


---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250309



## Inhaltsverzeichnis

<b>1 Editorial</b>	<b>2</b>
<b>2 Security-News</b>	<b>3</b>
2.1 Heise - Security-Alert . . . . .	3
<b>3 Sicherheitslücken</b>	<b>3</b>
3.1 EPSS . . . . .	3
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . . .	3
3.2 BSI - Warn- und Informationsdienst (WID) . . . . .	5
3.3 Sicherheitslücken Meldungen von Tenable . . . . .	9
<b>4 Die Hacks der Woche</b>	<b>10</b>
4.0.1 Private video . . . . .	10
<b>5 Cyberangriffe: (Mär)</b>	<b>11</b>
<b>6 Ransomware-Erpressungen: (Mär)</b>	<b>11</b>
<b>7 Quellen</b>	<b>16</b>
7.1 Quellenverzeichnis . . . . .	16
<b>8 Impressum</b>	<b>18</b>

## 1 Editorial

Guten Morgen,

willkommen zum Cybersecurity Morgenreport von Cyberwald, Ihrem täglichen Begleiter in der Welt der IT-Sicherheit. Als nicht-kommerzielles Projekt ist es unser Anliegen, Awareness und Wissen rund um das Thema Cybersecurity kostenlos zu vermitteln. In der heutigen digitalen Welt ist es für Unternehmen von entscheidender Bedeutung, sich über aktuelle Sicherheitsrisiken zeitnah zu informieren. Cyberbedrohungen entwickeln sich ständig weiter und können erhebliche Schäden verursachen, wenn sie nicht rechtzeitig erkannt und abgewehrt werden. Durch die Nutzung aktueller Informationen können Unternehmen ihre IT-Sicherheitsmaßnahmen stärken und sich effektiv gegen diese Bedrohungen schützen.

Unser Ziel ist es, Ihnen, den IT-Verantwortlichen, einen kompakten und leicht verständlichen Überblick über aktuelle Sicherheitsrisiken zu geben. Wir präsentieren Ihnen täglich Sicherheitsmeldungen und Berichte über neue Sicherheitslücken, die Ihre Systeme und Daten bedrohen könnten.

Darüber hinaus listen wir aktuelle Cyberangriffe und Ransomware-Vorfälle auf. Dies ist von besonderer Bedeutung, da es Unternehmen ermöglicht, sich auf mögliche Supply-Chain- und Phishing-Angriffe vorzubereiten. Durch das Verständnis der Methoden und Taktiken, die von Cyberkriminellen verwendet werden, können Unternehmen ihre Verteidigungsmaßnahmen entsprechend anpassen und stärken.

Für den Cybersecurity Morgenreport greifen wir automatisiert auf öffentliche Informationsquellen zu, filtern und sortieren diese Informationen, um sie Ihnen in einer übersichtlichen Form zur Verfügung zu stellen. Wir bemühen uns, die Inhalte so verständlich wie möglich zu gestalten und vorzugsweise vollständig in deutscher Sprache wiederzugeben. Bei Bedarf übersetzen wir die öffentlichen Informationen und fassen sie durch eine KI zusammen.

Der Cybersecurity Morgenreport ist ein dynamisches Projekt. Wir passen und erweitern unsere Inhalte ständig, um Ihnen die relevantesten und aktuellsten Informationen zu liefern. Derzeit befinden wir uns im Alpha-Stadium des Projekts und freuen uns über Ihr Feedback und Ihre Anregungen.

Wir hoffen, dass der Cybersecurity Morgenreport Ihnen hilft, Ihre IT-Sicherheitsmaßnahmen zu verbessern und Ihre Systeme vor den ständig wechselnden Bedrohungen zu schützen. Bleiben Sie sicher und informiert mit dem Cybersecurity Morgenreport von Cyberwald.

Ihr Cyberwald-Team

## 2 Security-News

### 2.1 Heise - Security-Alert

## 3 Sicherheitslücken

Eine Sicherheitslücke oder Schwachstelle ist ein Fehler in einer Software oder Hardware, der es einem Angreifer ermöglicht, in ein Computersystem einzudringen und Schaden anzurichten. Diese Lücke stellt eine Bedrohung für die Sicherheit des Systems dar, da sie ausgenutzt werden kann, um das System zu kompromittieren. Sicherheitslücken entstehen oft durch unzureichenden Schutz des Computers vor Netzwerkangriffen, zum Beispiel durch fehlende Firewall oder andere Sicherheitssoftware. Auch Programmierfehler im Betriebssystem, Webbrowser oder anderen Anwendungen können Sicherheitslücken verursachen. Bekannte Sicherheitslücken sollten daher so schnell wie möglich durch das Einspielen eines Patches geschlossen werden, um die Angriffsfläche der IT-Systeme zu verringern.

### 3.1 EPSS

Das Exploit Prediction Scoring System wird für eine bekannte Software-Sicherheitslücke / CVE auf einer Skala von 0 (0%) bis 1 (100%) angegeben und soll die Wahrscheinlichkeit für das Auftreten eines Exploits in naher Zukunft darstellen. Ein höherer Wert bedeutet eine höhere Wahrscheinlichkeit, dass eine Schwachstelle in naher Zukunft ausgenutzt wird. EPSS kann auch als Rahmen für die Priorisierung von Schwachstellen unter Verwendung einer Kombination von Metriken betrachtet werden. Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

#### 3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2025-0108	0.967640000	0.997970000	<a href="#">Link</a>
CVE-2024-9474	0.974550000	0.999800000	<a href="#">Link</a>
CVE-2024-9465	0.939910000	0.993870000	<a href="#">Link</a>
CVE-2024-9463	0.961860000	0.996720000	<a href="#">Link</a>
CVE-2024-8963	0.966010000	0.997650000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-7593	0.967500000	0.997960000	<a href="#">Link</a>
CVE-2024-6670	0.904230000	0.991220000	<a href="#">Link</a>
CVE-2024-5910	0.967810000	0.998000000	<a href="#">Link</a>
CVE-2024-55956	0.968970000	0.998310000	<a href="#">Link</a>
CVE-2024-53704	0.960740000	0.996530000	<a href="#">Link</a>
CVE-2024-5217	0.948330000	0.994790000	<a href="#">Link</a>
CVE-2024-50623	0.969520000	0.998460000	<a href="#">Link</a>
CVE-2024-50603	0.924330000	0.992560000	<a href="#">Link</a>
CVE-2024-4879	0.952210000	0.995250000	<a href="#">Link</a>
CVE-2024-4577	0.951770000	0.995210000	<a href="#">Link</a>
CVE-2024-4358	0.921450000	0.992370000	<a href="#">Link</a>
CVE-2024-41713	0.957210000	0.995950000	<a href="#">Link</a>
CVE-2024-40711	0.964240000	0.997240000	<a href="#">Link</a>
CVE-2024-4040	0.967700000	0.997980000	<a href="#">Link</a>
CVE-2024-38856	0.941790000	0.994050000	<a href="#">Link</a>
CVE-2024-36401	0.961880000	0.996720000	<a href="#">Link</a>
CVE-2024-3400	0.958850000	0.996200000	<a href="#">Link</a>
CVE-2024-3273	0.937240000	0.993620000	<a href="#">Link</a>
CVE-2024-32113	0.938440000	0.993720000	<a href="#">Link</a>
CVE-2024-28995	0.969950000	0.998570000	<a href="#">Link</a>
CVE-2024-28987	0.957000000	0.995900000	<a href="#">Link</a>
CVE-2024-27348	0.960910000	0.996550000	<a href="#">Link</a>
CVE-2024-27198	0.970470000	0.998740000	<a href="#">Link</a>
CVE-2024-24919	0.963920000	0.997130000	<a href="#">Link</a>
CVE-2024-23897	0.973580000	0.999570000	<a href="#">Link</a>
CVE-2024-2389	0.928740000	0.992860000	<a href="#">Link</a>
CVE-2024-23692	0.967310000	0.997910000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-21893	0.960410000	0.996470000	<a href="#">Link</a>
CVE-2024-21887	0.973690000	0.999610000	<a href="#">Link</a>
CVE-2024-20767	0.964870000	0.997370000	<a href="#">Link</a>
CVE-2024-1709	0.957060000	0.995910000	<a href="#">Link</a>
CVE-2024-1212	0.946600000	0.994560000	<a href="#">Link</a>
CVE-2024-0986	0.954890000	0.995610000	<a href="#">Link</a>
CVE-2024-0195	0.962680000	0.996900000	<a href="#">Link</a>
CVE-2024-0012	0.969610000	0.998500000	<a href="#">Link</a>

### 3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 07 Mar 2025

**[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Fri, 07 Mar 2025

**[UPDATE] [hoch] Kibana: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, authentifzierter Angreifer kann eine Schwachstelle in Kibana ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 07 Mar 2025

**[NEU] [hoch] Linux Kernel: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um nicht spezifizierte Auswirkungen zu erzeugen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Fri, 07 Mar 2025

***[UPDATE] [hoch] Ansible: Mehrere Schwachstellen ermöglichen Ausführen von beliebigem Programmcode***

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Ansible ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 07 Mar 2025

***[UPDATE] [hoch] Squid: Mehrere Schwachstellen***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.

- [Link](#)

—

Fri, 07 Mar 2025

***[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

—

Fri, 07 Mar 2025

***[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

—

Fri, 07 Mar 2025

***[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Denial of Service***

Ein Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um einen Denial of Service Angriff durchzuführen oder nicht näher beschriebene Auswirkungen zu erzielen.

- [Link](#)

—

Fri, 07 Mar 2025

***[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen***

Ein Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um einen Denial of Service Zustand herbeizuführen oderum einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Fri, 07 Mar 2025

***[UPDATE] [hoch] IBM QRadar SIEM (Log Source Management App): Mehrere Schwachstellen***

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in IBM QRadar SIEM ausnutzen, um einen Cross-Site-Scripting-Angriff zu starten, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu erzeugen, Daten zu manipulieren, vertrauliche Informationen offenzulegen und Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—

Fri, 07 Mar 2025

**[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht SQL Injection und Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um eine SQL Injection durchzuführen und in der Folge beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 07 Mar 2025

**[UPDATE] [hoch] libxml2: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in libxml2 ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder einen nicht näher spezifizierten Angriff zu starten.

- [Link](#)

—

Fri, 07 Mar 2025

**[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Linux und Ubuntu Linux ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 07 Mar 2025

**[UPDATE] [hoch] GitLab: Mehrere Schwachstellen**

Ein entfernter authentisierter Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um Cross-Site-Scripting-Angriffe durchzuführen und vertrauliche Informationen preiszugeben. Skripting-Angriff.

- [Link](#)

—

Fri, 07 Mar 2025

**[UPDATE] [hoch] VMware ESXi: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in VMware ESXi, VMware Workstation, VMware Fusion und VMware Cloud Foundation ausnutzen, um beliebigen Code auszuführen, erhöhte Rechte zu erlangen und vertrauliche Informationen preiszugeben.

- [Link](#)

—



Fri, 07 Mar 2025

**[UPDATE] [hoch] Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um Spoofing-Angriffe durchzuführen, Sicherheitsmaßnahmen zu umgehen, erhöhte Privilegien zu erlangen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, Daten zu manipulieren, beliebigen Code auszuführen oder nicht spezifizierte Auswirkungen zu verursachen.

- [Link](#)

—

Fri, 07 Mar 2025

**[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen ermöglichen Denial of Service**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Thu, 06 Mar 2025

**[NEU] [hoch] Apache Traffic Server: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache Traffic Server ausnutzen, um Sicherheitsvorkehrungen zu umgehen und weitere, nicht spezifizierte Auswirkungen zu erzielen.

- [Link](#)

—

Thu, 06 Mar 2025

**[UPDATE] [hoch] GitLab: Mehrere Schwachstellen**

Ein entfernter authentisierter Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um Cross-Site-Scripting-Angriffe durchzuführen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, erhöhte Berechtigungen zu erlangen und Daten zu manipulieren.

- [Link](#)

—

Thu, 06 Mar 2025

**[NEU] [hoch] Axis Axis OS: Mehrere Schwachstellen**

Ein entfernter authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Axis Axis OS ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und erhöhte Rechte zu erlangen.

- [Link](#)

—

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/7/2025	[Oracle Linux 8 : firefox (ELSA-2025-2452)]	critical
3/7/2025	[LibreOffice 24.8.x < 24.8.5 / 25.2.x < 25.2.1 (cve-2025-1080)]	critical
3/7/2025	[Fortinet Fortigate RADIUS Protocol CVE-2024-3596 (FG-IR-24-255)]	critical
3/7/2025	[Fortinet FortiWeb RADIUS Protocol CVE-2024-3596 (FG-IR-24-255)]	critical
3/6/2025	[Linux Distros Unpatched Vulnerability : CVE-2025-21826]	critical
3/6/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-58085]	critical
3/6/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-58076]	critical
3/6/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-58052]	critical
3/6/2025	[Linux Distros Unpatched Vulnerability : CVE-2025-21833]	critical
3/6/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-58051]	critical
3/6/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-58077]	critical
3/6/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-58062]	critical
3/6/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-58074]	critical
3/6/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-58082]	critical
3/7/2025	[Amazon Linux AMI : kernel (ALAS-2025-1963)]	high
3/7/2025	[Amazon Linux AMI : kernel (ALAS-2025-1962)]	high
3/7/2025	[Amazon Linux 2023 : libtirpc, libtirpc-devel (ALAS2023-2025-890)]	high
3/7/2025	[Amazon Linux 2023 : aws-kinesis-agent (ALAS2023-2025-889)]	high
3/7/2025	[Amazon Linux AMI : kernel (ALAS-2025-1961)]	high
3/7/2025	[Kibana 8.15.x < 8.17.3 (ESA_2025_06)]	high

Datum	Schwachstelle	Bewertung
3/7/2025	[Cisco Secure Client for Windows with Secure Firewall Posture Engine DLL Hijacking (cisco-sa-secure-dll-injection-AOyzEqSg)]	high
3/6/2025	[Linux Distros Unpatched Vulnerability : CVE-2025-21831]	high
3/6/2025	[Debian dsa-5875 : chromium - security update]	high

## 4 Die Hacks der Woche

mit Martin Haunschmid

### 4.0.1 Private video

Vorschaubild [Zum Youtube Video](#)

## 5 Cyberangriffe: (Mär)

Datum	Opfer	Land	Information
2025-03-06	Bikur Rofeh	[ISR]	<a href="#">Link</a>
2025-03-05	Ålands Centralandelslag (ÅCA)	[FIN]	<a href="#">Link</a>
2025-03-05	Endless Mountains Health Systems (EMHS)	[USA]	<a href="#">Link</a>
2025-03-04	Unikorn Semiconductor Corp.	[TWN]	<a href="#">Link</a>
2025-03-04	Stadtwerke Schwerte	[DEU]	<a href="#">Link</a>
2025-03-04	Adina Hotels	[AUS]	<a href="#">Link</a>
2025-03-03	Whitman Hospital and Medical Clinics	[USA]	<a href="#">Link</a>
2025-03-03	Mission, Texas	[USA]	<a href="#">Link</a>
2025-03-02	HomeTeamNS	[SGP]	<a href="#">Link</a>
2025-03-02	POLSA (Polish Space Agency)	[POL]	<a href="#">Link</a>
2025-03-02	Adval Tech Group	[CHE]	<a href="#">Link</a>
2025-03-02	Penn-Harris-Madison school district	[USA]	<a href="#">Link</a>
2025-03-02	Ivinhema	[BRA]	<a href="#">Link</a>
2025-03-02	Berkeley Research Group (BRG)	[USA]	<a href="#">Link</a>
2025-03-01	National Presto Industries, Inc.	[USA]	<a href="#">Link</a>

## 6 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-08	[www.dcarosolutions.com]	ransomhub	<a href="#">Link</a>
2025-03-06	[mitchellmcnutt.com]	ransomhub	<a href="#">Link</a>
2025-03-07	[www.jpwindustries.com]	ransomhub	<a href="#">Link</a>
2025-03-08	[univ-rennes.fr]	funksec	<a href="#">Link</a>
2025-03-05	[Tech NH]	lynx	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-07	[Allworx]	bianlian	<a href="#">Link</a>
2025-03-07	[Minnesota Orthodontics]	bianlian	<a href="#">Link</a>
2025-03-07	[REYCOTEL]	arcusmedia	<a href="#">Link</a>
2025-03-07	[total-ps.com]	ransomhub	<a href="#">Link</a>
2025-03-07	[Hancock Public School]	interlock	<a href="#">Link</a>
2025-03-07	[Auctions !]	funksec	<a href="#">Link</a>
2025-03-07	[lofotenseafood.com]	lynx	<a href="#">Link</a>
2025-03-07	[ADDA (adda.io)]	ransomexx	<a href="#">Link</a>
2025-03-04	[www.cdg.us]	qilin	<a href="#">Link</a>
2025-03-07	[Swift Haulage Berhad]	akira	<a href="#">Link</a>
2025-03-07	[Strike on vacation my friend]	funksec	<a href="#">Link</a>
2025-03-07	[Aj Taylor Electrical Contractors Ltd]	sarcoma	<a href="#">Link</a>
2025-03-07	[Sittab INC]	akira	<a href="#">Link</a>
2025-03-07	[wheats.com]	ransomhub	<a href="#">Link</a>
2025-03-07	[srmg.com.au]	ransomhub	<a href="#">Link</a>
2025-03-07	[ACDC Express]	lynx	<a href="#">Link</a>
2025-03-07	[sorbonne-universite.fr]	funksec	<a href="#">Link</a>
2025-03-06	[RFA Decor]	akira	<a href="#">Link</a>
2025-03-05	[www.portlandschools.org]	ransomhub	<a href="#">Link</a>
2025-03-05	[www.hinton.ca]	ransomhub	<a href="#">Link</a>
2025-03-06	[Tugwell Pump & Supply]	lynx	<a href="#">Link</a>
2025-03-05	[www.centersheetmetal.com]	ransomhub	<a href="#">Link</a>
2025-03-05	[www.convention.qc.ca]	ransomhub	<a href="#">Link</a>
2025-03-06	[hickorylaw.com]	ransomhub	<a href="#">Link</a>
2025-03-06	[lovesac.com]	ransomhub	<a href="#">Link</a>
2025-03-06	[agi.net]	monti	<a href="#">Link</a>
2025-03-06	[Adval Tech]	lynx	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-06	[WJCC Public Schools (wjccschools.org)]	fog	<a href="#">Link</a>
2025-03-06	[Connekted, Inc.]	qilin	<a href="#">Link</a>
2025-03-06	[Dynamic Closures]	lynx	<a href="#">Link</a>
2025-03-06	[Naples Heritage Golf & Country Club]	incransom	<a href="#">Link</a>
2025-03-06	[Ministry of Foreign Affairs of Ukraine]	qilin	<a href="#">Link</a>
2025-03-06	[Oberlin Cable Co-op (oberlin.net)]	fog	<a href="#">Link</a>
2025-03-06	[Elite Advanced Laser Corporation]	akira	<a href="#">Link</a>
2025-03-05	[1X Internet]	fog	<a href="#">Link</a>
2025-03-05	[Bizcode]	fog	<a href="#">Link</a>
2025-03-05	[Manning Publications Co.]	fog	<a href="#">Link</a>
2025-03-05	[Engikam]	fog	<a href="#">Link</a>
2025-03-05	[FHNW]	fog	<a href="#">Link</a>
2025-03-05	[Aeonsparx]	fog	<a href="#">Link</a>
2025-03-05	[Flightsim studio]	fog	<a href="#">Link</a>
2025-03-05	[Neopoly]	fog	<a href="#">Link</a>
2025-03-05	[Kr3m]	fog	<a href="#">Link</a>
2025-03-05	[InfoReach]	fog	<a href="#">Link</a>
2025-03-05	[Euranova]	fog	<a href="#">Link</a>
2025-03-05	[Inelmatic]	fog	<a href="#">Link</a>
2025-03-05	[Kotliva]	fog	<a href="#">Link</a>
2025-03-05	[Blue Planet]	fog	<a href="#">Link</a>
2025-03-05	[Eumetsat]	fog	<a href="#">Link</a>
2025-03-05	[Melexis]	fog	<a href="#">Link</a>
2025-03-06	[City government office in Van (Turkey) - van.bel.tr]	skira	<a href="#">Link</a>
2025-03-06	[Law Diary (USA)]	skira	<a href="#">Link</a>
2025-03-06	[Carruth Compliance Consulting]	skira	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-06	[CCL Products India]	skira	<a href="#">Link</a>
2025-03-06	[Krisala Developer (India)]	skira	<a href="#">Link</a>
2025-03-05	[The 19 biggest gitlabs]	fog	<a href="#">Link</a>
2025-03-05	[willms-fleisch.de]	safepay	<a href="#">Link</a>
2025-03-05	[Pervedant]	lynx	<a href="#">Link</a>
2025-03-05	[SCOLARO FETTER GRIZANTI & McGOUGH, P.C. (scolaro.com)]	fog	<a href="#">Link</a>
2025-03-05	[www.black-star.fr]	ransomhub	<a href="#">Link</a>
2025-03-05	[Adrenalina]	akira	<a href="#">Link</a>
2025-03-05	[Cyncly Company]	akira	<a href="#">Link</a>
2025-03-05	[City Plumbing & Electric Supply Co]	akira	<a href="#">Link</a>
2025-03-03	[www.japanrebuilt.jp]	ransomhub	<a href="#">Link</a>
2025-03-04	[www.sunsweet.com]	ransomhub	<a href="#">Link</a>
2025-03-05	[Best Collateral, Inc.]	rhysida	<a href="#">Link</a>
2025-03-04	[Chicago Doorways, LLC]	qilin	<a href="#">Link</a>
2025-03-05	[Schmiedetechnik Plettenberg GmbH & Co KG]	lynx	<a href="#">Link</a>
2025-03-04	[365labs - Security Corp]	monti	<a href="#">Link</a>
2025-03-04	[PFS Grupo - Plan de igualdad, Sostenibilidad]	qilin	<a href="#">Link</a>
2025-03-04	[Pampili (pampili.com.br)]	fog	<a href="#">Link</a>
2025-03-04	[Keystone Pacific Property Management LLC]	bianlian	<a href="#">Link</a>
2025-03-04	[Mosley Glick O'Brien, Inc.]	bianlian	<a href="#">Link</a>
2025-03-04	[FANTIN group]	akira	<a href="#">Link</a>
2025-03-04	[Grupo Baston Aerosol (baston.com.br)]	fog	<a href="#">Link</a>
2025-03-04	[Ray Fogg Corporate Properties]	akira	<a href="#">Link</a>
2025-03-04	[goencon.com]	ransomhub	<a href="#">Link</a>
2025-03-04	[Seabank Group]	lynx	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-04	[Tata Technologies]	hunters	<a href="#">Link</a>
2025-03-04	[Wendy Wu Tours]	killsec	<a href="#">Link</a>
2025-03-04	[rockhillwc.com]	qilin	<a href="#">Link</a>
2025-03-04	[bpmmicro.com]	qilin	<a href="#">Link</a>
2025-03-04	[peruzzi.com]	qilin	<a href="#">Link</a>
2025-03-04	[IOVATE.COM]	clop	<a href="#">Link</a>
2025-03-04	[Legal Aid Society of Salt Lake]	bianlian	<a href="#">Link</a>
2025-03-04	[Ewald Consulting]	bianlian	<a href="#">Link</a>
2025-03-04	[Netcom-World]	apos	<a href="#">Link</a>
2025-03-04	[InternetWay]	apos	<a href="#">Link</a>
2025-03-04	[cimenyan.desa.id]	funksec	<a href="#">Link</a>
2025-03-03	[familychc.com]	ransomhub	<a href="#">Link</a>
2025-03-03	[andreyengineering.com]	ransomhub	<a href="#">Link</a>
2025-03-03	[drvitenas.com]	kairos	<a href="#">Link</a>
2025-03-03	[usarice.com]	kairos	<a href="#">Link</a>
2025-03-03	[Sunnking SustainableSolutions]	akira	<a href="#">Link</a>
2025-03-03	[LINKGROUP]	arcusmedia	<a href="#">Link</a>
2025-03-03	[Openreso]	arcusmedia	<a href="#">Link</a>
2025-03-03	[Itapeseg]	arcusmedia	<a href="#">Link</a>
2025-03-03	[logic insectes]	arcusmedia	<a href="#">Link</a>
2025-03-03	[RJ IT Solutions]	arcusmedia	<a href="#">Link</a>
2025-03-03	[Grafitec]	arcusmedia	<a href="#">Link</a>
2025-03-03	[synaptic.co.tz]	arcusmedia	<a href="#">Link</a>
2025-03-03	[quigleyeye.com]	cactus	<a href="#">Link</a>
2025-03-03	[La Unión]	lynx	<a href="#">Link</a>
2025-03-03	[Central McGowan (centralmcgowan.com)]	fog	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-03	[Klesk Metal Stamping Co (kleskmetalstamping.com)]	fog	<a href="#">Link</a>
2025-03-03	[Forstenlechner Installationstechnik]	akira	<a href="#">Link</a>
2025-03-03	[ceratec.com]	abyss	<a href="#">Link</a>
2025-03-02	[Pre Con Industries]	play	<a href="#">Link</a>
2025-03-02	[IT-IQ Botswana]	play	<a href="#">Link</a>
2025-03-02	[North American Fire Hose]	play	<a href="#">Link</a>
2025-03-02	[Couri Insurance Agency]	play	<a href="#">Link</a>
2025-03-02	[Optometrics]	play	<a href="#">Link</a>
2025-03-02	[International Process Plants]	play	<a href="#">Link</a>
2025-03-02	[Ganong Bros]	play	<a href="#">Link</a>
2025-03-02	[FM.GOB.AR]	monti	<a href="#">Link</a>
2025-03-02	[gruppocogesi.org]	lockbit3	<a href="#">Link</a>
2025-03-02	[Bell Ambulance]	medusa	<a href="#">Link</a>
2025-03-02	[Workforce Group]	killsec	<a href="#">Link</a>
2025-03-01	[germancentre.sg]	incransom	<a href="#">Link</a>
2025-03-01	[JEFFREYCOURT.COM]	clop	<a href="#">Link</a>
2025-03-01	[APTEAN.COM]	clop	<a href="#">Link</a>
2025-03-01	[Wayne County, Michigan]	interlock	<a href="#">Link</a>
2025-03-01	[The Smeg Group]	interlock	<a href="#">Link</a>
2025-03-01	[Newton & Associates, Inc]	rhysida	<a href="#">Link</a>

## 7 Quellen

### 7.1 Quellenverzeichnis

- 1) Cyberwatch - <https://github.com/Casualtek/Cyberwatch>
- 2) Ransomware.live - <https://data.ransomware.live>

- 3) Heise Security Alerts! - <https://www.heise.de/security/alerts/>
- 4) First EPSS - <https://www.first.org/epss/>
- 5) BSI WID - <https://wid.cert-bund.de/>
- 6) Tenable Plugins - <https://www.tenable.com/plugins/>
- 7) Exploit - [packetstormsecurity.com](https://packetstormsecurity.com)
- 8) 0-Day - <https://www.zerodayinitiative.com/rss/published/>
- 9) Die Hacks der Woche - <https://martinhaunschmid.com/videos>

## 8 Impressum



***Herausgeber:***

Marlon Hübner  
Brückenstraße 3  
57629 Höchstenbach

***E-Mail***

[info@cyberwald.com](mailto:info@cyberwald.com)

Cyberwald ist ein privates, nicht-kommerzielles Projekt zur Förderung des Bewusstseins für Cybersicherheit.