

IT-Security you can trust.

Bewerten · Optimieren · Zertifizieren

Deutschland · Österreich

TÜV
TRUST IT
TÜV AUSTRIA Group

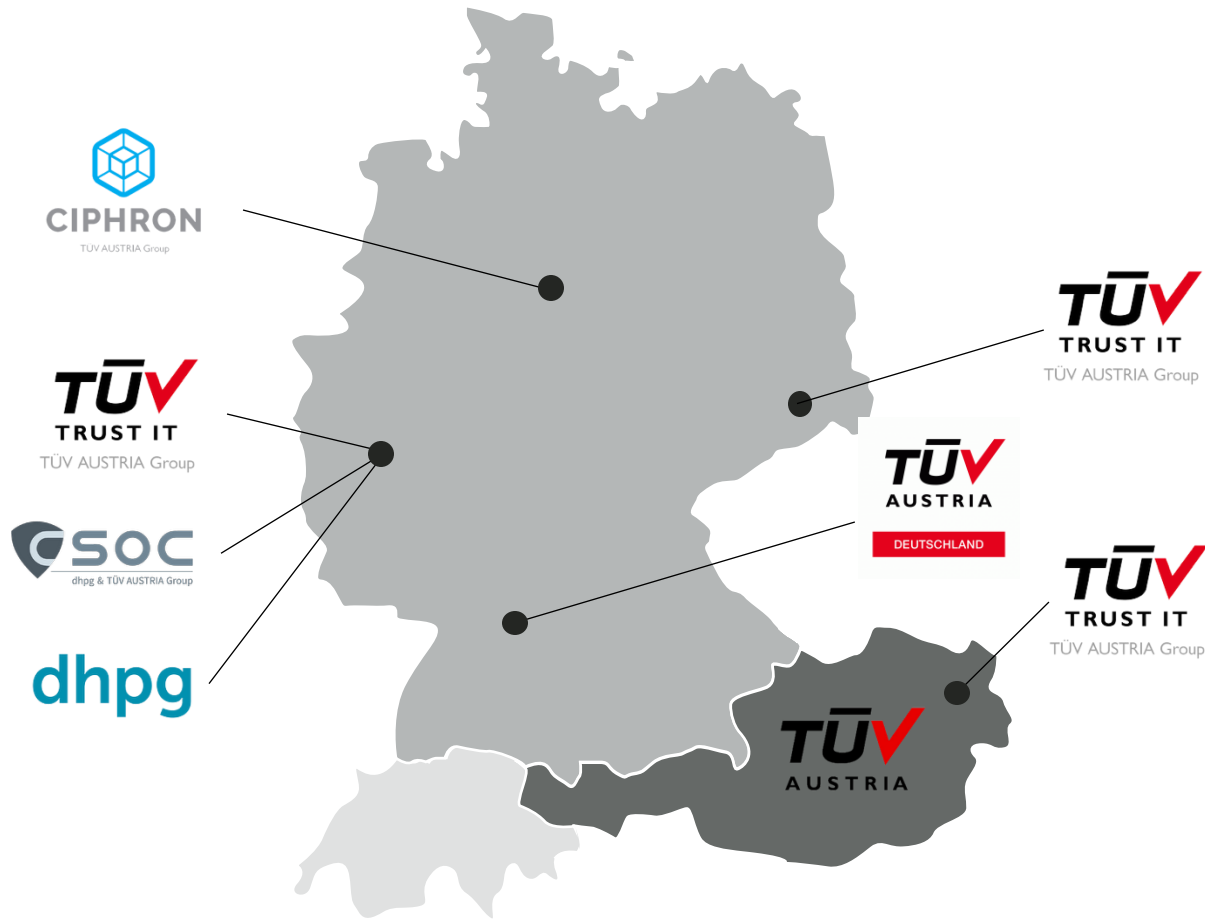
„Cybercrime im E-Commerce – Gefahren, Risiken und effektive Schutzmaßnahmen“

TÜV TRUST IT GmbH

Unternehmensgruppe TÜV AUSTRIA – gegründet 1872

- Beratung, Schulungen und Zertifizierungsleistungen zu Informationssicherheit, Datenschutz und Compliance
- Über 200 Sicherheitsexperten
- Erfahrene Spezialisten mit breitem Branchen Know-how
- Unsere Mission: Der Schutz Ihrer Informationswerte!





TÜV TRUST IT GmbH

Köln, Dresden, Wien

TÜV Austria Deutschland GmbH

Filderstadt (bei Stuttgart)

Certified Security Operations Center GmbH

Bornheim (bei Bonn)

CIPHRON GmbH

Hannover

dhpg (Konzern-Partner)

Bonn (Hauptsitz)

ISMS

- KRITIS / NIS-2
- ISO 27001
- DORA
- BSI IT G
- SWIFT CSCF
- TISAX

Business Continuity

- BCMS
- ISO 22301
- BSI 200-4
- Notfall-Übung (Cyber-Drill)

Offensive Security

- Penetration Testing
- Red Teaming
- V-Scanning
- Digital Health
 - TR-03161 (DiGa/DiPa)

Defensive Security

- SOC/SIEM
- Härtung, Resilienz
- Incident Response
- Cloud Security
- Forensik

Datenschutz & IT Legal

- DSMS
- DSGVO
- Cloud Security

eID & Trust Services

- eIDAS VO
- Audits
- Zertifizierung
- Support

SAP® Security

- Berechtigungsprüfung
- Sicherheitsprüfungen
- Workshops
- Zertifizierte SAP-Sicherheit

OT-Security

- Trusted IoT
- IEC 62443
- SOC / SIEM



Cyber incidents

(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)



Natural catastrophes¹

(e.g., storm, flood, earthquake, wildfire, extreme weather events)



Business interruption

(incl. supply chain disruption)



Changes in legislation and regulation

(e.g., new directives, protectionism, environmental, social, and governance, and sustainability requirements)



Climate change

(e.g., physical, operational and financial risks as a result of global warming)



Fire, explosion²



Political risks and violence

(e.g., political instability, war, terrorism, coup d'état, civil unrest, strikes, riots, looting)



Macroeconomic developments

(e.g., inflation, deflation, monetary policies, austerity programs)



Shortage of skilled workforce³



Market developments

(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)

The most
important
business risks
in 2025:
Europe

Was ist die Motivation / Hintergründe?

- Staatliches Hacking: Nordkorea, Iran, China, Russland (wollen in die Köpfe)
 - Gleiche Motivation, man hilft sich
- Hacktivismus (Gruppierungen), Sabotage, Spionage, Desinformation, Kriminalität
 - Verunsicherung, Demotivation, Unterbrechen von Dienstleistung, Business
- Hacker arbeiten vormittags für staatlichen Arbeitgeber – nachmittags dann kriminell für die eigene Brieftasche
- Lageberichte von Jahr zu Jahr immer gleiche Message: Bedrohungslage war noch nie so kritisch wie jetzt
=>Steigerung/Jahr
 - 70% aller Spam-Mails sind Angriffe (34% Erpressung, 32% Betrug, Ransomware größte Bedrohung)
- Nur eine kleine Anzahl an Vorfällen in den Medien
- Cyberangriffe laufen nicht schnell (3-12 Monate), taktisches und strategisches Vorgehen in kleinen Schritten
- Deep-Fakes / KI: erzeugen von Phishing-Angriffen mit fiktiven digitalen ID's, Voice und Video Fakes
- Tipp: Putin's Bären - Die gefährlichsten Hacker der Welt
<https://www.ardmediathek.de/video/putins-baeren/putins-baeren-die-gefaehrlichsten-hacker-der-welt/swr/Y3JpZDovL3N3ci5kZS9hZXggbzlwMDQ0NjI>

Wussten Sie, dass...

... Anwender bis
zu **130 digitale
Benutzerkonten**
haben?

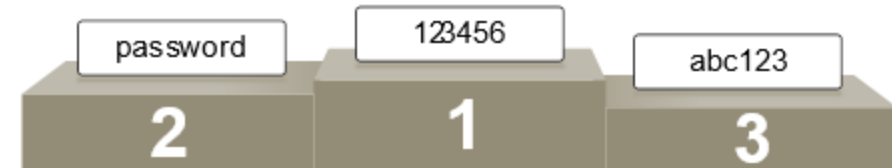
... Anwender **12 Tage
Ihres Lebens** damit
verbringen, nach
Ihren
Benutzernamen und
Passwörtern zu
suchen?



Frühere Passwortregeln führten zu schlechten User-Angewohnheiten:

- Die meisten Passwörter sind kürzer als 10 Zeichen
- 52% der Anwender benutzen dieselben Passwörter für mehrere Benutzerkonten
- Mehr als 80% der erfolgreichen Datenschutzverletzungen erfolgen mittels Brute Force oder dem Einsatz gestohlener oder verlorener Zugangsdaten

Lieblingspasswörter:



Verbreitete Passwörter:



32 %
Fantasiewörter
Leider leicht
zu knacken



21 %
**Geburtstag
oder
Haustiernamen**



11 %
**Lange, sichere
Sätze**
Sicher, aber
selten genutzt

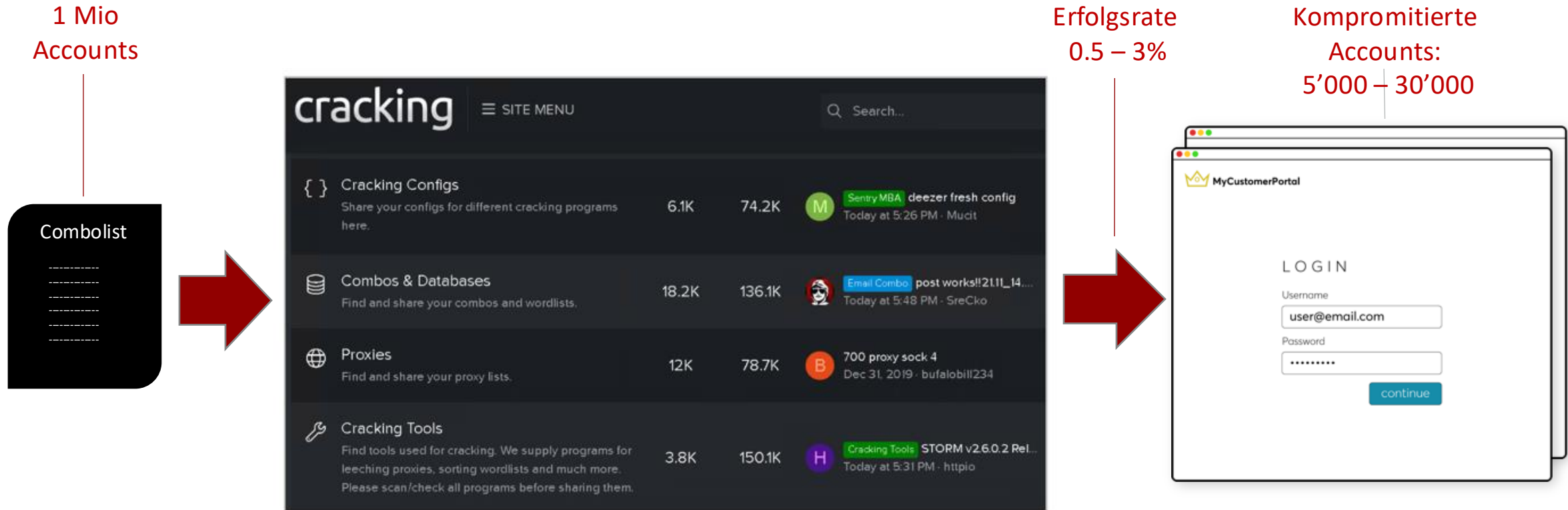
Bequem, aber nicht sicher – Mehrfach genutzte Passwörter

52 %
Nutzen ein Passwort
für mehrere Websites



13 %
Haben nur ein Passwort
für alles

Quelle: Verizon Data Breach Investigations Report 2020



Gestohlene Passwörter

- Phishing- oder Malware
- Data leaks
(z.B. Marriot, LinkedIn, Equifax, etc.)
- Kann im Darknet erworben werden
- Viel und mehrfach verwendete User/Passwort Kombinationen

Optimierte Tools für spezifische Ziele

- Bank Zugänge
- Cloud Speicher
- Spiele, Wetten und Glücksspiele
- Fluggesellschaften und Hotels
- Dating Portale
- E-Commerce Accounts/Handel

Attackierte Websites

- Bank Zugänge
- Cloud Speicher
- Spiele, Wetten und Glücksspiele
- Fluggesellschaften und Hotels
- Dating Portale
- E-Commerce Accounts/Handel
- etc...

Anbieter verdienen 3X

Millionen Bewerberdaten gefährdet

McDonalds AI-Bot mit Passwort „123456“ gehackt

16.07.2025 · Von [Melanie Staudacher](#) · 2 min Lesedauer · 

Peinlicher Fehler bei McDonalds: Sicherheitsforscher konnten sich Zugriff auf das Adminkonto der Bewerbungsplattform von McDonalds verschaffen und so sensible Bewerberdaten einsehen. Dies war mit wenig Aufwand möglich, da sie das Passwort für die Plattform einfach erraten konnten.



Die Datenbank von Paradox.ai, die Plattform, über die McDonalds den KI-Chatbot Olivia für seine Bewerber bereitstellt, war mit einem leicht zu erratenden Passwort gesichert.

(Bild: Dall-E / Vogel IT-Medien GmbH / KI-generiert)

Für den Recruiting-Prozess setzt das Fast-Food-Unternehmen McDonalds einen KI-Chatbot namens „Olivia“ ein. Über die Website „McHire“ stellt dort das KI-Softwareunternehmen Paradox.ai seine Lösung bereit. Olivia fragt die Kontaktdaten und Lebensläufe der Bewerberinnen und Bewerber ab, die gerne bei McDonalds arbeiten möchten, und beantwortet deren

Angriffsarten

- Phishing: Social Engineering über E-Mail, SMS oder Telefon
- Ransomware: Erpressung durch Datenverschlüsselung
- Man-in-the-Middle: Abhören & Manipulation von Datenverkehr
- Zero-Day Exploits: Ausnutzung unbekannter Schwachstellen
- Credential Stuffing: Automatisierte Nutzung gestohlener Zugangsdaten
- Supply-Chain-Angriffe: Kompromittierung von Drittanbietern oder Softwarelieferanten
- Advanced Persistent Threats (APT): Langfristige, gezielte Angriffe durch gut organisierte Gruppen, oft mit Spionage-Absicht



- Große Opferzahl
- Allgemein gehaltene Formulierung
- Verleiten Benutzer zu bestimmten Verhalten
- Design von Mails und Websites oft Nachahmung von bekannten Firmen
- Früher oft Fehler in Sprache und Grammatik
- Heute ist die Grammatik besser
- Erkennbarkeit wird immer schwieriger (KI)
- Next Level: „Spear-Phishing“

- Schulung und Sensibilisierung der Mitarbeiter
- Multi-Faktor-Authentifizierung (MFA)
- Authentifizierung von E-Mails: DKIM (Domain Keys Identified Mail) und SPF (Sender Policy Framework) oder Zertifikate zur Authentifizierung von E-Mails einsetzen.
- Firewalls und Sicherheitssoftware
- E-Mail-Filter
- Verschlüsselung von Daten
- Regelmässige Penetrationstests (Webseite+Infrastruktur)

- **SQL-Injection (SQLi):**
Angreifer fügen schädliche SQL-Befehle in Eingabefelder ein, um Datenbanken zu manipulieren.
- **Cross-Site Scripting (XSS):**
Einschleusen von JavaScript-Code in Webseiten, der im Browser des Opfers ausgeführt wird.
- **Cross-Site Request Forgery (CSRF):**
Angreifer bringt den Benutzer dazu, unbeabsichtigt eine Aktion auf einer vertrauenswürdigen Seite auszuführen.
(Ausnutzen des Session-Cookies)
- **Server-Side Request Forgery (SSRF):**
Angreifer zwingt den Server, interne oder externe Ressourcen abzurufen. (URL-/Pfadangaben..., ohne Validierung)
- **Denial of Service (DoS) / Distributed DoS (DDoS):**
Überlastung der Anwendung durch massenhafte Anfragen.
- **Session Hijacking:**
Diebstahl von Session-Cookies, um sich als Benutzer auszugeben.

- **Command Injection:**
Einschleusen von Systembefehlen über unsichere Eingaben, um Server-Kommandos auszuführen.
- **Broken Authentication:**
Schwache oder fehlerhafte Authentifizierungsmechanismen ermöglichen Kontoübernahme.
- **Business Logic Attacks:**
Ausnutzen von Schwächen in der Geschäftslogik, z. B. Umgehen von Zahlungsprozessen.
- **Clickjacking:**
Benutzer wird dazu gebracht, versteckte Buttons oder Links in einer E-Mail zu klicken und Nutzung einer offenen Webanwendung.
- **Path Manipulation:**
Manipulation von Dateipfaden, um Zugriff auf nicht vorgesehene Ressourcen zu erhalten.
 - **Directory Traversal:**
Zugriff auf Dateien außerhalb des vorgesehenen Verzeichnisses durch Manipulation von Pfadangaben.
 - **File Inclusion (LFI/RFI):**
Einbinden lokaler oder externer Dateien in die Anwendung, oft für Codeausführung.

Beispiel: Login Bypass mittels SQL Injection

- Unsicherer Code für Login
- Eingabe wird ohne Validierung eingebettet

```
var username = input.username;
var password = input.password;

function login(username, password){
    sql = "SELECT user FROM users WHERE username='" + username + "' and password='" + password + "'";
```

- Eingabe von "administrator'--"

```
SELECT user FROM users WHERE username=''and password=''
```

```
SELECT user FROM users WHERE username='administrator'--' and password=''
```

- Login als Administrator möglich

- HTTP Security-Header (Aktivierung von Schutz-Attributen)
- Input Validierung bei Eingabefelder
- Sichere Kommunikation (Verschlüsselte Datenübertragung, HTTPS)
- Session-/ Token-Management (Session-Timeout)
- Patchmanagement (Fokus Third-Party)
- Authentifizierung (z.B. Counter bei Falscheingabe)
- Cookie-Einstellungen (Sicherheitsattribute aktivieren)
- Rate-Limiting (Limitierung der Anfragerate auf Webseiten)

....

Niemand ist sicher. Cyberkriminelle greifen Unternehmen jeder Größe und aus jeder Branche an – auch in Deutschland. Diese Unternehmen erlitten im Jahr 2025 bisher einen Cyberangriff...

- <https://www.security-insider.de/cyberangriffe-auf-unternehmen-in-deutschland-2025-analyse-a-f71268d8ef2cc593d2cc64a82df23ee2/?cmp=nl-ed617ce-bb32-418b-8967-bc79e3a81876&uuid=D99EEC75-36C9-4770-BF58-6782FC1E4134>

Inhaltsverzeichnis:

Cyberangriffe September 2025 in Deutschland

Cyberangriffe August 2025 in Deutschland

Cyberangriffe Juli 2025 in Deutschland

Cyberangriffe Juni 2025 in Deutschland

Cyberangriffe Mai 2025 in Deutschland

Cyberangriffe April 2025 in Deutschland

Cyberangriffe März 2025 in Deutschland

Cyberangriffe Februar 2025 in Deutschland

Cyberangriffe Januar 2025 in Deutschland

Die Bedrohungslage in Deutschland ist „besorgniserregend“, heißt es vom Bundesamt für Sicherheit in der Informationstechnik (BSI). Neben aktuell 309.000 neuen Malware-Varianten pro Tag werden auch Large Language Models (LLMs) immer häufiger von Cyberkriminellen missbraucht. Das Resultat: Laut Blackberry gibt es 37.000 Cyberangriffe weltweit pro Tag. Check Point zufolge haben deutsche Organisationen mit 1.220 Cyberattacken pro Woche zu kämpfen – Tendenz steigend. Dass die Bedrohungslage in Deutschland

anhaltend hoch ist, bestätigt auch das Bundeslagebild Cybercrime 2024 des Bundeskriminalamts.

Watchguard warnt vor KI-Krieg

Malware-Flut erreicht neuen Höchststand

29.07.2025 · Quelle: Pressemitteilung · 2 min Lesedauer · 

Laut Watchguard explodiert die Malware-Zahl im ersten Quartal 2025. KI macht Phishing glaubwürdiger und Angriffe effizienter. Während Ransomware abnimmt, nehmen Zero-Day-Exploits und getarnte Angriffe stark zu.



Auf Basis der Daten der „Unified Security Platform“ analysiert Watchguard regelmäßig Cyberbedrohungen. In diesem Jahr verzeichnete der Hersteller den höchsten Malware-Wert aller Zeiten.

(Bild: rolffimages - stock.adobe.com)

Die schlechte Nachricht des „Internet Security Reports“  von Watchguard ist, dass es im ersten Quartal 2025 171 Prozent mehr **Malware** gab als im Vergleich zum ersten Quartal 2024. Dies ist der höchste Wert den die Experten des Security-Anbieters jemals verzeichnet haben. Die gute

Ransomware

Fasana stellt Insolvenzantrag nach Cyberangriff

24.06.2025 · Von Melanie Staudacher · 2 min Lesedauer · 

Der Serviettenhersteller Fasana erlitt einen Ransomware-Angriff. Weil daraufhin nicht mehr produziert werden konnte, meldete das Unternehmen Insolvenz an. Fasana sucht nun nach einem Käufer, damit die rund 240 Stellen gerettet werden können.



Nachdem ein Ransomware-Angriff die IT-Systeme und somit auch die Produktion lahmlegte, sucht Fasana nun nach einem Käufer.

(Bild: © Coloures-Pic - stock.adobe.com)

Am 19. Mai 2025 funktionierte in der Papierserviettenfabrik Fasana aus Euskirchen nichts mehr. Sämtliche Drucker hätten nur noch ein Erpresserschreiben geliefert, anstelle der angeforderten Dokumente, wie die Kölnisch Rundschau **berichtete** . Sämtliche Lapotps und PC seien plötzlich nutzlos gewesen, die Produktion habe infolge eines Cyberangriffs still gestanden. Nur Aufträge, die noch in den Druckmaschinen gespeichert gewesen seien, hätten noch ausgeführt werden können.

- Auszug...
 - Auch E-Mail-Adressen, Social-Media-Accounts, Messenger-Accounts und SMS-fähige Telefonnummern bieten laut BSI weiterhin große Angriffsflächen. Im aktuellen Berichtszeitraum – von Juli 2024 bis Juni 2025 – wurden durchschnittlich **119 neue Schwachstellen pro Tag** bekannt, ...
 - Größte Bedrohungen für Deutschland: Cybercrime-as-a-Service bleibe weit verbreitet. Insbesondere **Ransomware-as-a-Service**. Hauptbetroffene seien weiterhin kleine und mittlere Unternehmen.
 - Maliziöse Webseiten, die das Ziel verfolgen Phishing-Attacken auszuführen oder Schadcode zu verbreiten, würden stark zunehmen. Weltweit entstünden über **800 neue Phishing-Seiten pro Tag**, die meist nur wenige Stunden aktiv seien.

Jahr	Neue Schwachstellen pro Tag im Schnitt	Veränderung zum Vorjahr
2022	68	
2023	78	+ 14 Prozent
2024	96	+ 23 Prozent
2025	119	+ 24 Prozent

Claudia Plattner:
„Unser Job,
Geschwindigkeit schaffen,
Angriffsfläche verringern“
17.11.2025

Das Wichtigste in Kürze:

- Der staatliche und polizeiliche Druck auf Unternehmen wurde erhöht. Einige Regierungen, wie die der USA oder Australiens, haben ein Zahlungsverbot von Lösegeld eingeführt oder drohen damit, was wiederum für die Opfer die Kosten-Risiko-Rechnung verändert.
- Zwar brachen große Ransomware-as-a-Service-Gruppen zusammen, doch kleinere Gruppierungen und Einzelakteure sind nach wie vor sehr aktiv.
- Ransomware-Banden fokussieren sich zunehmend auf dreifache Erpressung.
- Die Angreifer nutzen KI nicht nur für Phishing, sondern auch für Verhandlungs-Bots und Affiliate-gesteuerte Kartell-Modelle.

<https://www.security-insider.de/ransomware-ki-kartell-modelle-dreifache-erpressung-a-f4eecde224cddb6f5568fa300ff3030/?cmp=nl-dd8677e7-3d55-4684-9757-84c3e76ddfb1&uuid=D99EEC75-36C9-4770-BF58-6782FC1E4134>

Quelle: Security-insider.de

Opfer, Modelle und Tools

So arbeiten Ransomware-Gruppen heute

15.08.2025 · Quelle: Pressemitteilung · 5 min Lesedauer · 

Ransomware-Gruppen setzen auf KI, Kartell-Modelle und dreifache Erpressung. Laut Check Point ist das Ökosystem fragmentierter denn je – und stellt Unternehmen vor neue Herausforderungen bei Verteidigung, Prävention und Risikoabwägung.



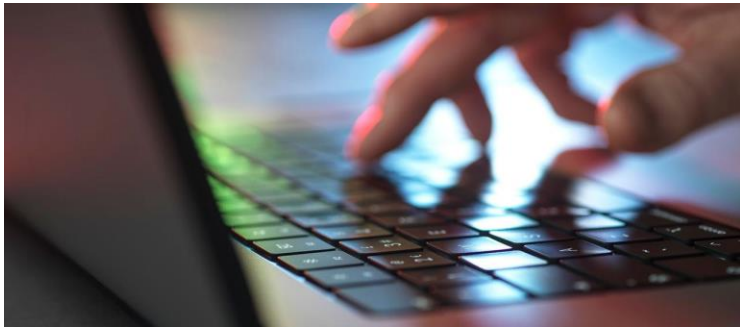
Die Analysten von Check Point werfen einen Blick auf die aktuellen Techniken, Taktiken und Verkaufsmodelle von Ransomware-Akteuren.

(Bild: mikkellwilliam via Getty Images)

Die Sicherheitsforscher von Check Point haben den Report „[The State of Ransomware](#)“  für das zweite Quartal 2025 veröffentlicht.

„Deutschland größtes Hacker-Ziel in der Europäischen Union (Platz 4 der Top 10 WW)

Kriminelle Hacker nehmen weiterhin Firmen, Organisationen und private Anwender ins Visier.“



Quellen:

- <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf?page=1>
- <https://www.tagesschau.de/wirtschaft/digitales/microsoft-hacker-102.html>

Russische Angriffe auf NATO-Staaten und Ukraine

- Die größte Gefahr im Cyberraum geht dem Report zufolge von Hackern aus Russland, China, Nordkorea und dem Iran aus. Russland nutze Hackergruppen vor allem dazu, um die Ukraine und NATO-Mitgliedsstaaten anzugreifen. Nordkorea, aber auch dem Iran gehe es hauptsächlich darum, mit Ransomware-Angriffen Geld für staatliche Zwecke zu erpressen.
- Bei klassischen Angriffen versuchen Hacker vor allem, sich die Zugangsdaten zu den Anwenderkonten zu beschaffen. Dabei agieren die Angreifer vor allem mit Phishing-E-Mails, mit denen die Opfer dazu verleitet werden sollen, ihre Zugangsdaten auf einem gefälschten System anzugeben.
- Microsoft ist der größte Softwarehersteller der Welt. Laut Aussagen der Experten des Konzerns ließen sich **99,9 Prozent dieser Angriffe durch eine Multi-Faktor-Authentifizierung abwehren.**

Welche gibt es?

- NIST Cybersecurity Framework: Erkennen, Schützen, Reagieren
- OWASP Top 10: Häufigste Schwachstellen in Webanwendungen, KI, API, etc.
- ISO 27001: Informationssicherheitsmanagementsystem
- BSI IT-Grundschutz: Deutsche Standards für IT-Sicherheit
- BSI TR-03161: Anforderungen an Anwendungen im Gesundheitswesen
- IEC 62443(-4-1): Secure product development lifecycle requirements

Ihr Mehrwert: **sicher Digitalisieren**



Holger Hinzmann

Senior Account Manager

Mobil: 0151 – 195 29610

holger.hinzmann@tuv-austria.com



TÜV TRUST IT GmbH

Unternehmensgruppe TÜV AUSTRIA

Waltherstraße 49 – 51

51069 Köln

Phone: +49 221 96 97 89 0

www.it-tuv.com