


---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250304



## 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>13</b>
7.1 Quellenverzeichnis . . . . .	13
<b>8 Impressum</b>	<b>14</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	0.997960000	<a href="#">Link</a>
CVE-2024-9474	0.974700000	0.999830000	<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	0.997950000	<a href="#">Link</a>
CVE-2024-6670	0.904230000	0.991200000	<a href="#">Link</a>
CVE-2024-5910	0.967810000	0.997990000	<a href="#">Link</a>
CVE-2024-55956	0.968970000	0.998300000	<a href="#">Link</a>
CVE-2024-53704	0.960740000	0.996510000	<a href="#">Link</a>
CVE-2024-5217	0.948330000	0.994800000	<a href="#">Link</a>
CVE-2024-50623	0.969520000	0.998450000	<a href="#">Link</a>
CVE-2024-50603	0.924330000	0.992530000	<a href="#">Link</a>
CVE-2024-4879	0.952210000	0.995240000	<a href="#">Link</a>
CVE-2024-4577	0.951770000	0.995200000	<a href="#">Link</a>
CVE-2024-4358	0.921450000	0.992340000	<a href="#">Link</a>
CVE-2024-41713	0.957210000	0.995930000	<a href="#">Link</a>
CVE-2024-40711	0.964240000	0.997230000	<a href="#">Link</a>
CVE-2024-4040	0.967700000	0.997970000	<a href="#">Link</a>
CVE-2024-38856	0.941790000	0.994040000	<a href="#">Link</a>
CVE-2024-36401	0.961880000	0.996720000	<a href="#">Link</a>
CVE-2024-3400	0.958850000	0.996180000	<a href="#">Link</a>
CVE-2024-3273	0.935040000	0.993390000	<a href="#">Link</a>
CVE-2024-32113	0.938440000	0.993720000	<a href="#">Link</a>
CVE-2024-28995	0.969950000	0.998560000	<a href="#">Link</a>
CVE-2024-28987	0.965400000	0.997480000	<a href="#">Link</a>
CVE-2024-27348	0.960910000	0.996530000	<a href="#">Link</a>
CVE-2024-27198	0.970470000	0.998730000	<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	0.964810000	0.997360000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-21893	0.956970000	0.995870000	<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	0.995890000	<a href="#">Link</a>
CVE-2024-1212	0.946600000	0.994570000	<a href="#">Link</a>
CVE-2024-0986	0.954890000	0.995600000	<a href="#">Link</a>
CVE-2024-0195	0.962680000	0.996890000	<a href="#">Link</a>
CVE-2024-0012	0.970250000	0.998630000	<a href="#">Link</a>

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

Mon, 03 Mar 2025

#### **[UPDATE] [hoch] GNU Emacs: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in GNU Emacs ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Mon, 03 Mar 2025

#### **[UPDATE] [hoch] Rancher: Mehrere Schwachstellen**

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Rancher ausnutzen, um Dateien zu manipulieren, administrative Rechte zu erlangen und einen Denial-of-Service-Zustand auszulösen.

- [Link](#)

—

Mon, 03 Mar 2025

#### **[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, seine Privilegien zu erweitern, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- [Link](#)

—

Mon, 03 Mar 2025

**[UPDATE] [hoch] EDK2 NetworkPkg IP stack implementation: Mehrere Schwachstellen**

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der EDK2 NetworkPkg IP stack implementation ausnutzen, um beliebigen Programmcode auszuführen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand auszulösen.

- [Link](#)

—

Mon, 03 Mar 2025

**[UPDATE] [hoch] Microsoft Azure: Mehrere Schwachstellen ermöglichen Privilegieneskalation**

Ein Angreifer kann mehrere Schwachstellen in Microsoft Azure ausnutzen, um seine Privilegien zu erhöhen und um einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Mon, 03 Mar 2025

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um einen Spoofing-Angriff durchzuführen, beliebigen Code auszuführen, Dateien zu manipulieren, vertrauliche Informationen offenzulegen oder Cross-Site-Scripting-Angriffe durchzuführen.

- [Link](#)

—

Mon, 03 Mar 2025

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen, Daten zu manipulieren, einen Denial-of-Service-Zustand zu erzeugen und vertrauliche Informationen preiszugeben.

- [Link](#)

—

Mon, 03 Mar 2025

**[UPDATE] [hoch] Microsoft Azure CLI: Mehrere Schwachstellen ermöglichen Privilegieneskalation und Codeausführung**

Ein Angreifer kann mehrere Schwachstellen in Microsoft Azure CLI, Microsoft Azure, Microsoft Azure Service Fabric und Microsoft Azure Stack ausnutzen, um seine Privilegien zu erhöhen und beliebigen Code auszuführen.

- [Link](#)

—

Mon, 03 Mar 2025

**[UPDATE] [hoch] Oracle Fusion Middleware: Mehrere Schwachstellen**

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Oracle Fusion Middleware ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

---

Mon, 03 Mar 2025

**[UPDATE] [hoch] IBM App Connect Enterprise: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in IBM App Connect Enterprise ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

---

Mon, 03 Mar 2025

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen preiszugeben oder einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

---

Mon, 03 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](#)

---

Mon, 03 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](#)

---

Mon, 03 Mar 2025

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Firefox ESR und Thunderbird ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, vertrauliche Informationen preiszugeben, Sicherheitsmaßnahmen zu umgehen oder Spoofing-Angriffe durchzuführen.



- [Link](#)

—

Mon, 03 Mar 2025

**[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen**

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

- [Link](#)

—

Mon, 03 Mar 2025

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

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

- [Link](#)

—

Mon, 03 Mar 2025

**[UPDATE] [hoch] Google Chrome/Microsoft Edge: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome/Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen und um einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Mon, 03 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 Zustand oder andere, nicht näher beschriebene Auswirkungen zu verursachen.

- [Link](#)

—

Mon, 03 Mar 2025

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen preiszugeben, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu erzeugen oder Spoofing-Angriffe durchzuführen.

- [Link](#)

—

Mon, 03 Mar 2025

**[UPDATE] [hoch] Red Hat Enterprise Linux (Fast Datapath): Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

---

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-0061]	critical
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-0457]	critical
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-2653]	critical
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-2763]	critical
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-1717]	critical
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-1718]	critical
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-2122]	critical
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-1573]	critical
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-1033]	critical
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-1719]	critical
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-0870]	critical
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-0029]	critical
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-0114]	critical
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-2123]	critical
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-1531]	critical
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-1541]	critical
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-0880]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-0881]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-0207]	high

Datum	Schwachstelle	Bewertung
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-2146]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-0461]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-0042]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-2142]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-2098]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-0067]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-2150]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-2124]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-0867]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-2049]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-2328]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-2375]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-1177]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-0877]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-0698]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-1097]	high
3/4/2025	[Linux Distros Unpatched Vulnerability : CVE-2012-1150]	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
2025-03-02	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>

## 6 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[andreyevengineering.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	[New .Gov ?]	arcusmedia	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
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	[breakawayconcretecutting.com]	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.