



Ausgabe: 20230816

# 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

# Security-News

## Heise - Security-Alert

### *Schadcode-Attacken via WLAN auf einige Automodelle von Ford möglich*

Eine Schwachstelle im Infotainmentsystem gefährdet bestimmte Modellserien von Ford und Lincoln. Die Fahrsicherheit soll davon aber nicht beeinträchtigt sein.

- [Link](#)

---

### *Schwerwiegende Sicherheitslücken bedrohen hierzulande kritische Infrastrukturen*

Aufgrund von mehreren Schwachstellen in einem SDK, das im Industriebereich zum Einsatz kommt, sind Attacken auf kritische Infrastrukturen möglich.

- [Link](#)

---

### *Statischer Schlüssel in Dell Compellent leakt Zugangsdaten für VMware vCenter*

Aufgrund einer Schwachstelle in Dells Compellent Integration Tools for VMware (CITV) können Angreifer Log-in-Daten entschlüsseln.

- [Link](#)

---

### *Sicherheitsupdates für Nextcloud: Angreifer können Daten löschen*

Die Cloud-Computing-Software Nextcloud ist verwundbar. Sicherheitsupdates sind verfügbar.

- [Link](#)

---

### *Videomeeting-Anwendungen: Zoom rüstet Produkte gegen mögliche Attacken*

Wichtige Sicherheitsupdates, für unter anderem den Windows-Client von Zoom, schließen mehrere Lücken.

- [Link](#)

---

### *Patchday: Kritische Schadcode-Lücken bedrohen Android 11, 12 und 13*

Google und weitere Hersteller von Android-Geräten haben ihren monatlichen Sammel-Sicherheitsupdates veröffentlicht.

- [Link](#)

---

### *Patchday: Angreifer können Zugangsbeschränkungen von SAP PowerDesigner umgehen*

Attacken vorbeugen: Firmen-Admins sollten ihre SAP-Anwendungen auf den aktuellen Stand bringen.

- [Link](#)

---

### *Patchday: Anwendungen von Adobe können Schadcode auf PCs lassen*

Es sind wichtige Sicherheitsupdates für Adobe Commerce, Dimension, Reader und XMP Toolkit SDK erschienen.

- [Link](#)

---

### *Patchday: Angreifer umgehen Schutzmechanismus von Windows*

Microsoft schließt unter anderem in Message Queuing, Outlook und Teams gefährliche Schadcode-Lücken.

- [Link](#)

---

### *Druck-Management-Lösung: Sicherheitslücken gefährden Papercut-Server*

Im schlimmsten Fall können Angreifer Schadcode auf Papercut-Servern ausführen. Nicht alle Systeme sind standardmäßig gefährdet.

- [Link](#)

---

# 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.

## 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.

### CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3519	0.911990000	0.984640000	<a href="#">Link</a>
CVE-2023-35078	0.965240000	0.994080000	<a href="#">Link</a>
CVE-2023-34362	0.940540000	0.988060000	<a href="#">Link</a>
CVE-2023-33246	0.963860000	0.993530000	<a href="#">Link</a>
CVE-2023-28771	0.918810000	0.985250000	<a href="#">Link</a>
CVE-2023-28121	0.937820000	0.987610000	<a href="#">Link</a>
CVE-2023-27372	0.971220000	0.996770000	<a href="#">Link</a>
CVE-2023-27350	0.971160000	0.996750000	<a href="#">Link</a>
CVE-2023-25717	0.966450000	0.994610000	<a href="#">Link</a>
CVE-2023-25194	0.918160000	0.985190000	<a href="#">Link</a>
CVE-2023-21839	0.961530000	0.992810000	<a href="#">Link</a>
CVE-2023-21554	0.902620000	0.983820000	<a href="#">Link</a>
CVE-2023-20887	0.960660000	0.992560000	<a href="#">Link</a>
CVE-2023-0669	0.967490000	0.995060000	<a href="#">Link</a>

## BSI - Warn- und Informationsdienst (WID)

Tue, 15 Aug 2023

### [UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, einen Denial of Service Zustand herbeizuführen, Dateien zu manipulieren, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen oder sonstige Auswirkungen zu verursachen.

- [Link](#)

Tue, 15 Aug 2023

### [UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, beliebigen Programmcode auszuführen, Informationen offenzulegen, seine Privilegien zu erweitern, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen, Sicherheitsvorkehrungen zu umgehen oder sonstige Auswirkungen zu verursachen.

- [Link](#)

Tue, 15 Aug 2023

**[UPDATE] [kritisch] Citrix Systems ShareFile StorageZones Controller: Schwachstelle ermöglicht Übernahme der Kontrolle**

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in Citrix Systems ShareFile StorageZones Controller ausnutzen, um den Controller zu kompromittieren.

- [Link](#)

---

Tue, 15 Aug 2023

**[UPDATE] [hoch] Node.js: Mehrere Schwachstellen**

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um seine Privilegien zu erweitern, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

---

Tue, 15 Aug 2023

**[UPDATE] [kritisch] vm2: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in vm2 ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Tue, 15 Aug 2023

**[UPDATE] [hoch] IBM Java: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in IBM Java ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Tue, 15 Aug 2023

**[UPDATE] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen**

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Microsoft .NET Framework, Microsoft ASP.NET, Microsoft Azure DevOps Server und Microsoft Visual Studio ausnutzen, um beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen oder Informationen offenzulegen.

- [Link](#)

---

Tue, 15 Aug 2023

**[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in AMD Prozessoren ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.

- [Link](#)

---

Tue, 15 Aug 2023

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

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in poppler ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

---

Mon, 14 Aug 2023

**[NEU] [hoch] Red Hat OpenShift Service Mesh und Service Mesh Containers: Mehrere Schwachstellen**

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Red Hat OpenShift Service Mesh und Service Mesh Containers, sowie Red Hat Enterprise Linux ausnutzen, um einen Denial of Service Zustand herbeizuführen, Dateien zu manipulieren, Sicherheitsvorkehrungen zu umgehen oder Informationen offenzulegen.

- [Link](#)

---

Mon, 14 Aug 2023

**[NEU] [UNGEPATCHT] [hoch] ESET Server Security: Schwachstelle ermöglicht Privilegien-  
eskalation**

Ein lokaler Angreifer kann eine Schwachstelle in ESET Server Security, ESET NOD32 Antivirus und ESET Endpoint Security ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

---

Mon, 14 Aug 2023

***[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen***

Ein entfernter, anonym, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen im Apache HTTP Server ausnutzen, um seine Rechte zu erweitern, Sicherheitsrestriktionen zu umgehen oder um einen Denial of Service Angriff durchzuführen.

- [Link](#)

---

Mon, 14 Aug 2023

***[UPDATE] [hoch] Net-SNMP: Mehrere Schwachstellen ermöglichen Privilegieneskalation***

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Net-SNMP ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

---

Mon, 14 Aug 2023

***[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen***

Ein entfernter Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um Sicherheitsvorkehrungen zu umgehen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand herzustellen.

- [Link](#)

---

Mon, 14 Aug 2023

***[UPDATE] [kritisch] GNU libc: Mehrere Schwachstellen ermöglichen Codeausführung und Denial of Service***

Ein Angreifer kann mehrere Schwachstellen in GNU libc ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service zu verursachen.

- [Link](#)

---

Mon, 14 Aug 2023

***[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht nicht spezifizierten Angriff***

Ein Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

---

Mon, 14 Aug 2023

***[UPDATE] [hoch] expat: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen***

Ein Angreifer kann mehrere Schwachstellen in expat ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

---

Mon, 14 Aug 2023

***[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Erlangen von Administratorrechten***

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um Administratorrechte zu erlangen.

- [Link](#)

---

Mon, 14 Aug 2023

***[UPDATE] [hoch] Rsync: Schwachstelle ermöglicht Manipulation von Dateien***

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Rsync ausnutzen, um Dateien zu manipulieren.

- [Link](#)

---

Mon, 14 Aug 2023

***[UPDATE] [hoch] Linux Kernel (ksmbd): Mehrere Schwachstellen***

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service-Zustand herbeizuführen, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen, Privilegien zu erweitern und beliebigen Code auszuführen.

- [Link](#)

---

Datum	Schwachstelle	Bewertung
8/15/2023	[Google Chrome < 116.0.5845.96 Multiple Vulnerabilities]	critical
8/15/2023	[Google Chrome < 116.0.5845.96 Multiple Vulnerabilities]	critical
8/15/2023	[Oracle Linux 7 : openssh (ELSA-2023-12711)]	critical
8/15/2023	[Oracle Linux 6 : openssh (ELSA-2023-4428)]	critical
8/15/2023	[Oracle Linux 8 : thunderbird (ELSA-2023-4497)]	critical
8/15/2023	[Oracle Linux 7 : thunderbird (ELSA-2023-4495)]	critical
8/15/2023	[Oracle Linux 9 : thunderbird (ELSA-2023-4499)]	critical
8/15/2023	[FreeBSD : krb5 – Double-free in KDC TGS processing (a6986f0f-3ac0-11ee-9a88-206a8a720317)]	critical
8/15/2023	[RHEL 7 / 8 : Red Hat JBoss Core Services Apache HTTP Server 2.4.57 (RHSA-2023:4629)]	critical
8/15/2023	[AlmaLinux 9 : rust (ALSA-2023:4634)]	high
8/15/2023	[AlmaLinux 9 : .NET 6.0 (ALSA-2023:4644)]	high
8/15/2023	[AlmaLinux 9 : .NET 7.0 (ALSA-2023:4642)]	high
8/15/2023	[Security Updates for Microsoft Dynamics 365 Business Central (August 2023)]	high
8/15/2023	[Oracle Linux 8 : libcap (ELSA-2023-4524)]	high
8/15/2023	[Oracle Linux 7 : kernel (ELSA-2023-4151)]	high
8/15/2023	[Oracle Linux 8 : python-flask (ELSA-2023-12710)]	high
8/15/2023	[Oracle Linux 8 : kernel (ELSA-2023-4517)]	high
8/15/2023	[Oracle Linux 8 : postgresql:13 (ELSA-2023-4527)]	high
8/15/2023	[Oracle Linux 8 : nodejs:16 (ELSA-2023-4537)]	high
8/15/2023	[Oracle Linux 8 : nodejs:18 (ELSA-2023-4536)]	high
8/15/2023	[Oracle Linux 8 : postgresql:12 (ELSA-2023-4535)]	high
8/15/2023	[Oracle Linux 6 : kernel (ELSA-2023-1822)]	high
8/15/2023	[Oracle Linux 8 : postgresql:10 (ELSA-2023-4539)]	high
8/15/2023	[FreeBSD : postgresql-server -- Extension script @substitutions@ within quoting allow SQL injection (cfd2a634-3785-11ee-94b4-6cc21735f730)]	high
8/15/2023	[Juniper Junos OS Vulnerability (JSA71639)]	high
8/15/2023	[RHEL 7 : python (RHSA-2023:3555)]	high
8/15/2023	[Security Updates for Microsoft Office Products (Aug 2023) (macOS)]	high
8/15/2023	[Oracle Linux 8 : .NET / 6.0 (ELSA-2023-4645)]	high
8/15/2023	[Oracle Linux 8 : .NET / 7.0 (ELSA-2023-4643)]	high
8/15/2023	[Ubuntu 22.04 LTS / 23.04 : WebKitGTK vulnerabilities (USN-6289-1)]	high

## Die Hacks der Woche

mit Martin Haunschmid

**Wasser predigen und Wein trinken? Ivanti, als Security Hersteller DARF so etwas nicht passieren!**



[Zum Youtube Video](#)



## Cyberangriffe: (Aug)

Datum	Opfer	Land	Information
-------	-------	------	-------------

## Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-08-09	[FTRIA CO. LTD]	noescape	<a href="#">Link</a>
2023-08-15	[www.cognizant.com]	clon	<a href="#">Link</a>
2023-08-15	[Recaro]	alphv	<a href="#">Link</a>
2023-08-15	[Postel SpA]	medusa	<a href="#">Link</a>
2023-08-15	[ABA Research - Business Information 2]	alphv	<a href="#">Link</a>
2023-08-15	[Keystone Insurance Services]	8base	<a href="#">Link</a>
2023-08-15	[ANS]	8base	<a href="#">Link</a>
2023-08-15	[Aspect Structural Engineers]	8base	<a href="#">Link</a>
2023-08-08	[Fondation De Verdeil]	noescape	<a href="#">Link</a>
2023-08-14	[Freeport-McMoran - NYSE: FCX]	alphv	<a href="#">Link</a>
2023-08-14	[jhillburn.com]	lockbit3	<a href="#">Link</a>
2023-08-14	[qbcqatar.com.qa]	lockbit3	<a href="#">Link</a>
2023-08-07	[John L Lowery & Associates]	noescape	<a href="#">Link</a>
2023-08-07	[Federal Bar Association]	noescape	<a href="#">Link</a>
2023-08-14	[leecorpinc.com]	lockbit3	<a href="#">Link</a>
2023-08-14	[econsult.com]	lockbit3	<a href="#">Link</a>
2023-08-14	[Saint Xavier University]	alphv	<a href="#">Link</a>
2023-08-14	[Agriloja.pt]	everest	<a href="#">Link</a>
2023-08-14	[CB Energy Australlia]	medusa	<a href="#">Link</a>
2023-08-14	[Borets (Levare.com) ]	medusa	<a href="#">Link</a>
2023-08-13	[majan.com]	lockbit3	<a href="#">Link</a>
2023-08-13	[luterkort.se]	lockbit3	<a href="#">Link</a>
2023-08-13	[difccourts.ae]	lockbit3	<a href="#">Link</a>
2023-08-13	[zaun.co.uk]	lockbit3	<a href="#">Link</a>
2023-08-13	[roxcel.com.tr]	lockbit3	<a href="#">Link</a>
2023-08-13	[meaf.com]	lockbit3	<a href="#">Link</a>
2023-08-13	[stmarysschool.co.za]	lockbit3	<a href="#">Link</a>
2023-08-13	[rappenglitz.de]	lockbit3	<a href="#">Link</a>
2023-08-13	[siampremier.co.th]	lockbit3	<a href="#">Link</a>
2023-08-12	[National Institute of Social Services for Retirees and Pensioners]	rhysida	<a href="#">Link</a>
2023-08-12	[Armortex]	bianlian	<a href="#">Link</a>
2023-08-12	[arganoInterRel]	alphv	<a href="#">Link</a>
2023-08-11	[Rite Technology]	akira	<a href="#">Link</a>
2023-08-11	[zain.com]	lockbit3	<a href="#">Link</a>
2023-08-10	[Top Light]	play	<a href="#">Link</a>
2023-08-10	[Algorry Zappia & Associates]	play	<a href="#">Link</a>
2023-08-10	[EAI]	play	<a href="#">Link</a>
2023-08-10	[The Belt Railway Company of Chicago]	akira	<a href="#">Link</a>
2023-08-10	[Optimum Technology]	akira	<a href="#">Link</a>
2023-08-10	[Boson]	akira	<a href="#">Link</a>
2023-08-10	[Stockdale Podiatry]	8base	<a href="#">Link</a>
2023-08-09	[oneatlas.com]	lockbit3	<a href="#">Link</a>
2023-08-05	[Lower Yukon School District]	noescape	<a href="#">Link</a>
2023-08-06	[Thermenhotel Stoiser]	incransom	<a href="#">Link</a>
2023-08-09	[el-cerrito.org]	lockbit3	<a href="#">Link</a>
2023-08-09	[fashions-uk.com]	lockbit3	<a href="#">Link</a>
2023-08-09	[cbcstjohns.co.za]	lockbit3	<a href="#">Link</a>
2023-08-09	[octoso.de]	lockbit3	<a href="#">Link</a>
2023-08-09	[ricks-motorcycles.com]	lockbit3	<a href="#">Link</a>
2023-08-09	[janus-engineering.com]	lockbit3	<a href="#">Link</a>
2023-08-09	[csem.qc.ca]	lockbit3	<a href="#">Link</a>
2023-08-09	[asfcustomers.com]	lockbit3	<a href="#">Link</a>
2023-08-09	[sekuro.com.tr]	lockbit3	<a href="#">Link</a>
2023-08-09	[TIMECO]	akira	<a href="#">Link</a>
2023-08-09	[chula.ac.th]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-08-09	[etisaleg.com]	lockbit3	Link
2023-08-09	[2plan.com]	lockbit3	Link
2023-08-08	[Sabalan Azmayesh]	arvinclub	Link
2023-08-09	[Optimum Health Solutions]	rhysida	Link
2023-08-09	[unitycouncil.org]	lockbit3	Link
2023-08-09	[independenceia.org]	lockbit3	Link
2023-08-09	[www.finitia.net]	abyss	Link
2023-08-09	[Ramtha]	rhysida	Link
2023-08-08	[Batesville didn't react on appeal and allows Full Leak]	ragnarlocker	Link
2023-08-08	[ZESA Holdings]	everest	Link
2023-08-08	[Magic Micro Computers]	alphv	Link
2023-08-08	[Emerson School District]	medusa	Link
2023-08-08	[CH informatica]	8base	Link
2023-08-07	[Thonburi Energy Storage Systems (TESM)]	qilin	Link
2023-08-07	[Räddningstjänsten Västra Blekinge]	akira	Link
2023-08-07	[Papel Prensa SA]	akira	Link
2023-08-01	[Kreacta]	noescape	Link
2023-08-07	[Parsian Bitumen]	arvinclub	Link
2023-08-07	[varian.com]	lockbit3	Link
2023-08-06	[Delaney Browne Recruitment]	8base	Link
2023-08-06	[IBL]	alphv	Link
2023-08-05	[Draje food industrial group]	arvinclub	Link
2023-08-06	[Oregon Sports Medicine]	8base	Link
2023-08-06	[premierbpo.com]	alphv	Link
2023-08-06	[SatCom Marketing]	8base	Link
2023-08-05	[Rayden Solicitors]	alphv	Link
2023-08-05	[haynesintl.com]	lockbit3	Link
2023-08-05	[Kovair Software Data Leak]	everest	Link
2023-08-05	[Henlaw]	alphv	Link
2023-08-04	[mipe.com]	lockbit3	Link
2023-08-04	[armortex.com]	lockbit3	Link
2023-08-04	[iqcontrols.com]	lockbit3	Link
2023-08-04	[scottevest.com]	lockbit3	Link
2023-08-04	[atser.com]	lockbit3	Link
2023-08-04	[Galicia en Goles]	alphv	Link
2023-08-04	[tetco.com]	lockbit3	Link
2023-08-04	[SBS Construction]	alphv	Link
2023-08-04	[Koury Engineering]	akira	Link
2023-08-04	[Pharmatech Repblica Dominicana was hacked. All sensitive company and customer information ]	alphv	Link
2023-08-04	[Grupo Garza Ponce was hacked! Due to a massive company vulnerability, more than 2 TB of se]	alphv	Link
2023-08-04	[seaside-kish co]	arvinclub	Link
2023-08-04	[Studio Domaine LLC]	nokoyawa	Link
2023-08-04	[THECHANGE]	alphv	Link
2023-08-04	[Ofimedic]	alphv	Link
2023-08-04	[Abatti Companies - Press Release]	monti	Link
2023-08-03	[Spokane Spinal Sports Care Clinic]	bianlian	Link
2023-08-03	[pointpleasant.k12.nj.us]	lockbit3	Link
2023-08-03	[Roman Catholic Diocese of Albany]	nokoyawa	Link
2023-08-03	[Venture General Agency]	akira	Link
2023-08-03	[Datawatch Systems]	akira	Link
2023-08-03	[admsc.com]	lockbit3	Link
2023-08-03	[United Tractors]	rhysida	Link
2023-08-03	[RevZero, Inc]	8base	Link
2023-08-03	[Rossman Realty Group, inc.]	8base	Link
2023-08-03	[riggsabney]	alphv	Link
2023-08-02	[fec-corp.com]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-08-02	[bestmotel.de]	lockbit3	<a href="#">Link</a>
2023-08-02	[Tempur Sealy International]	alphv	<a href="#">Link</a>
2023-08-02	[constructioncrd.com]	lockbit3	<a href="#">Link</a>
2023-08-02	[Helen F. Dalton Lawyers]	alphv	<a href="#">Link</a>
2023-08-02	[TGRWA ]	akira	<a href="#">Link</a>
2023-08-02	[Guido]	akira	<a href="#">Link</a>
2023-08-02	[Bickel & Brewer - Press Release]	monti	<a href="#">Link</a>
2023-08-02	[SHERMAN.EDU]	cl0p	<a href="#">Link</a>
2023-08-02	[COSI]	karakurt	<a href="#">Link</a>
2023-08-02	[unicorpusa.com]	lockbit3	<a href="#">Link</a>
2023-08-01	[Garage Living, The Dispenser USA]	play	<a href="#">Link</a>
2023-08-01	[Aapd]	play	<a href="#">Link</a>
2023-08-01	[Birch, Horton, Bittner & Cherot]	play	<a href="#">Link</a>
2023-08-01	[DAL-TECH Engineering]	play	<a href="#">Link</a>
2023-08-01	[Coral Resort]	play	<a href="#">Link</a>
2023-08-01	[Professionnel France]	play	<a href="#">Link</a>
2023-08-01	[ACTIVA Group]	play	<a href="#">Link</a>
2023-08-01	[Aquatlantis]	play	<a href="#">Link</a>
2023-08-01	[Kogetsu]	mallox	<a href="#">Link</a>
2023-08-01	[Parathon by JDA eHealth Systems]	akira	<a href="#">Link</a>
2023-08-01	[KIMCO Staffing Service]	alphv	<a href="#">Link</a>
2023-08-01	[Pea River Electric Cooperative]	nokoyawa	<a href="#">Link</a>
2023-08-01	[MBS Equipment TTI]	8base	<a href="#">Link</a>
2023-08-01	[gerb.bg]	lockbit3	<a href="#">Link</a>
2023-08-01	[persingerlaw.com]	lockbit3	<a href="#">Link</a>
2023-08-01	[Jacklett Construction LLC]	8base	<a href="#">Link</a>

# Quellen

## 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) Die Hacks der Woche - <https://martinhaunschmid.com/videos>

# 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.