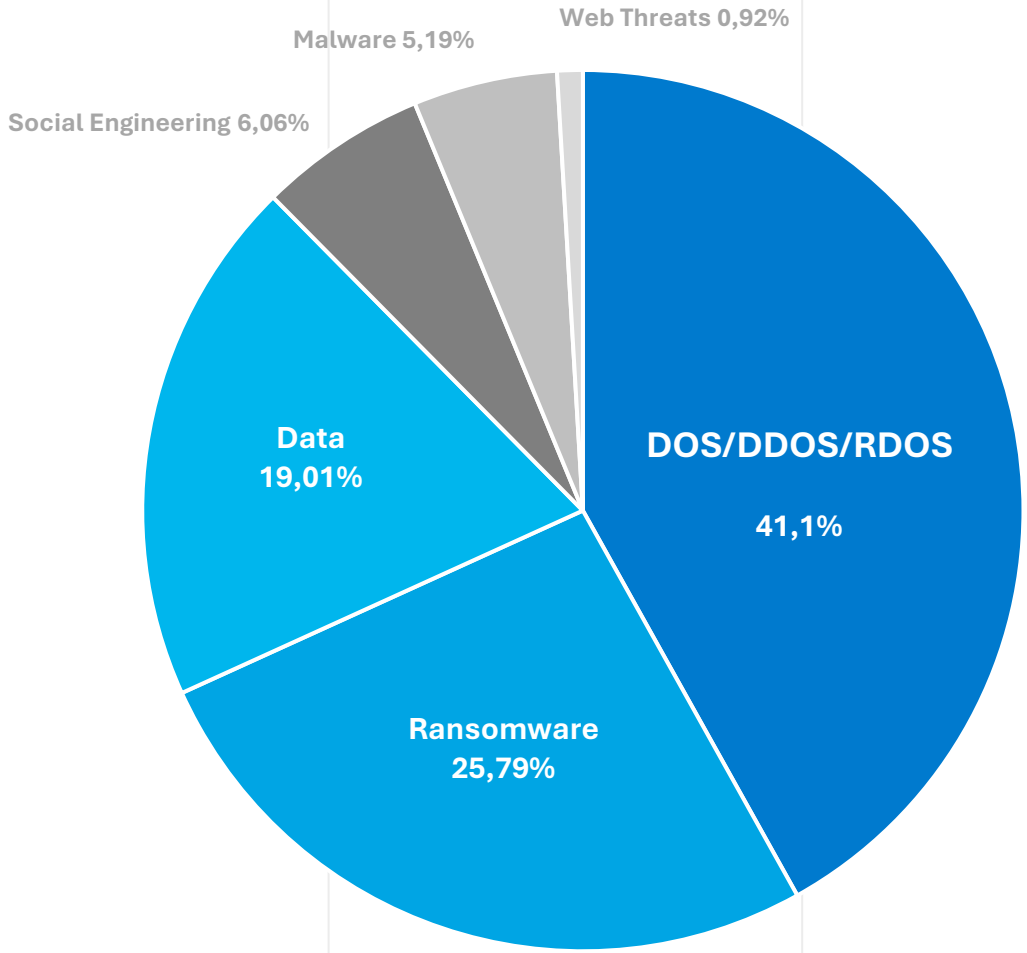
Es zeit sich auch, dass die Angriffe immer professioneller werden und organisierte Kriminalität sich einen Raum im digitalen Bereich schafft.

Organisierte Kriminalität ist mittlerweile so professionell aufgestellt, dass sie auch datenschutzrechtliche oder andere Compliance Beratung beim Ransomware Angriff bekommen. Die organisierten Banden beraten Sie gerne, wie viel Zeit Ihnen für die Meldung noch bleibt.



Referenz: https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022#item-16370

Threat Landscape 2024



Referenz: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

DDoS und Ransomware stehen für ein weiteres Jahr an der Spitze.

Ransomware-Angriffe haben sich auf einem recht hohen Niveau stabilisiert.

Ransomware hat sich zu einer milliardenschweren Industrie entwickelt, die Hacking- und Erpressungstechniken kombiniert.

Ransomware

nviso.eu

Ein historischer Rückblick

1989
Der Ursprung

Aids-Trojaner. Verbreitet über Disketten.

Forderte 189 $, die an ein Postfach in Panama gesendet werden sollten.

2013
Ransomware-as-a-Service

Wannacry betraf Organisationen weltweit.

FBI berichtete erstmals über 1 Milliarde $ an Ransomware-Zahlungen.

Cryptolocker erpresste 3 Millionen $, hauptsächlich in BTC.

2017
Globale Auswirkungen

Wannacry betraf Organisationen weltweit.

FBI berichtete erstmals über 1 Milliarde $ an Ransomware-Zahlungen.

2023
Lösegeldrekord

Über 1,25 Milliarden $.

76 % der Ransomware-Angriffe beinhalteten Datenexfiltration.

2024
Bemerkenswerter Rückgang

831 Millionen $. Unternehmen weigern sich zu zahlen.

Stärkere Sicherheit. Niedrigere Lösegelder..

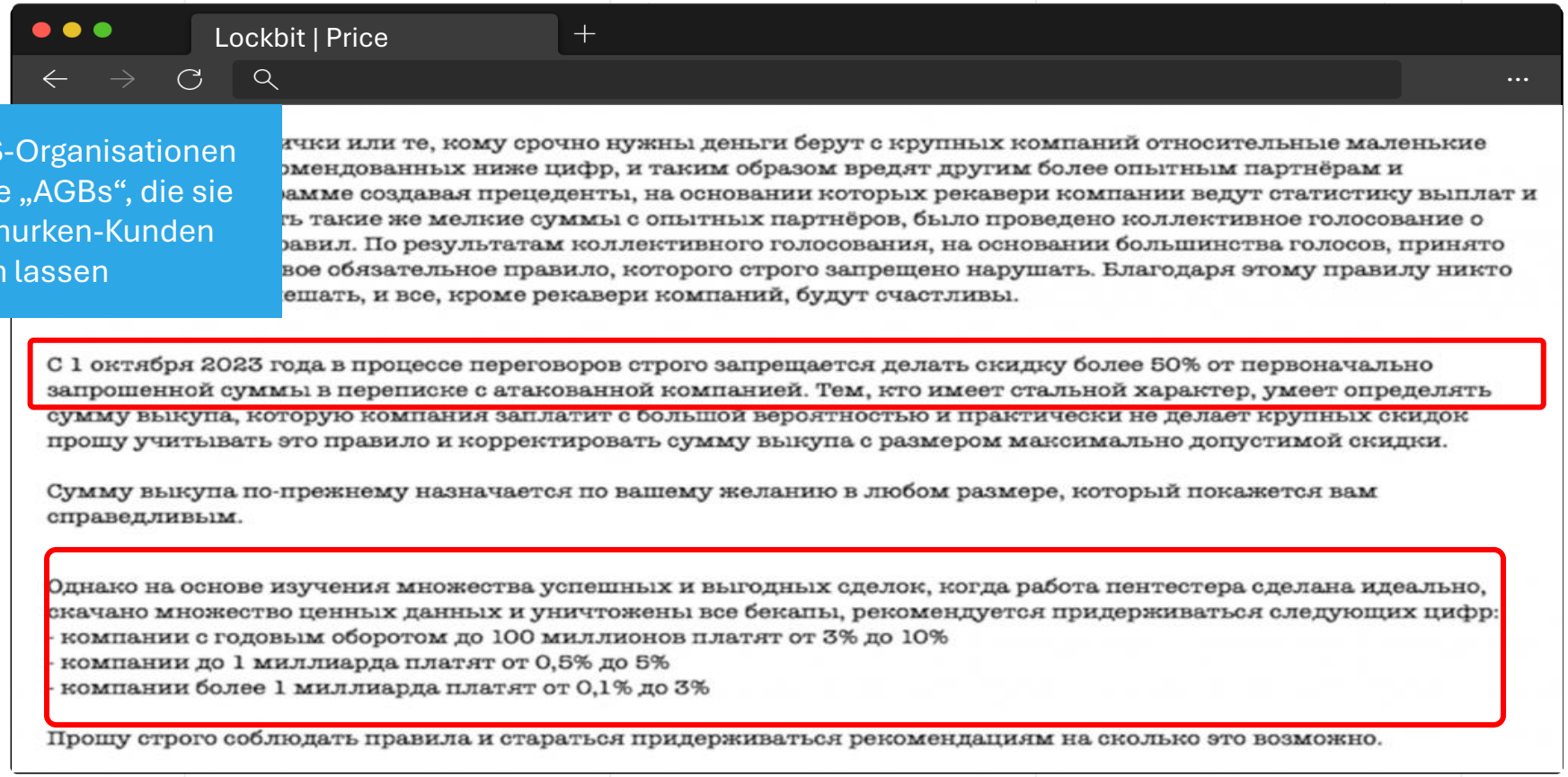
Wo moderne Technik und Kriminalität aufeinandertreffen

	Ransomware	**Kokainhandel**
Umsatz/Einheit	**140.000 $/Angriff**	60.000 $/Kilo
Betriebskosten/Einheit	2.500 $/Angriff*	5.000 $/Kilo
Gewinnspanne	98 %	91 %
Verhaftungen/Einheit	**0,0008****	0,50
Todesfälle/Einheit	0	0,25
Markteintrittsbarrieren	Keine	Sehr hoch

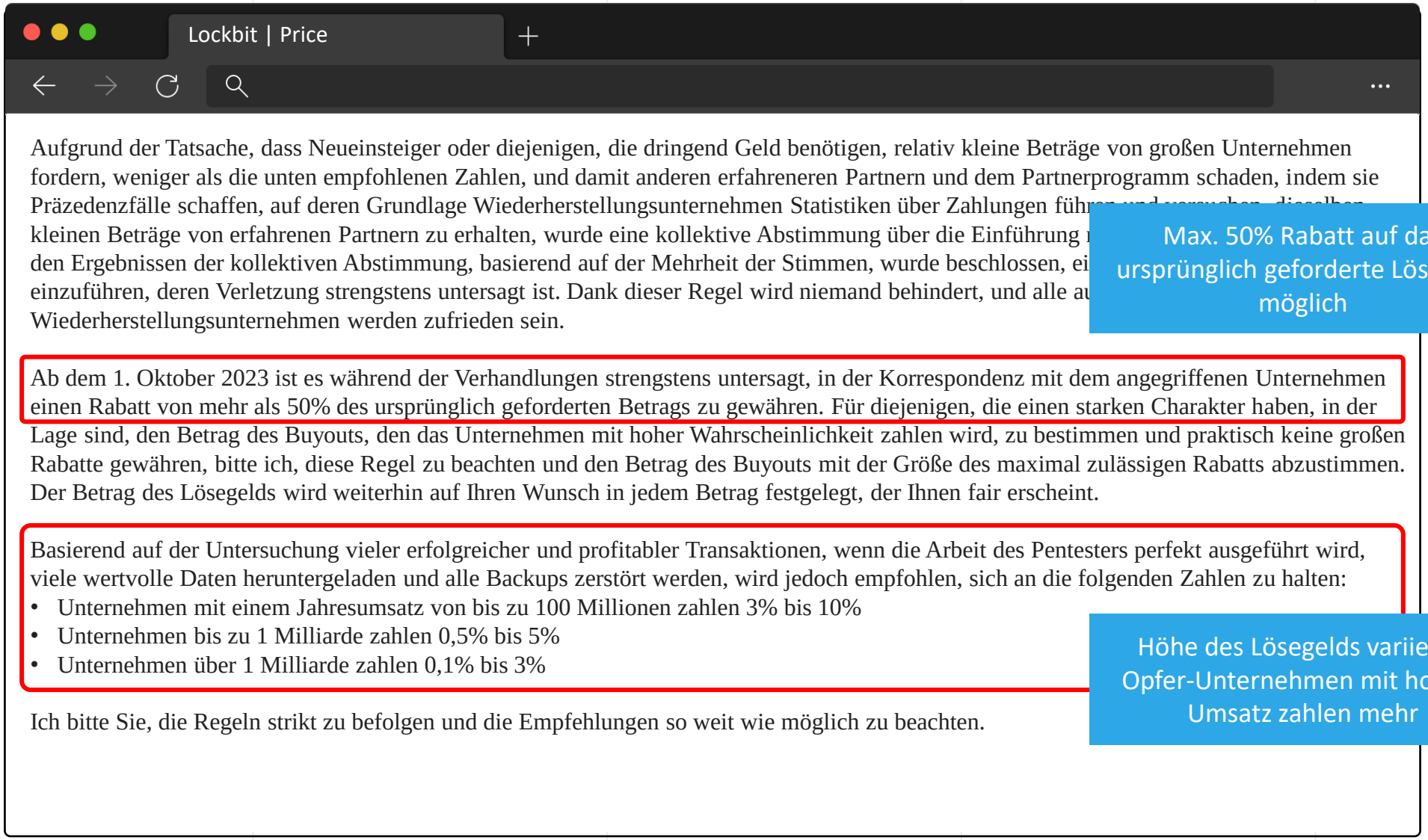
**Estimate based on reported costs of network access credentials, and amount of hours a threat actor expends on the average attack*
***Estimated roughly 25,000 ransomware attacks of impact in 2020. Research found evidence of less than 20 total arrests globally.*

Wo moderne Technik und Kriminalität aufeinandertreffen

Ransomware-SaaS-Organisationen haben sogar eigene „AGBs“, die sie sich von ihren Schurken-Kunden bestätigen lassen



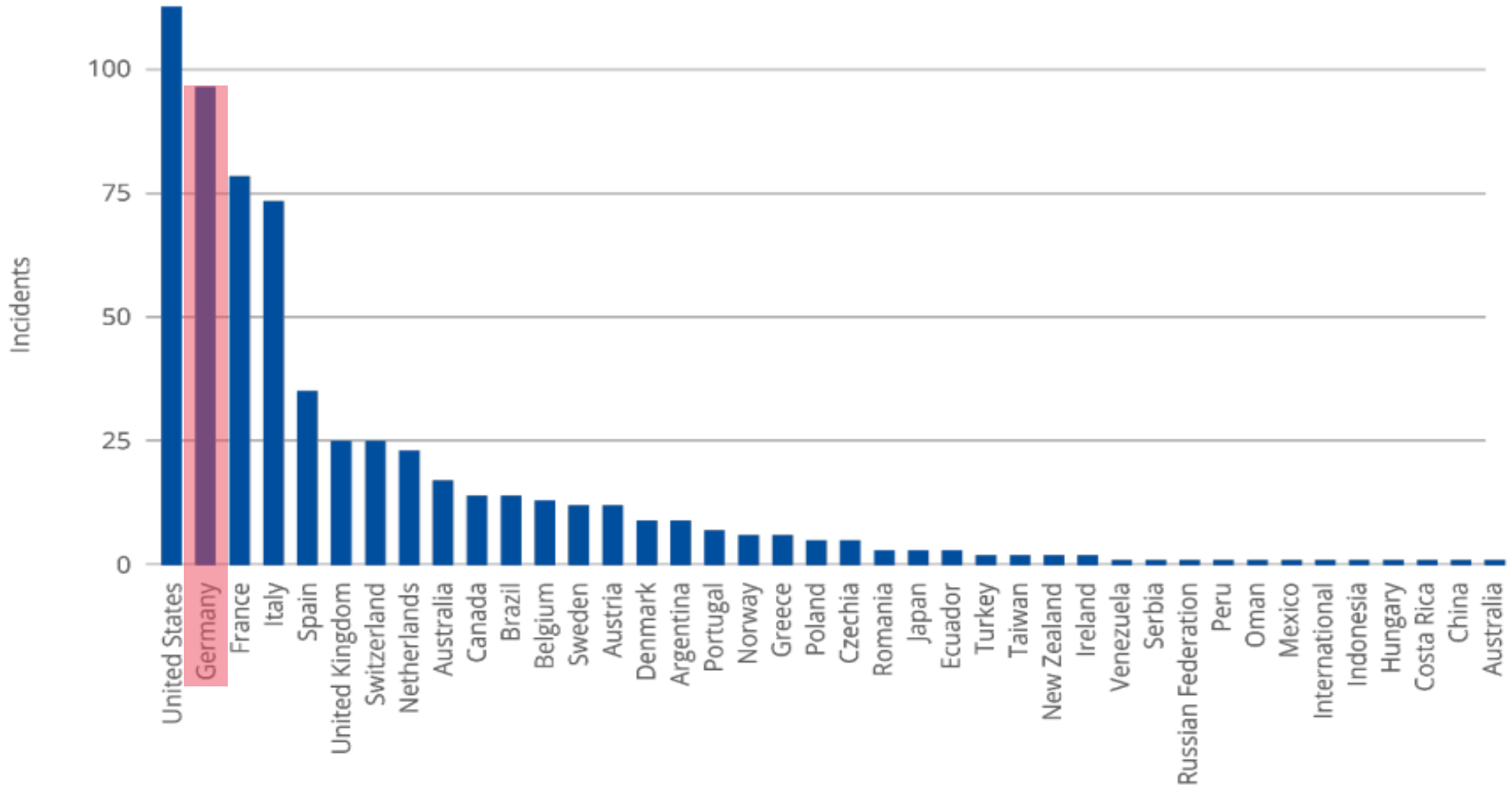
Wo moderne Technik undKriminalität aufeinandertreffen



Max. 50% Rabatt auf das ursprünglich geforderte Lösegeld möglich

Höhe des Lösegelds variiert – Opfer-Unternehmen mit hohem Umsatz zahlen mehr

Anzahl der Ransomware-Vorfälle



Quelle: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Ransomware%20Attacks.pdf

nviso.eu

Aktuelle Bedrohungslandschaft

Gemäß dem Bundesamt für Sicherheit in der Informations-technik wurden im vergangenen Jahr insbesondere **Ransomware** Angriffe auf Wirtschafts-unternehmen im KMU-Bereich durchgeführt.

Gemäß dem BSI Lagebericht ist eine steigende Anzahl an Ransomware as a Service Angriffen zu verzeichnen und zählt deshalb auch zu den Top Bedrohungen weiterhin in Deutschland.

Ransomware ist ein großes kriminelles Geschäft

- Es ist nicht eine Frage, ob es passiert, sondern wann und mit welchem Ausmaß.
- Ungefähr **49% der globalen Ransomware-Angriffe** zielen auf kleine Unternehmen ab.*
- **75 %** der **globalen KMUs** könnten ihren Betrieb nicht fortsetzen, wenn sie von Ransomware getroffen werden.**
- Die **Kosten umfassen mehr als nur Lösegeld**: Es entstehen **Ausfallzeiten und Reputationsschäden**.

*Quelle: https://www.yardsticktechnologies.com/why-ransomware-remains-a-top-threat-for-smbs-in-2024/
**Quelle: https://www.strongdm.com/blog/small-business-cyber-security-statistics

Schließen von Sicherheitslücken bleibt entscheidend – durch Updates oder kompensierende Maßnahmen

nviso.eu

Aktuelle Bedrohungslandschaft für KMUs

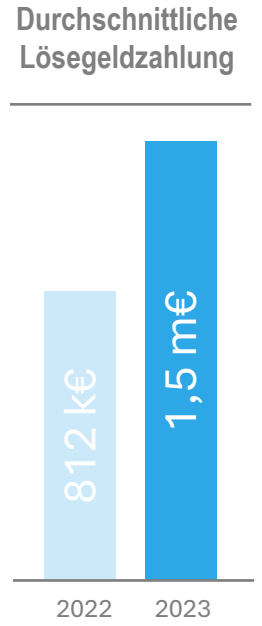
Gemäß dem Bundesamt für Sicherheit in der Informations-technik wurden im vergangenen Jahr insbesondere **Ransomware** Angriffe auf Wirtschafts-unternehmen im KMU-Bereich durchgeführt.

Ablauf einer Ransomware

Gemäß dem BSI Lagebericht ist eine steigende Anzahl an Ransomware as a Service Angriffen zu verzeichnen und zählt deshalb auch zu den Top Bedrohungen weiterhin in Deutschland.

Ransomware ist eine große Gefahr für KMUs

- Deutlicher Anstieg der **Lösegeldzahlungen mit doppelter Erpressung**, bei der man zahlt: (1) für den Entschlüsselungsschlüssel und (2) um die Veröffentlichung gestohlener Daten zu vermeiden.
- Die **Kosten von Ransomware-Angriffen** gehen über das Lösegeld hinaus – z.B. Kosten für Wiederherstellung, Zeit zur Wiederherstellung von Backups…
- Ein ausgereiftes **kriminelles Ökosystem**, betrieben durch Malware-as-a-Service.



Quelle: Sophos - State of ransomware 2023

Schließen von Sicherheitslücken bleibt entscheidend – durch Updates oder kompensierende Maßnahmen

nviso.eu

Aktuelle Bedrohungslandschaft – Wie gehen Angreifer vor?

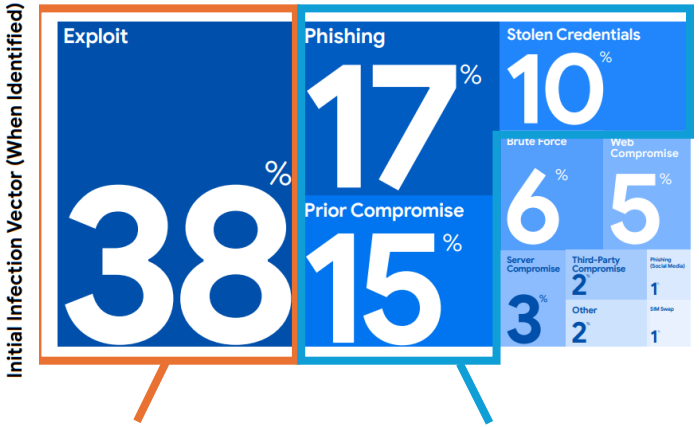
Bei Ransomware haben Angreifer aktuell zwei monetäre Ziele:

1. Lösegelderpressung für die Wiederherstellung der Daten
2. Erpressung bzgl. Veröffentlichung der Daten im Dark Web.

Organisierte Kriminalität müssen Sie sich vorstellen, wie ein gut organisiertes Unternehmen. Diese Organisationen haben Fachbereiche und Fachexperten in den verschiedenen Kompetenzrichtungen.

Ransomware setzt zunehmend auf gezielte und gut vorbereitete Angriffe

Die Angreifer bereiten ihren Angriff vor, indem sie…



Das Internet nach Schwachstellen durchsuchen (Exploit)

Anmeldedaten stehlen:

- durch Phishing
- oder die Ausnutzung anderer Verstöße (z. B. vorherige Kompromittierungen)

Quelle: 2024 Google M-Trends report

Es geht darum vorbereitet zu sein – mit Reaktionsplänen, effektiven Backups und regelmäßigem Üben von Angriffen

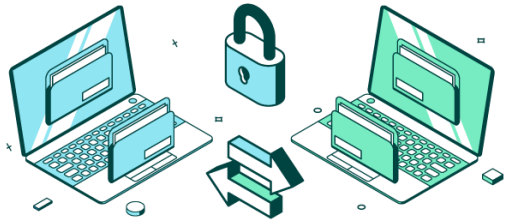
Aktuelle Bedrohungslandschaft – Wie gehen Angreifer vor?

Folgen von hochentwickelten staatlich unterstützten Angriffen

14 Toyota-Werke stehen still nach aufeinanderfolgenden Hackerangriffen auf Toyotas Zulieferer Kojima Industries, Denso und Bridgestone.

Ein fehlerhaftes Update von Crowdstrike führte dazu, dass Millionen von Windows-Rechnern abstürzten, was oft einen physischen Zugriff auf die Maschinen erforderlich machte, um sie zurückzusetzen.

Mehr 'triviale' Sicherheitsverletzungen bei Lieferanten



Die Ransomware-Gruppe CI0p entdeckte eine Schwachstelle in der SaaS-Datenübertragungslösung MoveIT und nutzte sie im Jahr 2023, um Daten von 77 Millionen Personen zu stehlen von 2.600 Unternehmen, darunter BBC, British Airways, EY, PwC, Shell, Siemens, ING, Deutsche Bank, Postbank und anderen.

Ein Versagen bei Drittanbietern wird zunehmend bei der Incident Response berücksichtigt.

Auch bei der Anbieterauswahl müssen die Risiken und Cybersicherheit berücksichtig werden.

Resilienz

Ransomware Killchain

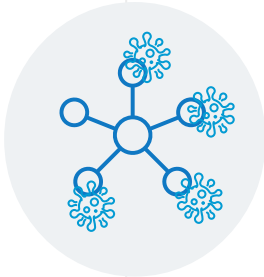
Phase 1

Initial Infection

Phase 2

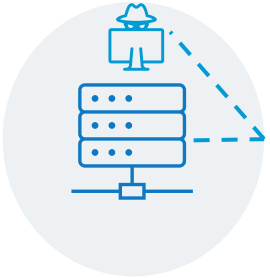
Privilege Escalation

Phase 3



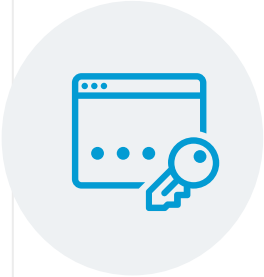
Lateral Movement

Phase 4



Data Exfiltration

Phase 5



Encryption

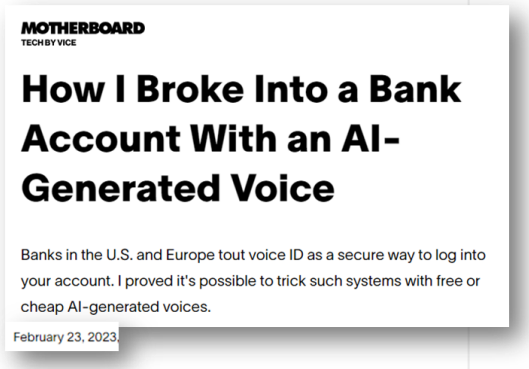
Phase 6

Incident Response

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Wir bauen Resilienz für unsere Geschäftsprozesse

Das Ausnutzen von einer Schwachstelle von Software-Produkten ist der häufigsten Wege für den Angriffsvektor für Ransomware-Gruppen. Social-Engineering Methoden kommen auch immer mehr zum Einsatz bei CEO-Fraud, Phishing oder Identitätsdiebstahl. Oftmals verwenden die Angreifer hier Künstliche-Intelligenz.
Das Ziel ist es Zugriff auf einen Account oder System zu bekommen.


MOTHERBOARD
TECH BY VICE

How I Broke Into a Bank Account With an AI-Generated Voice

Banks in the U.S. and Europe tout voice ID as a secure way to log into your account. I proved it's possible to trick such systems with free or cheap AI-generated voices.

February 23, 2023

Quelle: https://www.vice.com/en/article/dy7axa/how-i-broke-into-a-bank-account-with-an-ai-generated-voice

Wie können sich Unternehmen in dieser Phase schützen?

- Patch-Management ist eine **kontinuierliche** Aufgabe, da Sicherheitslücken unaufhörlich ausgenutzt werden.
- Ein gutes Zusammenspiel zwischen Schwachstellenmanagement & Patch-Management ist unabdingbar. **Deduplizierung** und **Priorisierung** helfen Ihnen den richtigen Fokus zu haben.
- **Multi-Faktor-Authentifizierung**, sekundäre Bestätigungsmethoden und biometrische Verhaltensmerkmale können zusätzliche Verifizierungsebenen bieten.
- Kontinuierliche **Sensibilisierung** von Mitarbeitern & Entscheidungsträgern mit Bezug auf das **private Leben**.

Bauen Sie eine offene Kultur des Vertrauens auf – Damit Personen Sicherheitsvorfälle rechtzeitig melden!

Initial Infection

Wir bauen Resilienz für unsere Geschäftsprozesse

Angreifer nutzen auch Desinformation, um Organisationen zu Fehler zu bewegen.
Das Ziel ist es Zugriff auf einen Account oder System zu bekommen. Oftmals versucht ein Angreifer über Fernzugänge die initiale Infektion zu starten.


US-BÖRSE

Wie ein KI-Bild den US-Leitindex abstürzen ließ

von Julia Groth
23. Mai 2023

Quelle: **WirtschaftsWoche** - https://www.wiwo.de/finanzen/boerse/us-boerse-wie-ein-ki-bild-den-us-leitindex-abstuerzen-liess/29164922.html

Wie können sich Unternehmen in dieser Phase schützen?

- Bauen Sie eine gute Übersicht Ihrer Fernzugänge auf – Generell sollten diese nur mittels **VPNs** und **Zwei-Faktor-Authentifizierung** genutzt werden.
- Zur Reduzierung von Phishing Angriffen sollten Emails rein als Text-Datei dargestellt werden, somit können sehen Sie immer den wirklichen Externen Link. Zusätzlich sind keine Scriptausführungen möglich.
- **Deaktivierung** von Virtual Basic and Active **Scripts / Makros** sollten deaktiviert sein.
- **Übersicht von IT-Assets** – 4/10 Sicherheitsvorfällen installieren Angreifer legitime Verkaufssoftware, um den Fernzugang herzustellen.

Bauen Sie einen kontinuierlichen Prozess auf, um eine gute Übersicht Ihrer IT-Assets zu erlangen.

nviso.eu

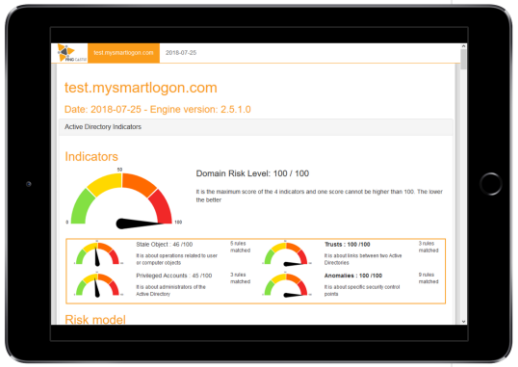
Phase 2

Privilege Escalation

Wir bauen Resilienz für unsere Geschäftsprozesse

In dieser Phase probieren Angreifer ihre Rechte zu erweitern und weitere Zugriffe zu erhalten. Insbesondere ist das Ziel administrative Berechtigungen zu erhalten.

Kostenlose Tools, wie Pingcastle, können Ihnen helfen Ihr AD zu sichern.



Quelle:https://www.pingcastle.com/documentation/healthcheck/

Quelle: IT-Grundschutz protection module APP2.2 Active Directory Domain Services

Wie können sich Unternehmen in dieser Phase schützen?

- Regelmäßige **Überwachung** & **Hygiene** von **Directory Services**, wie Active Directory. Wie beim Frühjahrs- & Sommer- / Winterputz achten Sie auf die Hygiene Ihres ADs.
- **Application Whitelisting** – nur zugelassene Programme dürfen ausgeführt werden. Somit wird dem Angreifer das Ausführen von Software untersagt.
- Härtung von IT Systemen durch Deaktivierung von „Default“ oder „unbenutzten“ Benutzern, Verwendung von sicheren Protokollen, Deaktivierung von ungenutzten Diensten,
- Reduktion von Admins & Aufbau von einem Tiered Admin

- Admins haben keinen Internetzugriff.

Beginnen Sie immer mit den kritischsten Systemen für Ihr Geschäft!

nviso.eu

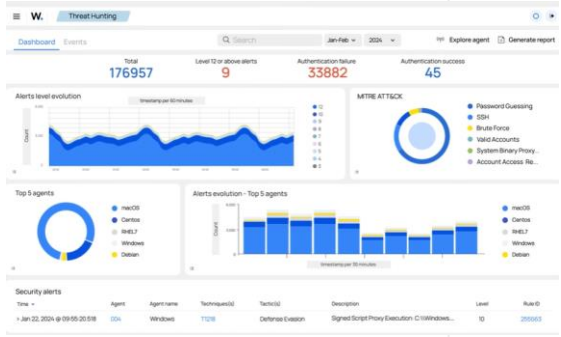
Phase 3

Lateral Movement

Wir bauen Resilienz für unsere Geschäftsprozesse

In dieser Phase probieren Angreifer ihre Rechte zu nutzen, um sich lateral im Netzwerk zu bewegen. Der Angreifer versucht beispielsweise auf das Backup-System oder Domain Controller zu kommen, um diesen kompromittieren. Damit sind die Auswirkungen von Ransomware-Angriffen besonders erfolgreich und drastisch.

Auf Open Source XDR & SIEM Lösungen können Ihnen im Abwehrkampf helfen!



Quelle:https://wazuh.com/

Wie können sich Unternehmen in dieser Phase schützen?

- Aufbau von Netzwerksegmentierung auf Basis eines Sicherheitskonzeptes.
- Verwendung von automatischer Antviren-Software nach dem aktuellsten Stand. Geben Sie diesen AVs Berechtigungen automatische Incident Response durchzuführen, indem Prozessausführungen blockiert werden oder ganze Geräte isoliert werden.
- Aufbau von **zentraler Überwachung** von **Logdaten**, um verdächtiges Verhalten in Ihrem Netzwerk festzustellen. Nutzen Sie hier jegliche Automatisierung, die Ihnen die Tools zur Verfügung stellen.
- Nutzen Sie eine **einheitliche Sprache**, um Angriffe zu verstehen – z.B. **MITRE ATT&CK**

Versuchen Sie soviel es geht zu automatisieren!

nviso.eu

Wir bauen Resilienz für unsere Geschäftsprozesse

In dieser Phase probieren Angreifer Daten zu abfiltrieren und diese in den Systemen sowie am Backup zu verschlüsseln.

Führen Sie regelmäßige Funktionale Restore Tests durch.

Wie können sich Unternehmen in dieser Phase schützen?

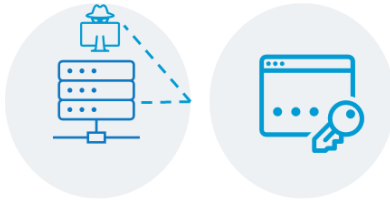
- **Back-ups** sind Ihre letzte Bastion – müssen aber gegen moderne Bedrohungen geschützt werden. Bauen Sie ein offline Backup auf, welches getrennt von Ihrem Netzwerk ist. Es ist wichtig, dass Sie entsprechende Pläne und Vorbereitungen testen, wie Sie den Neustart von Prozessen und Wiederherstellung von Daten durch das Backup ermöglichen. Ansonsten ist Ihr **Backup wertlos**.

- Kennen Sie die **Abhängigkeiten** von **Kerninfrastrukturelementen** und Ihren **Anwendungen**. Es hilft Ihnen nichts, wenn die Anwendung eine Wiederanlaufszeit von 24h hat und die unterliegende Infrastruktur nicht vor 3 Tagen vorhanden ist.

- Bauen Sie entsprechende **SLAs** mit Ihren **Dienstleistern** auf – damit Sie in der Krise entsprechende Hilfe erhalten.

Testen Sie Ihre Resilienz regelmäßig!

Phase 4 **Phase 5**



Data Exfiltration

Encryption

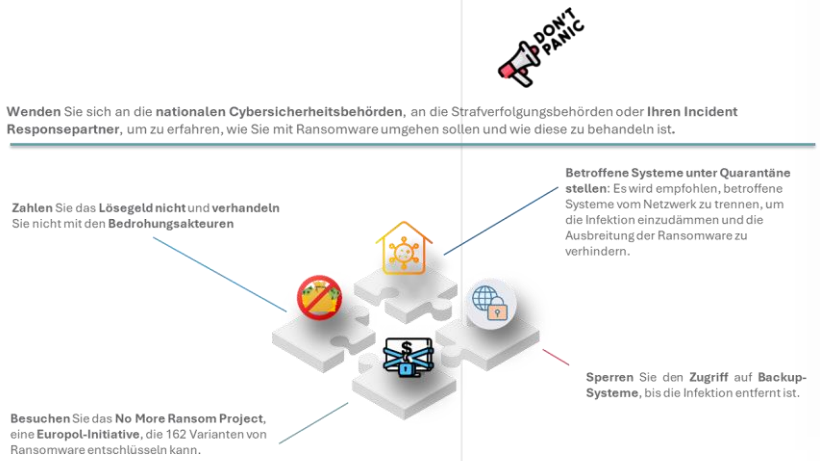
nviso.eu

Phase 6

Incident Response

Wir bauen Resilienz für unsere Geschäftsprozesse

In dieser Phase probieren Angreifer von Ihnen das Lösegeld zu erlangen



Wie können sich Unternehmen in dieser Phase schützen?

- Bauen Sie ein **Notfallplan** auf – in diesem sollten **Grundsätze** zu **Entscheidungsfindung** sowie Reaktionen [z.B**. Wir zahlen niemals das Lösegeld, wenn unser Backup funktioniert**] und **Kommunikationen** definieren.
- Bauen Sie Verträge mit 1-2 **Incident Response** Anbietern auf.
- Bauen Sie auch eine Grundlage, wie und wann Sie Ihr Unternehmen wieder aus der Krise herausmanövrieren. Eine Krise bedeutet Stress für alle Mitarbeiter. Es ist wichtig, dass der **Wiederanlauf** auch **definiert** ist und die entsprechenden Voraussetzungen auch durchdacht wurden [z.B. Welche Hardware müsste ich einkaufen für meine IT-Assets?]

Überlassen Sie die Verhandlung oder den Austausch mit der Organisierten Kriminalität Experten.

Praktische Ransomware Simulation

Testen Sie Ihre Resilienz gegen Ransomware-Angriffe durch eine ganz praktische Prüfung.

COMMERZBANK

Für Commerzbank-Kunden für nur 9.900 €

Gültig nur bis Ende Mai 2025

Unser Vorgehen:

Kick-Off
Wir einigen uns auf ein Szenario und die konkreten Rahmenbedingungen für die Simulation und halten diese in einem Simulationsplan fest.

Ausführung
Unsere sichere Ransomware wird auf den Zielsystemen ausgerollt. Je nach Szenario wird das IT Teamvon dem Angriff informiert oder nicht.

Entdeckung & Wiederherstellung
Ihr IT-Team entdeckt den Angriff und folgt den Playbooks zur Wiederherstellung der betroffenen Systeme.

Erkenntnis und Maßnahmenplan
Wir stellen die Lücken bei der Erkennung und Wiederherstellung fest und leiten die Maßnahmen zur Behebung ab.

Codename „Cardinalis“

Von NVISO‘s Red Team speziell für Ransomware-Simulationen entwickelte Ransomware.

Hauptmerkmale:

- **Realismus:** Entwickelt basierend auf dem Vorgehen echter Ransomware
- **Sicherheit**: Verschlüsselt nur die für die Simulation konfigurierten Dateien und Ordner
- **Unsichtbar**: Bietet fortschrittliche Techniken zur Umgehung von AV und EDR
- **Modularität**: Kann mit verschiedenen Funktionen ausgeführt werden, z. B. C2-Kommunikation
- **Protokollierung**: Integrierte Protokollierung zur Unterstützung des Blue Teams bei Untersuchungen und Folgemaßnahmen.

Interesse? Ich bin gerne persönlich für Sie da!

Julian Obenland-Recker
Geschäftsführer & Partner NVISO GmbH

E-Mail: julian.obenlandrecker@nviso.eu
Telefon: +49 171 301 77 86
Website: www.nviso.eu