



Ausgabe: 20230806

# 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

### *Sicherheitsupdates F5 BIG-IP: Angreifer können Passwörter erraten*

Es sind wichtige Sicherheitspatches für mehrere BIG-IP-Produkte von F5 erschienen. Admins sollten zeitnah handeln.

- [Link](#)

---

### *Sicherheitsupdates: Angreifer können Aruba-Switches kompromittieren*

Bestimmte Switch-Modelle von Aruba sind verwundbar. Die Entwickler haben eine Sicherheitslücke geschlossen.

- [Link](#)

---

### *Upgrade nötig: Kritische Lücke bedroht ältere MobileIron-Ausgaben von Ivanti*

Angreifer können an einer kritischen Schwachstelle in der nicht mehr im Support befindlichen Mobile-Device-Management-Lösung Ivanti MobileIron ansetzen.

- [Link](#)

---

### *Firefox, Thunderbird und Tor Browser bekommen Sicherheitsupdates*

Angreifer könnten aus der Firefox-Sandbox ausbrechen. Die Entwickler haben noch weitere Lücken geschlossen.

- [Link](#)

---

### *Angreifer kapern Minecraft-Server über BleedingPipe-Exploit*

Mehrere Minecraft-Modifikationen weisen eine Schwachstelle auf, die Angreifer derzeit aktiv ausnutzen. Davon sollen neben Servern auch Clients betroffen sein.

- [Link](#)

---

### *Sicherheitsupdate: WordPress-Websites mit Plug-in Ninja Forms attackierbar*

Angreifer könnten über eine Sicherheitslücke im Ninja-Forms-Plug-in auf eigentlich geschützte WordPress-Daten zugreifen.

- [Link](#)

---

### *Jetzt patchen! Ivanti schließt erneut Zero-Day-Lücke in EPMM*

Derzeit nehmen Angreifer Ivanti Endpoint Manager Mobile (EPMM) ins Visier. Nun gibt es einen Patch gegen eine weitere Schwachstelle.

- [Link](#)

---

### *Angreifer können NAS- und IP-Videoüberwachungssysteme von Qnap lahmlegen*

Mehrere Netzwerkprodukte von Qnap sind für eine DoS-Attacken anfällig. Dagegen abgesicherte Software schafft Abhilfe.

- [Link](#)

---

### *Jetzt patchen! Angreifer attackieren E-Mail-Lösung Zimbra*

Es ist ein wichtiges Sicherheitsupdate für Zimbra Collaboration Suite erschienen. Admins sollten zügig handeln.

- [Link](#)

---

### *Sicherheitsupdate: Angreifer können Sicherheitslösung Sophos UTM attackieren*

Sophos Unified Threat Management ist verwundbar. Aktuelle Software schafft Abhilfe.

- [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	0.984490000	<a href="#">Link</a>
CVE-2023-35078	0.955330000	0.991090000	<a href="#">Link</a>
CVE-2023-34362	0.940540000	0.987950000	<a href="#">Link</a>
CVE-2023-33246	0.955810000	0.991200000	<a href="#">Link</a>
CVE-2023-28771	0.918810000	0.985140000	<a href="#">Link</a>
CVE-2023-28121	0.937820000	0.987520000	<a href="#">Link</a>
CVE-2023-27372	0.970090000	0.996170000	<a href="#">Link</a>
CVE-2023-27350	0.971160000	0.996740000	<a href="#">Link</a>
CVE-2023-25717	0.960700000	0.992550000	<a href="#">Link</a>
CVE-2023-25194	0.918160000	0.985080000	<a href="#">Link</a>
CVE-2023-21839	0.953670000	0.990630000	<a href="#">Link</a>
CVE-2023-20887	0.960590000	0.992510000	<a href="#">Link</a>
CVE-2023-0669	0.965030000	0.993910000	<a href="#">Link</a>

## BSI - Warn- und Informationsdienst (WID)

Fri, 04 Aug 2023

**[NEU] [UNGEPATCHT] [kritisch] ffmpeg: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymmer Angreifer kann eine Schwachstelle in ffmpeg ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Fri, 04 Aug 2023

**[NEU] [hoch] Ivanti Endpoint Manager Mobile.: Schwachstelle ermöglicht Manipulation von Dateien**

Ein entfernter, anonymmer Angreifer kann eine Schwachstelle in Ivanti Endpoint Manager Mobile. ausnutzen, um Dateien zu manipulieren.

- [Link](#)

Fri, 04 Aug 2023

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

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um vertrauliche Informationen offenzulegen, Sicherheitsmechanismen zu umgehen, den Benutzer zu täuschen und nicht näher beschriebene Auswirkungen zu erzielen.

- [Link](#)

---

Fri, 04 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](#)

---

Fri, 04 Aug 2023

***[UPDATE] [hoch] Red Hat OpenShift: Mehrere Schwachstellen***

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

- [Link](#)

---

Fri, 04 Aug 2023

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

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

- [Link](#)

---

Fri, 04 Aug 2023

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

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

---

Fri, 04 Aug 2023

***[NEU] [hoch] Veritas NetBackup: Mehrere Schwachstellen***

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Veritas NetBackup ausnutzen, um beliebigen Programmcode auszuführen und nicht spezifizierte Auswirkungen zu verursachen.

- [Link](#)

---

Thu, 03 Aug 2023

***[UPDATE] [hoch] vim: Mehrere Schwachstellen ermöglichen Codeausführung***

Ein entfernter, anonymen oder lokaler Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Code auszuführen, Speicher zu modifizieren und einen Denial of Service Zustand zu verursachen.

- [Link](#)

---

Thu, 03 Aug 2023

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

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Programmcode auszuführen, einen Denial of Service Zustand herbeizuführen oder Dateien zu manipulieren.

- [Link](#)

---

Thu, 03 Aug 2023

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

Ein entfernter, anonymen oder lokaler Angreifer kann mehrere Schwachstellen in vim ausnutzen, um einen Denial of Service Angriff durchzuführen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen und den Speicher zu manipulieren.

- [Link](#)

---

Thu, 03 Aug 2023

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

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und vertrauliche Informationen offenzulegen

- [Link](#)

---

Thu, 03 Aug 2023

**[UPDATE] [hoch] Python: Schwachstelle ermöglicht Denial of Service**

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

- [Link](#)

---

Thu, 03 Aug 2023

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

Ein entfernter, anonymen, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft .NET Framework, Microsoft Azure DevOps Server, Microsoft NuGet, Microsoft Visual Studio und Microsoft Visual Studio Code ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen, seine Rechte zu erweitern und Daten zu manipulieren.

- [Link](#)

---

Thu, 03 Aug 2023

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

Ein entfernter, authentisierter oder anonymen Angreifer kann mehrere Schwachstellen in Microsoft Visual Studio 2022, Microsoft Visual Studio Code und Microsoft .NET Framework ausnutzen, um seine Privilegien zu erweitern, beliebigen Programmcode auszuführen, Sicherheitsvorkehrungen zu umgehen oder Dateien zu manipulieren.

- [Link](#)

---

Thu, 03 Aug 2023

**[NEU] [hoch] HP LaserJet: Schwachstelle ermöglicht Privilegieneskalation**

Ein lokaler Angreifer kann eine Schwachstelle in HP LaserJet ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

---

Thu, 03 Aug 2023

**[UPDATE] [hoch] Ruby on Rails: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in Ruby on Rails ausnutzen, um einen Denial of Service Angriff durchzuführen, Daten zu manipulieren und Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

---

Thu, 03 Aug 2023

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

Ein lokaler Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um Informationen offenzulegen und um seine Privilegien zu erweitern.

- [Link](#)

---

Wed, 02 Aug 2023

**[UPDATE] [hoch] Red Hat OpenShift (Logging Subsystem): Schwachstelle ermöglicht Denial of Service**

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in Red Hat OpenShift (Logging Subsystem) ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

---

Wed, 02 Aug 2023

**[UPDATE] [hoch] Grafana: Schwachstelle ermöglicht Übernahme von Benutzerkonto**

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in Grafana ausnutzen, um ein Benutzerkonto zu übernehmen.

- [Link](#)

---

## Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/4/2023	[Fedora 37 : firefox (2023-a4e8720e0f)]	critical
8/4/2023	[Debian DSA-5465-1 : python-django - security update]	critical

Datum	Schwachstelle	Bewertung
8/4/2023	[FreeBSD : chromium – multiple vulnerabilities (6e4e8e87-9fb8-4e32-9f8e-9b4303f4bfd5)]	critical
8/4/2023	[Jenkins plugins Multiple Vulnerabilities (2022-11-15)]	critical
8/4/2023	[AlmaLinux 9 : firefox (ALSA-2023:4462)]	critical
8/4/2023	[AlmaLinux 8 : firefox (ALSA-2023:4468)]	critical
8/4/2023	[Slackware Linux 15.0 / current mozilla-firefox Multiple Vulnerabilities (SSA:2023-216-01)]	critical
8/4/2023	[Oracle Linux 7 : firefox (ELSA-2023-4461)]	critical
8/4/2023	[Oracle Linux 9 : firefox (ELSA-2023-4462)]	critical
8/4/2023	[Oracle Linux 8 : firefox (ELSA-2023-4468)]	critical
8/3/2023	[Siemens SCALANCE X-200RNA Switch Devices Use of Insufficiently Random Values (CVE-2022-46353)]	critical
8/5/2023	[openSUSE 15 Security Update : amanda (openSUSE-SU-2023:0205-1)]	high
8/5/2023	[openSUSE 15 Security Update : amanda (openSUSE-SU-2023:0206-1)]	high
8/5/2023	[Fedora 38 : seamonkey (2023-e7f8101829)]	high
8/5/2023	[Fedora 38 : amanda (2023-4db1d56125)]	high
8/5/2023	[Fedora 37 : libopenmpt (2023-d43fda08d6)]	high
8/5/2023	[Fedora 37 : amanda (2023-566e354e4a)]	high
8/5/2023	[Debian DSA-5467-1 : chromium - security update]	high
8/5/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xtrans (SUSE-SU-2023:3190-1)]	high
8/5/2023	[SUSE SLES12 Security Update : javapackages-tools, javassist, mysql-connector-java, protobuf, python-python-gflags (SUSE-SU-2023:3187-1)]	high
8/5/2023	[SUSE SLES12 Security Update : xtrans (SUSE-SU-2023:3189-1)]	high
8/5/2023	[Debian DLA-3516-1 : burp - LTS security update]	high
8/4/2023	[Fedora 38 : libsvg2 (2023-fc79ee273d)]	high
8/4/2023	[Fedora 38 : webkitgtk (2023-a479289864)]	high
8/4/2023	[Fedora 37 : chromium (2023-8a94349e38)]	high
8/4/2023	[Debian DSA-5464-1 : firefox-esr - security update]	high
8/4/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : go1.20 (SUSE-SU-2023:3181-1)]	high
8/4/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2023:3171-1)]	high
8/4/2023	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2023:3182-1)]	high
8/4/2023	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2023:3180-1)]	high
8/4/2023	[SUSE SLES12 Security Update : mariadb (SUSE-SU-2023:3174-1)]	high
8/4/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2023:3172-1)]	high
8/4/2023	[Debian DLA-3515-1 : cjose - LTS security update]	high
8/4/2023	[CBL Mariner 2.0 Security Update: nghttp2 (CVE-2023-35945)]	high
8/4/2023	[Jenkins plugins Multiple Vulnerabilities (2022-06-30)]	high
8/4/2023	[PHP 8.0.x < 8.0.30 Multiple Vulnerabilities]	high
8/4/2023	[Debian DSA-5466-1 : ntpsec - security update]	high
8/3/2023	[Siemens SCALANCE X-200RNA Switch Devices Uncontrolled Resource Consumption (CVE-2022-46352)]	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
2023-08-06	[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]	clap	<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.