



Ausgabe: 20230818

# 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

### *Jetzt patchen! Citrix ShareFile im Visier von Angreifern*

Unbekannte Angreifer nutzen eine kritische Sicherheitslücke in Citrix ShareFile StorageZones Controller aus. Updates sind verfügbar.

- [Link](#)

---

### *Lücken in Kennzeichenerkennungssoftware gefährden Axis-Überwachungskamera*

Mehrere Sicherheitslücken in Software für Überwachungskameras von Axis gefährden Geräte.

- [Link](#)

---

### *Sicherheitslücken: Angreifer können Hintertüren in Datenzentren platzieren*

Schwachstellen in Software von CyberPower und Dataprobe zur Energieüberwachung und -Verteilung gefährden Datenzentren.

- [Link](#)

---

### *Vielfältige Attacken auf Ivanti Enterprise Mobility Management möglich*

Angreifer können Schadcode auf Systeme mit Ivanti EMM schieben und ausführen. Eine dagegen abgesicherte Version schafft Abhilfe.

- [Link](#)

---

### *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](#)

---

## 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-2023-39143	0.921370000	0.985510000	<a href="#">Link</a>
CVE-2023-3519	0.911990000	0.984680000	<a href="#">Link</a>
CVE-2023-35078	0.965240000	0.994090000	<a href="#">Link</a>
CVE-2023-34362	0.936790000	0.987550000	<a href="#">Link</a>
CVE-2023-33246	0.963860000	0.993520000	<a href="#">Link</a>
CVE-2023-28771	0.918810000	0.985270000	<a href="#">Link</a>
CVE-2023-28121	0.937820000	0.987650000	<a href="#">Link</a>
CVE-2023-27372	0.971220000	0.996780000	<a href="#">Link</a>
CVE-2023-27350	0.971160000	0.996770000	<a href="#">Link</a>
CVE-2023-25717	0.966450000	0.994610000	<a href="#">Link</a>
CVE-2023-25194	0.924830000	0.985880000	<a href="#">Link</a>
CVE-2023-21839	0.961530000	0.992810000	<a href="#">Link</a>
CVE-2023-21554	0.902620000	0.983870000	<a href="#">Link</a>
CVE-2023-20887	0.960660000	0.992580000	<a href="#">Link</a>
CVE-2023-0669	0.967490000	0.995060000	<a href="#">Link</a>

---

## BSI - Warn- und Informationsdienst (WID)

Thu, 17 Aug 2023

### *[NEU] [hoch] Moxa Router: Mehrere Schwachstellen*

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Moxa Router ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen oder seine Privilegien zu erweitern.

- [Link](#)

---

Thu, 17 Aug 2023

### *[NEU] [hoch] Jenkins: Mehrere Schwachstellen*

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Jenkins ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

---

Thu, 17 Aug 2023

### *[NEU] [hoch] Cisco Unified Communications Manager (CUCM): Schwachstelle ermöglicht SQL Injection*

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Cisco Unified Communications Manager (CUCM) ausnutzen, um einen SQL Injection Angriff durchzuführen.

- [Link](#)

---

Thu, 17 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](#)

---

Thu, 17 Aug 2023

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

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

- [Link](#)

---

Thu, 17 Aug 2023

**[UPDATE] [hoch] Red Hat Enterprise Linux: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux und Oracle Linux ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Thu, 17 Aug 2023

**[UPDATE] [hoch] Red Hat Enterprise Linux Ceph Storage: Schwachstelle ermöglicht Privilegieneskalation**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux Ceph Storage ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

---

Thu, 17 Aug 2023

**[UPDATE] [hoch] Red Hat Integration Camel for Spring Boot: Mehrere Schwachstellen**

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Red Hat Integration Camel for Spring Boot ausnutzen, um die Vertraulichkeit, Verfügbarkeit und Integrität zu gefährden.

- [Link](#)

---

Thu, 17 Aug 2023

**[UPDATE] [hoch] Red Hat OpenShift Container Platform: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen**

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in der Red Hat OpenShift Container Platform ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

---

Thu, 17 Aug 2023

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

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

- [Link](#)

---

Thu, 17 Aug 2023

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

Ein entfernter anonymen Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um Informationen offenzulegen oder beliebigen Code auszuführen.

- [Link](#)

---

Thu, 17 Aug 2023

**[NEU] [hoch] IBM Security Guardium: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in IBM Security Guardium ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Wed, 16 Aug 2023

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

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

code auszuführen oder Informationen offenzulegen.

- [Link](#)

---

Wed, 16 Aug 2023

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

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

- [Link](#)

---

Wed, 16 Aug 2023

**[UPDATE] [hoch] Apache Portable Runtime (APR): Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in Apache Portable Runtime (APR) ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

---

Wed, 16 Aug 2023

**[UPDATE] [hoch] IBM Security Guardium: Mehrere Schwachstellen**

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in IBM Security Guardium ausnutzen, um Dateien zu manipulieren, beliebigen Programmcode auszuführen oder Informationen offenzulegen.

- [Link](#)

---

Wed, 16 Aug 2023

**[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen ermöglichen HTTP Response Splitting**

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um einen Response Splitting Angriff durchzuführen.

- [Link](#)

---

Wed, 16 Aug 2023

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

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

- [Link](#)

---

Wed, 16 Aug 2023

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

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

- [Link](#)

---

Wed, 16 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](#)

---

---

## Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/17/2023	[SUSE SLES12 Security Update : kernel (SUSE-SU-2023:3324-1)]	critical
8/17/2023	[Debian DLA-3532-1 : openssh - LTS security update]	critical
8/17/2023	[OracleVM 3.4 : openssh (OVMSA-2023-0019)]	critical
8/17/2023	[ShareFile Documents Unauthenticated Access (CTX559517)]	critical
8/17/2023	[Ubuntu 20.04 LTS : HAProxy vulnerability (USN-6294-2)]	critical

Datum	Schwachstelle	Bewertung
8/17/2023	[FreeBSD : chromium – multiple vulnerabilities (5666688f-803b-4cf0-9cb1-08c088f2225a)]	critical
8/16/2023	[Ubuntu 22.04 LTS : HAProxy vulnerability (USN-6294-1)]	critical
8/16/2023	[PHP 8.2.x < 8.2.9 Multiple Vulnerabilities]	critical
8/17/2023	[Fedora 37 : opensc (2023-2afb831742)]	high
8/17/2023	[Fedora 37 : llhttp / python-aiohttp (2023-105880e618)]	high
8/17/2023	[Fedora 38 : opensc (2023-29530cc60b)]	high
8/17/2023	[Fedora 37 : rust (2023-4824704a61)]	high
8/17/2023	[SUSE SLES12 Security Update : kernel (SUSE-SU-2023:3329-1)]	high
8/17/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : pcre2 (SUSE-SU-2023:3327-1)]	high
8/17/2023	[SUSE SLES12 Security Update : pcre2 (SUSE-SU-2023:3328-1)]	high
8/17/2023	[Mattermost Server < 7.8.8 / 7.9.x < 7.9.6 / 7.10.x < 7.10.4 Multiple Vulnerabilities]	high
8/17/2023	[PostgreSQL 11.x < 11.21 / 12.x < 12.16 / 13.x < 13.12 / 14.x < 14.9 / 15.x < 15.4 SQLi]	high
8/17/2023	[Debian DSA-5478-1 : openjdk-11 - security update]	high
8/17/2023	[OracleVM 3.4 : kernel-uek (OVMSA-2023-0017)]	high
8/17/2023	[OracleVM 3.4 : kernel-uek (OVMSA-2023-0018)]	high
8/17/2023	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : PostgreSQL vulnerabilities (USN-6296-1)]	high
8/17/2023	[OracleVM 3.4 : kernel-uek (OVMSA-2023-0016)]	high
8/17/2023	[Oracle Linux 7 : bash (ELSA-2020-1113)]	high
8/17/2023	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6300-1)]	high
8/17/2023	[Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6301-1)]	high
8/17/2023	[FreeBSD : clamav – Possible denial of service vulnerability in the AutoIt file parser (8e561cfe-3c59-11ee-b32e-080027f5fec9)]	high
8/17/2023	[FreeBSD : clamav – Possible denial of service vulnerability in the HFS+ file parser (51a59f36-3c58-11ee-b32e-080027f5fec9)]	high
8/17/2023	[FreeBSD : MySQL – Multiple vulnerabilities (759a5599-3ce8-11ee-a0d1-84a93843eb75)]	high
8/16/2023	[AlmaLinux 8 : rust-toolset:rhel8 (ALSA-2023:4635)]	high
8/16/2023	[AlmaLinux 8 : .NET 6.0 (ALSA-2023:4645)]	high
8/16/2023	[AlmaLinux 8 : .NET 7.0 (ALSA-2023:4643)]	high
8/16/2023	[Atlassian Confluence 7.13.15 < 7.13.19 / 7.19.7 < 7.19.11 / 8.1.1 < 8.4.1 DoS (CONFSERVER-90185)]	high
8/16/2023	[Ubuntu 16.04 ESM : GStreamer vulnerability (USN-6291-1)]	high
8/16/2023	[Ubuntu 23.04 : Ceph vulnerability (USN-6292-1)]	high
8/16/2023	[Ubuntu 22.04 LTS : Podman vulnerability (USN-6295-1)]	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
2023-08-17	Tempur Sealy International Inc.	[USA]	<a href="#">Link</a>
2023-08-15	Cleveland City Schools	[USA]	<a href="#">Link</a>
2023-08-14	Clorox	[USA]	<a href="#">Link</a>
2023-08-13	Swan Retail	[GBR]	<a href="#">Link</a>
2023-08-13	Verlagsgruppe in München	[DEU]	<a href="#">Link</a>
2023-08-11	Neogy	[ITA]	<a href="#">Link</a>
2023-08-11	Freeport-McMoRan Inc.	[USA]	<a href="#">Link</a>
2023-08-09	Multiple Listing Service (MLS)	[USA]	<a href="#">Link</a>
2023-08-08	Fondation de Verdeil	[CHE]	<a href="#">Link</a>
2023-08-06	Le Service de Santé de Madeira (Sesaram)	[PRT]	<a href="#">Link</a>
2023-08-03	Prospect Medical Holdings	[USA]	<a href="#">Link</a>
2023-08-03	Commission des services électriques de Montréal (CSEM)	[CAN]	<a href="#">Link</a>
2023-08-02	BPP	[GBR]	<a href="#">Link</a>
2023-08-01	Universität de Düsseldorf	[DEU]	<a href="#">Link</a>
2023-08-01	Programme de Soins Médicaux Intégrés (PAMI)	[ARG]	<a href="#">Link</a>

## Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-08-11	[au Domain Administration Ltd]	noescape	<a href="#">Link</a>
2023-08-11	[Contact 121 Pty Ltd]	noescape	<a href="#">Link</a>
2023-08-17	[umchealth.com]	lockbit3	<a href="#">Link</a>
2023-08-17	[sgl.co.th]	lockbit3	<a href="#">Link</a>
2023-08-17	[Agriloja.pt demo-leak]	everest	<a href="#">Link</a>
2023-08-17	[RIMSS]	akira	<a href="#">Link</a>
2023-08-17	[SFJAZZ.ORG]	lockbit3	<a href="#">Link</a>
2023-08-17	[mybps.us]	lockbit3	<a href="#">Link</a>
2023-08-17	[kriegerklatt.com]	lockbit3	<a href="#">Link</a>
2023-08-17	[ALLIANCE]	blackbasta	<a href="#">Link</a>
2023-08-17	[DEUTSCHELEASING]	blackbasta	<a href="#">Link</a>
2023-08-17	[VDVEN]	blackbasta	<a href="#">Link</a>
2023-08-17	[SYNQUESTLABS]	blackbasta	<a href="#">Link</a>
2023-08-17	[TWINTOWER]	blackbasta	<a href="#">Link</a>
2023-08-17	[Camino Nuevo CharterAcademy]	akira	<a href="#">Link</a>
2023-08-17	[Smart-swgcr.org]	lockbit3	<a href="#">Link</a>
2023-08-17	[The Clifton Public Schools]	akira	<a href="#">Link</a>
2023-08-17	[MBO-PPS.COM]	clon	<a href="#">Link</a>
2023-08-17	[MBOAMERICA.COM]	clon	<a href="#">Link</a>
2023-08-17	[KOMORI.COM]	clon	<a href="#">Link</a>
2023-08-16	[Dillon Supply]	metaencryptor	<a href="#">Link</a>
2023-08-16	[Epicure]	metaencryptor	<a href="#">Link</a>
2023-08-16	[Coswell]	metaencryptor	<a href="#">Link</a>
2023-08-16	[BOB Automotive Group]	metaencryptor	<a href="#">Link</a>
2023-08-16	[Seoul Semiconductor]	metaencryptor	<a href="#">Link</a>
2023-08-16	[Kraiburg Austria GmbH]	metaencryptor	<a href="#">Link</a>
2023-08-16	[Autohaus Ebert GmbH]	metaencryptor	<a href="#">Link</a>
2023-08-16	[CVO Antwerpen]	metaencryptor	<a href="#">Link</a>
2023-08-16	[ICON Creative Studio]	metaencryptor	<a href="#">Link</a>
2023-08-16	[Heilmann Gruppe]	metaencryptor	<a href="#">Link</a>
2023-08-16	[Schwälbchen Molkerei AG]	metaencryptor	<a href="#">Link</a>
2023-08-16	[Münchener Verlagsgruppe GmbH]	metaencryptor	<a href="#">Link</a>
2023-08-16	[Cequent]	akira	<a href="#">Link</a>
2023-08-16	[Tally Energy Services]	akira	<a href="#">Link</a>
2023-08-16	[CORDELLCORDELL]	alphv	<a href="#">Link</a>
2023-08-16	[Municipality of Ferrara]	rhysida	<a href="#">Link</a>
2023-08-16	[Hemmink]	incransom	<a href="#">Link</a>
2023-08-16	[ToyotaLift Northeast]	8base	<a href="#">Link</a>
2023-08-09	[FTRIA CO. LTD]	noescape	<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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
2023-08-09	[etisaleg.com]	lockbit3	<a href="#">Link</a>
2023-08-09	[2plan.com]	lockbit3	<a href="#">Link</a>
2023-08-08	[Sabalan Azmayesh]	arvinclub	<a href="#">Link</a>
2023-08-09	[Optimum Health Solutions]	rhysida	<a href="#">Link</a>
2023-08-09	[unitycouncil.org]	lockbit3	<a href="#">Link</a>
2023-08-09	[independenceia.org]	lockbit3	<a href="#">Link</a>
2023-08-09	[www.finitia.net]	abyss	<a href="#">Link</a>
2023-08-09	[Ramtha]	rhysida	<a href="#">Link</a>
2023-08-08	[Batesville didn't react on appeal and allows Full Leak]	ragnarlocker	<a href="#">Link</a>
2023-08-08	[ZESA Holdings]	everest	<a href="#">Link</a>
2023-08-08	[Magic Micro Computers]	alphv	<a href="#">Link</a>
2023-08-08	[Emerson School District]	medusa	<a href="#">Link</a>
2023-08-08	[CH informatica]	8base	<a href="#">Link</a>
2023-08-07	[Thonburi Energy Storage Systems (TESM)]	qilin	<a href="#">Link</a>
2023-08-07	[Räddningstjänsten Västra Blekinge]	akira	<a href="#">Link</a>
2023-08-07	[Papel Prensa SA]	akira	<a href="#">Link</a>
2023-08-01	[Kreacta]	noescape	<a href="#">Link</a>
2023-08-07	[Parsian Bitumen]	arvinclub	<a href="#">Link</a>
2023-08-07	[varian.com]	lockbit3	<a href="#">Link</a>
2023-08-06	[Delaney Browne Recruitment]	8base	<a href="#">Link</a>
2023-08-06	[IBL]	alphv	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-08-05	[Draje food industrial group]	arvinclub	<a href="#">Link</a>
2023-08-06	[Oregon Sports Medicine]	8base	<a href="#">Link</a>
2023-08-06	[premierbpo.com]	alphv	<a href="#">Link</a>
2023-08-06	[SatCom Marketing]	8base	<a href="#">Link</a>
2023-08-05	[Rayden Solicitors]	alphv	<a href="#">Link</a>
2023-08-05	[haynesintl.com]	lockbit3	<a href="#">Link</a>
2023-08-05	[Kovair Software Data Leak]	everest	<a href="#">Link</a>
2023-08-05	[Henlaw]	alphv	<a href="#">Link</a>
2023-08-04	[mipe.com]	lockbit3	<a href="#">Link</a>
2023-08-04	[armortex.com]	lockbit3	<a href="#">Link</a>
2023-08-04	[iqcontrols.com]	lockbit3	<a href="#">Link</a>
2023-08-04	[scottevest.com]	lockbit3	<a href="#">Link</a>
2023-08-04	[atser.com]	lockbit3	<a href="#">Link</a>
2023-08-04	[Galicia en Goles]	alphv	<a href="#">Link</a>
2023-08-04	[tetco.com]	lockbit3	<a href="#">Link</a>
2023-08-04	[SBS Construction]	alphv	<a href="#">Link</a>
2023-08-04	[Koury Engineering]	akira	<a href="#">Link</a>
2023-08-04	[Pharmatech Repblica Dominicana was hacked. All sensitive company and customer information ]	alphv	<a href="#">Link</a>
2023-08-04	[Grupo Garza Ponce was hacked! Due to a massive company vulnerability, more than 2 TB of se]	alphv	<a href="#">Link</a>
2023-08-04	[seaside-kish co]	arvinclub	<a href="#">Link</a>
2023-08-04	[Studio Domaine LLC]	nokoyawa	<a href="#">Link</a>
2023-08-04	[THECHANGE]	alphv	<a href="#">Link</a>
2023-08-04	[Ofimedic]	alphv	<a href="#">Link</a>
2023-08-04	[Abatti Companies - Press Release]	monti	<a href="#">Link</a>
2023-08-03	[Spokane Spinal Sports Care Clinic]	bianlian	<a href="#">Link</a>
2023-08-03	[pointpleasant.k12.nj.us]	lockbit3	<a href="#">Link</a>
2023-08-03	[Roman Catholic Diocese of Albany]	nokoyawa	<a href="#">Link</a>
2023-08-03	[Venture General Agency]	akira	<a href="#">Link</a>
2023-08-03	[Datawatch Systems]	akira	<a href="#">Link</a>
2023-08-03	[admsc.com]	lockbit3	<a href="#">Link</a>
2023-08-03	[United Tractors]	rhysida	<a href="#">Link</a>
2023-08-03	[RevZero, Inc]	8base	<a href="#">Link</a>
2023-08-03	[Rossman Realty Group, inc.]	8base	<a href="#">Link</a>
2023-08-03	[riggsabney]	alphv	<a href="#">Link</a>
2023-08-02	[fec-corp.com]	lockbit3	<a href="#">Link</a>
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]	clon	<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>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-08-01	[MBS Equipment TTI]	8base	Link
2023-08-01	[gerb.bg]	lockbit3	Link
2023-08-01	[persingerlaw.com]	lockbit3	Link
2023-08-01	[Jacklett Construction LLC]	8base	Link

# 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.