

Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250206



Inhaltsverzeichnis

1 Editorial	2
2 Security-News	3
2.1 Heise - Security-Alert	3
3 Sicherheitslücken	4
3.1 EPSS	4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit	5
3.2 BSI - Warn- und Informationsdienst (WID)	6
3.3 Sicherheitslücken Meldungen von Tenable	10
4 Die Hacks der Woche	12
4.0.1 Wo gehyped wird fallen Späne. Öffentliche Datenbank bei Deepseek	13
5 Cyberangriffe: (Feb)	14
6 Ransomware-Erpressungen: (Feb)	14
7 Quellen	19
7.1 Quellenverzeichnis	19
8 Impressum	21

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

Netgear: Nighthawk Pro Gaming-Router mit Schadcode-Leck

Netgear warnt vor Codeschmuggel-Lücken in Nighthawk Pro Gaming-Routern. Zudem haben einige Router nach Support-Ende eine Sicherheitslücke.

- [Link](#)

—

Veeam Backup: Codeschmuggel durch MitM-Lücke im Updater möglich

Veeam Backup enthält einen Updater, der für Man-in-the-Middle-Attacken anfällig ist. Angreifer können Schadcode einschleusen.

- [Link](#)

—

Zugriffsmanagement: HPE Aruba Networking CPPM ist verwundbar

Netzwerkadmins sollten HPE Aruba Networking ClearPass Policy Manager aus Sicherheitsgründen aktualisieren.

- [Link](#)

—

Support ausgelaufen: Keine Sicherheitsupdates mehr für attackierte Zyxel-Router

Derzeit hat es eine Mirai-Botnet-Malware auf bestimmte Routermodelle von Zyxel abgesehen. Weil der Support ausgelaufen ist, müssen Admins jetzt handeln.

- [Link](#)

—

Patchday Android: Angreifer nutzen Kernel-Sicherheitslücke aus

Es sind wichtige Sicherheitsupdates für Android 12, 12L, 13, 14 und 15 erschienen. Angreifer können Geräte kompromittieren.

- [Link](#)

—

HP Anyware: Linux-Client ermöglicht Rechteausweitung

In HPs Anyware-Client für Linux können Angreifer ihre Rechte am System ausweiten. Ein Softwareupdate steht bereit, das den Fehler korrigiert.

- [Link](#)

—

Sicherheitsupdates: Zahlreiche Lücken gefährden Backup-Appliances von Dell

Mehrere Sicherheitslücken in Dells Data Domain Operating System machen Backup-Appliances der PowerProtect-Serie attackierbar.

- [Link](#)

GarageBand: Böser Fehler kann zu Code-Ausführung führen

Die Mac-Version von Apples Gratis-DAW enthält eine Lücke, die sich offenbar durch Angreifer ausnutzen lässt. Ein Update liegt vor.

- [Link](#)

Medizinischer Überwachungsmonitor: Hintertür in Contec CMS8000 entdeckt

Angreifer können medizinische Hardware von Contec attackieren. Dabei kann Schadcode auf Geräte gelangen. Bislang gibt es kein Sicherheitsupdate.

- [Link](#)

SimpleHelp RMM: Angriffe auf Sicherheitslücken beobachtet

In SimpleHelp RMM missbrauchen Angreifer Sicherheitslücken, um Netzwerke zu kompromittieren. Updates stehen bereit.

- [Link](#)

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-2024-9474	0.974800000	0.999850000	Link
CVE-2024-9465	0.943220000	0.994120000	Link
CVE-2024-9463	0.961860000	0.996670000	Link
CVE-2024-8963	0.967990000	0.998010000	Link
CVE-2024-7593	0.971650000	0.999000000	Link
CVE-2024-6893	0.938390000	0.993640000	Link
CVE-2024-6670	0.910490000	0.991380000	Link
CVE-2024-5910	0.962890000	0.996900000	Link
CVE-2024-55956	0.967520000	0.997880000	Link
CVE-2024-5217	0.933860000	0.993150000	Link
CVE-2024-50623	0.969230000	0.998340000	Link
CVE-2024-4879	0.934670000	0.993220000	Link
CVE-2024-4577	0.958420000	0.996100000	Link
CVE-2024-4358	0.925270000	0.992430000	Link
CVE-2024-41713	0.957210000	0.995880000	Link
CVE-2024-40711	0.963400000	0.996990000	Link
CVE-2024-4040	0.969020000	0.998290000	Link
CVE-2024-38856	0.942880000	0.994090000	Link
CVE-2024-36401	0.952840000	0.995220000	Link
CVE-2024-3400	0.964000000	0.997110000	Link
CVE-2024-3273	0.937410000	0.993530000	Link
CVE-2024-32113	0.914790000	0.991650000	Link
CVE-2024-28995	0.965000000	0.997310000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-28987	0.961930000	0.996680000	Link
CVE-2024-27348	0.960260000	0.996390000	Link
CVE-2024-27198	0.968000000	0.998010000	Link
CVE-2024-24919	0.959630000	0.996280000	Link
CVE-2024-23897	0.973540000	0.999540000	Link
CVE-2024-23692	0.964470000	0.997210000	Link
CVE-2024-21893	0.957440000	0.995930000	Link
CVE-2024-21887	0.973220000	0.999480000	Link
CVE-2024-20767	0.965330000	0.997390000	Link
CVE-2024-1709	0.957220000	0.995880000	Link
CVE-2024-1212	0.937140000	0.993500000	Link
CVE-2024-0986	0.955530000	0.995640000	Link
CVE-2024-0195	0.962680000	0.996850000	Link
CVE-2024-0012	0.969980000	0.998520000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 05 Feb 2025

[UPDATE] [hoch] Red Hat OpenShift: Mehrere Schwachstelle

Ein entfernter, anonymer Angreifer kann mehrere Schwachstelle in Red Hat OpenShift ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen und beliebigen Code auszuführen.

- [Link](#)

—

Wed, 05 Feb 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](#)

—

Wed, 05 Feb 2025

[UPDATE] [hoch] Rsync: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Rsync ausnutzen, um vertrauliche Informationen preiszugeben, sich erhöhte Rechte zu verschaffen und Daten zu manipulieren.

- [Link](#)

—

Wed, 05 Feb 2025

[NEU] [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](#)

—

Wed, 05 Feb 2025

[UPDATE] [hoch] Perl: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit Administratorrechten

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Perl ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen.

- [Link](#)

—

Wed, 05 Feb 2025

[UPDATE] [hoch] cURL: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in cURL und libcurl ausnutzen, um Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen und um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Wed, 05 Feb 2025

[UPDATE] [hoch] GStreamer: Mehrere Schwachstellen ermöglichen Denial of Service

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

- [Link](#)

—

Wed, 05 Feb 2025

[UPDATE] [hoch] GStreamer: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in GStreamer ausnutzen, um Dateien zu manipulieren und einen Denial of Service Zustand herzustellen.

- [Link](#)

—

Wed, 05 Feb 2025

[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

—

Wed, 05 Feb 2025

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

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

- [Link](#)

—

Wed, 05 Feb 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](#)

—

Wed, 05 Feb 2025

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

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

- [Link](#)

—

Wed, 05 Feb 2025

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.

- [Link](#)

—

Wed, 05 Feb 2025

[UPDATE] [hoch] RADIUS: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein lokaler Angreifer kann eine Schwachstelle im RADIUS Protokoll ausnutzen, um Sicherheitsvorkeh-

rungen zu umgehen.

- [Link](#)

—

Wed, 05 Feb 2025

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

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

- [Link](#)

—

Wed, 05 Feb 2025

[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht Privilegieneskalation oder DoS

Ein lokaler Angreifer kann eine Schwachstelle in QEMU ausnutzen, um seine Privilegien zu erhöhen oder eine Denial-of-Service-Situation zu erzeugen.

- [Link](#)

—

Wed, 05 Feb 2025

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

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

- [Link](#)

—

Wed, 05 Feb 2025

[UPDATE] [hoch] Gitea: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Gitea ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Wed, 05 Feb 2025

[UPDATE] [hoch] Red Hat Enterprise Linux und OpenShift (go-git): Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux in der Grafana Komponente ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen preiszugeben und einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Wed, 05 Feb 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](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/5/2025	[Debian dsa-5858 : firefox-esr - security update]	critical
2/5/2025	[Amazon Linux 2023 : amazon-ssm-agent (ALAS2023-2025-824)]	critical
2/5/2025	[Amazon Linux 2023 : runfinch-finch (ALAS2023-2025-834)]	critical
2/5/2025	[Amazon Linux 2023 : containerd, containerd-stress (ALAS2023-2025-835)]	critical
2/5/2025	[Amazon Linux 2023 : nerdctl (ALAS2023-2025-833)]	critical
2/5/2025	[Amazon Linux 2023 : python3-virtualenv (ALAS2023-2025-831)]	critical
2/5/2025	[Slackware Linux 15.0 / current curl Multiple Vulnerabilities (SSA:2025-036-01)]	critical
2/5/2025	[Slackware Linux 15.0 / current mozilla-thunderbird Multiple Vulnerabilities (SSA:2025-036-03)]	critical
2/5/2025	[Dell EMC NetWorker Unquoted Search Path (DSA-2025-064)]	high
2/5/2025	[Juniper Junos OS Authentication for Critical Function (CVE-2024-21620)]	high
2/5/2025	[OpenLink Virtuoso < 7.2.14 DoS]	high
2/5/2025	[VMware Aria Operations for Logs < 8.18.3 Multiple Vulnerabilities (VMSA-2025-0003)]	high
2/5/2025	[F5 Networks BIG-IP : BIG-IP PEM vulnerability (K000140920)]	high
2/5/2025	[F5 Networks BIG-IP : BIG-IP PEM vulnerability (K000139778)]	high
2/5/2025	[F5 Networks BIG-IP : TMM vulnerability (K000134888)]	high

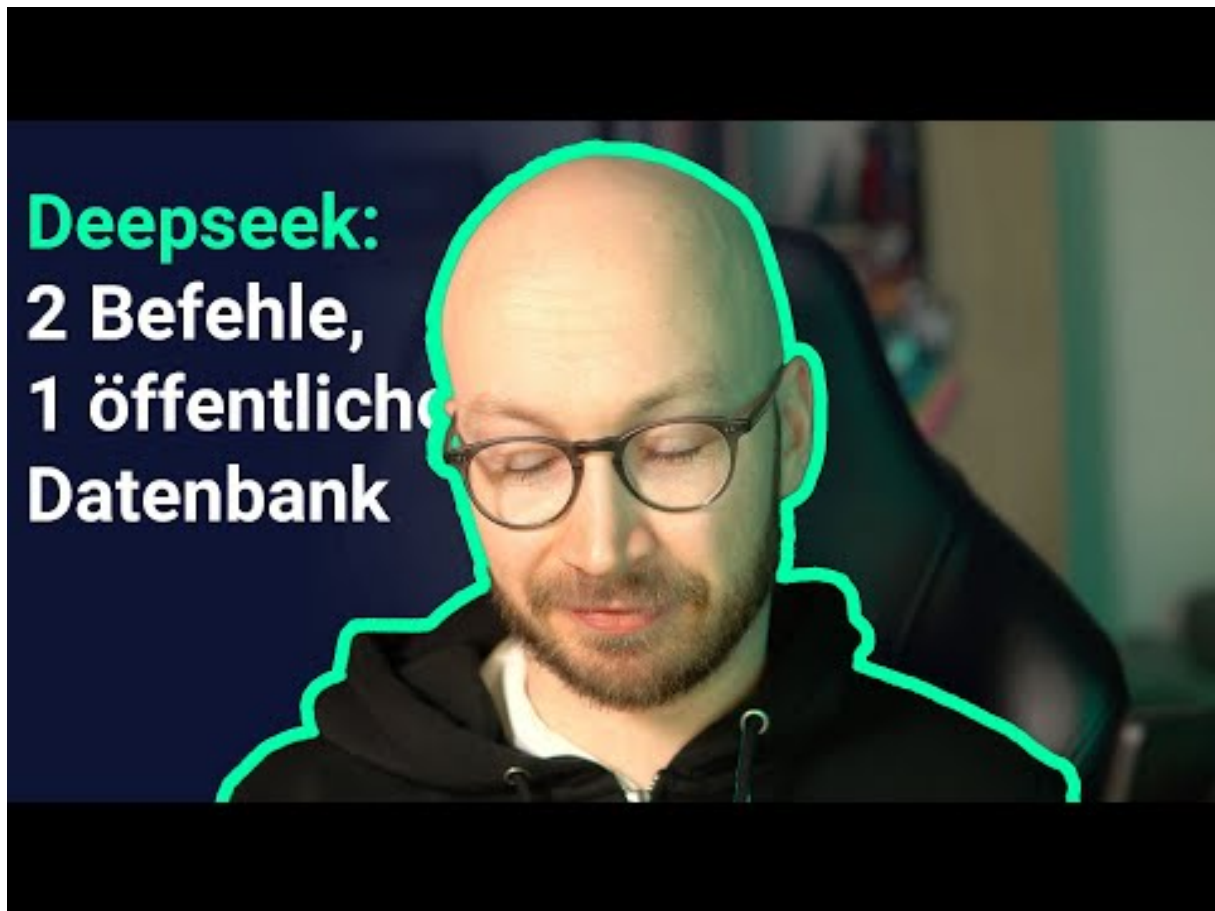
Datum	Schwachstelle	Bewertung
2/5/2025	[F5 Networks BIG-IP : BIG-IP message routing vulnerability (K000140947)]	high
2/5/2025	[F5 Networks BIG-IP : BIG-IP Configuration utility vulnerability (K000140578)]	high
2/5/2025	[F5 Networks BIG-IP : BIG-IP iControl REST vulnerability (K000138757)]	high
2/5/2025	[F5 Networks BIG-IP : BIG-IP SIP ALG profile vulnerability (K000138932)]	high
2/5/2025	[F5 Networks BIG-IP : BIG-IP ASM BAdoS vulnerability (K000140950)]	high
2/5/2025	[F5 Networks BIG-IP : BIG-IP SNMP vulnerability (K000140933)]	high
2/5/2025	[F5 Networks BIG-IP : BIG-IP APM access profile vulnerability (K000141003)]	high
2/5/2025	[F5 Networks BIG-IP : BIG-IP SIP ALG vulnerability (K000139780)]	high
2/5/2025	[F5 Networks BIG-IP : BIG-IP iControl REST and tmsh vulnerability (K000148587)]	high
2/5/2025	[F5 Networks BIG-IP : BIG-IP AFM vulnerability (K000141380)]	high
2/5/2025	[Amazon Linux AMI : less (ALAS-2025-1958)]	high
2/5/2025	[Amazon Linux AMI : postgresql92 (ALAS-2025-1959)]	high
2/5/2025	[Amazon Linux 2023 : python3.11, python3.11-devel, python3.11-idle (ALAS2023-2025-829)]	high
2/5/2025	[Amazon Linux 2023 : nodejs20, nodejs20-devel, nodejs20-full-i18n (ALAS2023-2025-822)]	high
2/5/2025	[Amazon Linux 2023 : bpftool, kernel, kernel-devel (ALAS2023-2025-823)]	high
2/5/2025	[Amazon Linux 2023 : wireshark-cli, wireshark-devel (ALAS2023-2025-837)]	high
2/5/2025	[Amazon Linux 2023 : bpftool, kernel, kernel-devel (ALAS2023-2025-836)]	high

Datum	Schwachstelle	Bewertung
2/5/2025	[Amazon Linux 2023 : bind, bind-chroot, bind-devel (ALAS2023-2025-838)]	high
2/5/2025	[Amazon Linux AMI : kernel (ALAS-2025-1957)]	high
2/5/2025	[Schneider Electric Modicon Improper Enforcement of Message Integrity During Transmission	
in a Communication Channel (CVE-2023-6408)]	high	

4 Die Hacks der Woche

mit Martin Haunschmid

4.0.1 Wo gehyped wird fallen Späne. Öffentliche Datenbank bei Deepseek



[Zum Youtube Video](#)

5 Cyberangriffe: (Feb)

Datum	Opfer	Land	Information
2025-02-02	Top-Medien	[CHE]	Link
2025-02-02	Mayer Steel Pipe Corporation	[TWN]	Link
2025-02-02	Nan Ya PCB (KunShan) Corp.	[TWN]	Link
2025-02-01	CESI	[FRA]	Link

6 Ransomware-Erpressungen: (Feb)

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-05	[McCORMICK TAYLOR]	qilin	Link
2025-02-05	[www.iecsolutions.com]	safepay	Link
2025-02-05	[corehandf.com]	threeam	Link
2025-02-05	[Dash Business]	bianlian	Link
2025-02-05	[Hall Chadwick]	bianlian	Link
2025-02-05	[NESCTC Security Services]	bianlian	Link
2025-02-05	[Shinsung Delta Tech]	lynx	Link
2025-02-05	[Banfi Vintners]	lynx	Link
2025-02-05	[annegrady.org]	ransomhub	Link
2025-02-05	[rablighting.com]	qilin	Link
2025-02-05	[boostheat.com]	apt73	Link
2025-02-05	[rattelacademy.com]	funksec	Link
2025-02-05	[cara.com.my]	funksec	Link
2025-02-05	[Mid-State Machine & Fabricating Corp]	play	Link
2025-02-04	[casperstruck.com]	kairos	Link
2025-02-04	[medicalreportsltd.com]	kairos	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-01	[LUA Coffee]	fog	Link
2025-02-01	[GFZ Helmholtz Centre for Geosciences]	fog	Link
2025-02-01	[PT. ITPRENEUR INDONESIA TECHNOLOGY]	fog	Link
2025-02-04	[Devlion]	fog	Link
2025-02-04	[SOLEIL]	fog	Link
2025-02-04	[hemio.de]	fog	Link
2025-02-03	[Madia]	fog	Link
2025-02-03	[X-lab group]	fog	Link
2025-02-03	[Bolin Centre for Climate Research]	fog	Link
2025-02-04	[Gitlabs: hemio.de, SOLEIL, Devlion]	fog	Link
2025-02-04	[escada.com]	ransomhub	Link
2025-02-04	[mielectric.com.br]	akira	Link
2025-02-04	[engineeredequip.com]	akira	Link
2025-02-04	[emin.cl]	akira	Link
2025-02-04	[alphascriptrx.com]	akira	Link
2025-02-04	[premierop.com]	akira	Link
2025-02-04	[acesaz.com]	akira	Link
2025-02-04	[mipa.com.br]	akira	Link
2025-02-04	[usm-americas.com]	akira	Link
2025-02-04	[feheq.com]	akira	Link
2025-02-04	[stewartautosales.com]	akira	Link
2025-02-04	[milleraa.com]	akira	Link
2025-02-04	[jsfrental.com]	akira	Link
2025-02-04	[summitmovinghouston.com]	akira	Link
2025-02-04	[dwgp.com]	akira	Link
2025-02-04	[easycom.com]	akira	Link
2025-02-04	[alfa.com.co]	akira	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-04	[westernwoodsinc.com]	akira	Link
2025-02-04	[viscira.com]	akira	Link
2025-02-04	[elitt-sas.fr]	akira	Link
2025-02-04	[cfctech.com]	akira	Link
2025-02-04	[armellini.com]	akira	Link
2025-02-04	[mbacomputer.com]	akira	Link
2025-02-04	[directex.net]	akira	Link
2025-02-04	[360energy.com.ar]	akira	Link
2025-02-04	[saludsa.com.ec]	akira	Link
2025-02-04	[intercomp.com.mt]	akira	Link
2025-02-04	[sportadmin.se]	ransomhub	Link
2025-02-04	[C & R Molds Inc]	bianlian	Link
2025-02-04	[Commercial Solutions]	bianlian	Link
2025-02-04	[www.aymcdonald.com]	ransomhub	Link
2025-02-04	[capstoneins.ca]	ransomhub	Link
2025-02-04	[clarkfreightways.com]	ransomhub	Link
2025-02-04	[mistralsolutions.com]	apt73	Link
2025-02-04	[India car owners]	apt73	Link
2025-02-04	[Alshu, Eshoo]	ransomhouse	Link
2025-02-04	[kksp.com]	qilin	Link
2025-02-04	[brainsystem.eu]	funksec	Link
2025-02-04	[Taking stock of 2024]	Part 2]	akira
2025-02-04	[esle.eu]	funksec	Link
2025-02-04	[forum-rainbow-rp.forumotion.eu]	funksec	Link
2025-02-04	[mgainnovation.com]	cactus	Link
2025-02-04	[cornwelltools.com]	cactus	Link
2025-02-04	[rashtiandrashti.com]	cactus	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-04	[alojaimi.com]	ransomhub	Link
2025-02-04	[www.aswgr.com]	ransomhub	Link
2025-02-04	[heartlandrvs.com]	ransomhub	Link
2025-02-04	[gaheritagefcu.org]	ransomhub	Link
2025-02-04	[SSMC]	cicada3301	Link
2025-02-04	[Rivers Casino and Rush Street Gaming]	cicada3301	Link
2025-02-04	[Asterra Properties]	cicada3301	Link
2025-02-04	[Caliente Construction]	cicada3301	Link
2025-02-04	[C2S Technologies Inc.]	everest	Link
2025-02-04	[ITSS]	everest	Link
2025-02-03	[brewsterfiredepartment.org]	safepay	Link
2025-02-03	[Dickerson & Nieman Realtors]	play	Link
2025-02-03	[Sheridan Nurseries]	play	Link
2025-02-03	[The Hill Brush]	play	Link
2025-02-03	[DPC Development]	play	Link
2025-02-03	[Woodway USA]	play	Link
2025-02-03	[Daniel Island Club]	play	Link
2025-02-03	[QGS Development]	play	Link
2025-02-03	[Gitlabs: Bolin Centre for Climate Research, X-lab group, Madia]	fog	Link
2025-02-03	[gruppozaccaria.it]	lockbit3	Link
2025-02-03	[Karadeniz Holding (karadenizholding.com)]	fog	Link
2025-02-03	[www.wongfleming.com]	ransomhub	Link
2025-02-03	[smithmidland.com]	ransomhub	Link
2025-02-03	[www.origene.com]	ransomhub	Link
2025-02-03	[Denton Regional Suicide Prevention Coalition]	qilin	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-03	[fasttrackcargo.com]	funksec	Link
2025-02-03	[Ponte16 Hotel & Casino]	killsec	Link
2025-02-03	[Elslaw.com (EARLY , LUCARELLI , SWEENEY & MEISENKOTHEN LAW)]	qilin	Link
2025-02-03	[DRI Title & Escrow]	qilin	Link
2025-02-03	[DPA Auctions]	qilin	Link
2025-02-03	[Altair Travel]	qilin	Link
2025-02-03	[Civil Design, Inc]	qilin	Link
2025-02-03	[The Gatesworth Senior Living St. Louis]	qilin	Link
2025-02-03	[GOVirtual-it.com (VIRTUAL IT)]	qilin	Link
2025-02-03	[coel.com.mx]	apt73	Link
2025-02-03	[Alford Walden Law]	qilin	Link
2025-02-03	[Pasco Systems]	qilin	Link
2025-02-03	[MPP Group of Companies]	qilin	Link
2025-02-03	[Pineland community service board]	spacebears	Link
2025-02-02	[usuhs.edu]	lockbit3	Link
2025-02-02	[Four Eye Clinics]	abyss	Link
2025-02-02	[jpcgroupinc.com]	abyss	Link
2025-02-02	[hreu.eu]	funksec	Link
2025-02-02	[Tosaf]	handala	Link
2025-02-02	[turbomp]	stormous	Link
2025-02-02	[Cyrious Software]	bianlian	Link
2025-02-02	[Medical Associates of Brevard]	bianlian	Link
2025-02-02	[Civic Committee]	bianlian	Link
2025-02-02	[Ayres Law Firm]	bianlian	Link
2025-02-02	[Growth Acceleration Partners]	bianlian	Link
2025-02-01	[fiberskynet.net]	funksec	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-01	[tirtaraharja.co.id]	funksec	Link
2025-02-01	[Gitlabs: PT. ITPRENEUR INDONESIA TECHNOLOGY, GFZ Helmholtz Centre for Geosciences, LUA Cof...]	fog	Link
2025-02-01	[myisp.live]	funksec	Link
2025-02-01	[DATACONSULTANTS.COM]	clop	Link
2025-02-01	[CHAMPIONHOMES.COM]	clop	Link
2025-02-01	[CIERANT.COM]	clop	Link
2025-02-01	[DATATRAC.COM]	clop	Link
2025-02-01	[Nano Health]	killsec	Link
2025-02-01	[St. Nicholas School]	8base	Link
2025-02-01	[Héron]	8base	Link
2025-02-01	[Tan Teck Seng Electric (Co) Pte Ltd]	8base	Link
2025-02-01	[High Learn Ltd]	8base	Link
2025-02-01	[CAMRIDGEPORT]	spacebears	Link
2025-02-01	[Falcon Gaming]	arcusmedia	Link
2025-02-01	[Eascon]	arcusmedia	Link
2025-02-01	[Utilissimo Transportes]	arcusmedia	Link
2025-02-01	[GATTELLI SpA]	arcusmedia	Link
2025-02-01	[Technico]	arcusmedia	Link
2025-02-01	[Wireless Solutions (Morris.Domain)]	lynx	Link

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
- 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

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