Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250306

Inhaltsverzeichnis

1 Editorial

Guten Morgen,

willkommen zum Cybersecurity Morgenreport von Cyberwald, Ihrem täglichen Begleiter in der Welt der IT-Sicherheit. Als nicht-kommerzielles Projekt ist es unser Anliegen, Awareness und Wissen rund um das Thema Cybersecurity kostenlos zu vermitteln. In der heutigen digitalen Welt ist es für Unternehmen von entscheidender Bedeutung, sich über aktuelle Sicherheitsrisiken zeitnah zu informieren. Cyberbedrohungen entwickeln sich ständig weiter und können erhebliche Schäden verursachen, wenn sie nicht rechtzeitig erkannt und abgewehrt werden. Durch die Nutzung aktueller Informationen können Unternehmen ihre IT-Sicherheitsmaßnahmen stärken und sich effektiv gegen diese Bedrohungen schützen.

Unser Ziel ist es, Ihnen, den IT-Verantwortlichen, einen kompakten und leicht verständlichen Überblick über aktuelle Sicherheitsrisiken zu geben. Wir präsentieren Ihnen täglich Sicherheitsmeldungen und Berichte über neue Sicherheitslücken, die Ihre Systeme und Daten bedrohen könnten.

Darüber hinaus listen wir aktuelle Cyberangriffe und Ransomware-Vorfälle auf. Dies ist von besonderer Bedeutung, da es Unternehmen ermöglicht, sich auf mögliche Supply-Chain- und Phishing-Angriffe vorzubereiten. Durch das Verständnis der Methoden und Taktiken, die von Cyberkriminellen verwendet werden, können Unternehmen ihre Verteidigungsmaßnahmen entsprechend anpassen und stärken.

Für den Cybersecurity Morgenreport greifen wir automatisiert auf öffentliche Informationsquellen zu, filtern und sortieren diese Informationen, um sie Ihnen in einer übersichtlichen Form zur Verfügung zu stellen. Wir bemühen uns, die Inhalte so verständlich wie möglich zu gestalten und vorzugsweise vollständig in deutscher Sprache wiederzugeben. Bei Bedarf übersetzen wir die öffentlichen Informationen und fassen sie durch eine KI zusammen.

Der Cybersecurity Morgenreport ist ein dynamisches Projekt. Wir passen und erweitern unsere Inhalte ständig, um Ihnen die relevantesten und aktuellsten Informationen zu liefern. Derzeit befinden wir uns im Alpha-Stadium des Projekts und freuen uns über Ihr Feedback und Ihre Anregungen.

Wir hoffen, dass der Cybersecurity Morgenreport Ihnen hilft, Ihre IT-Sicherheitsmaßnahmen zu verbessern und Ihre Systeme vor den ständig wechselnden Bedrohungen zu schützen. Bleiben Sie sicher und informiert mit dem Cybersecurity Morgenreport von Cyberwald.

Ihr Cyberwald-Team

2 Security-News

2.1 Heise - Security-Alert

3 Sicherheitslücken

Eine Sicherheitslücke oder Schwachstelle ist ein Fehler in einer Software oder Hardware, der es einem Angreifer ermöglicht, in ein Computersystem einzudringen und Schaden anzurichten. Diese Lücke stellt eine Bedrohung für die Sicherheit des Systems dar, da sie ausgenutzt werden kann, um das System zu kompromittieren. Sicherheitslücken entstehen oft durch unzureichenden Schutz des Computers vor Netzwerkangriffen, zum Beispiel durch fehlende Firewall oder andere Sicherheitssoftware. Auch Programmierfehler im Betriebssystem, Webbrowser oder anderen Anwendungen können Sicherheitslücken verursachen. Bekannte Sicherheitslücken sollten daher so schnell wie möglich durch das Einspielen eines Patches geschlossen werden, um die Angriffsfläche der IT-Systeme zu verringern.

3.1 EPSS

Das Exploit Prediction Scoring System wird für eine bekannte Software-Sicherheitslücke / CVE auf einer Skala von 0 (0%) bis 1 (100%) angegeben und soll die Wahrscheinlichkeit für das Auftreten eines Exploits in naher Zukunft darstellen. Ein höherer Wert bedeutet eine höhere Wahrscheinlichkeit, dass eine Schwachstelle in naher Zukunft ausgenutzt wird. EPSS kann auch als Rahmen für die Priorisierung von Schwachstellen unter Verwendung einer Kombination von Metriken betrachtet werden. Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2025-0108	0.967640000	0.997960000	Link
CVE-2024-9474	0.974550000	0.999800000	Link
CVE-2024-9465	0.939910000	0.993880000	Link
CVE-2024-9463	0.961860000	0.996710000	Link
CVE-2024-8963	0.966010000	0.997650000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-7593	0.967500000	0.997950000	Link
CVE-2024-6670	0.904230000	0.991210000	Link
CVE-2024-5910	0.967810000	0.998000000	Link
CVE-2024-55956	0.968970000	0.998310000	Link
CVE-2024-53704	0.960740000	0.996520000	Link
CVE-2024-5217	0.948330000	0.994800000	Link
CVE-2024-50623	0.969520000	0.998460000	Link
CVE-2024-50603	0.924330000	0.992540000	Link
CVE-2024-4879	0.952210000	0.995240000	Link
CVE-2024-4577	0.951770000	0.995200000	Link
CVE-2024-4358	0.921450000	0.992370000	Link
CVE-2024-41713	0.957210000	0.995930000	Link
CVE-2024-40711	0.964240000	0.997240000	Link
CVE-2024-4040	0.967700000	0.997980000	Link
CVE-2024-38856	0.941790000	0.994040000	Link
CVE-2024-36401	0.961880000	0.996720000	Link
CVE-2024-3400	0.958850000	0.996190000	Link
CVE-2024-3273	0.937240000	0.993620000	Link
CVE-2024-32113	0.938440000	0.993720000	Link
CVE-2024-28995	0.969950000	0.998570000	Link
CVE-2024-28987	0.965400000	0.997480000	Link
CVE-2024-27348	0.960910000	0.996540000	Link
CVE-2024-27198	0.970470000	0.998730000	Link
CVE-2024-24919	0.963920000	0.997130000	Link
CVE-2024-23897	0.973580000	0.999570000	Link
CVE-2024-2389	0.928740000	0.992860000	Link
CVE-2024-23692	0.967310000	0.997910000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-21893	0.960410000	0.996460000	Link
CVE-2024-21887	0.973690000	0.999600000	Link
CVE-2024-20767	0.964870000	0.997370000	Link
CVE-2024-1709	0.957060000	0.995900000	Link
CVE-2024-1212	0.946600000	0.994560000	Link
CVE-2024-0986	0.954890000	0.995600000	Link
CVE-2024-0195	0.962680000	0.996900000	Link
CVE-2024-0012	0.969610000	0.998490000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 05 Mar 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um einen Denial of Service Zustand herbeizuführen oderum einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Wed, 05 Mar 2025

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Linux und Ubuntu Linux ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 05 Mar 2025

[NEU] [hoch] Kibana: Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Kibana ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 05 Mar 2025

[NEU] [hoch] Google Chrome: Mehrere Schwachstellen ermöglichen Denial of Service

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

- Link

—

Wed, 05 Mar 2025

[NEU] [hoch] Commvault Backup & Recovery: Schwachstelle ermöglicht Codeausführung

Ein Angreifer kann eine Schwachstelle in Commvault Backup & Recovery ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 05 Mar 2025

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um Spoofing-Angriffe durchzuführen, Sicherheitsmaßnahmen zu umgehen, erhöhte Privilegien zu erlangen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, Daten zu manipulieren, beliebigen Code auszuführen oder nicht spezifizierte Auswirkungen zu verursachen.

- Link

—

Wed, 05 Mar 2025

[NEU] [hoch] Pixel Patchday March 2025: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um sich erweiterte Rechte zu verschaffen, vertrauliche Informationen preiszugeben und einen Denial-of-Service-Zustand auszulösen.

- Link

—

Wed, 05 Mar 2025

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

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

- Link

—

Wed, 05 Mar 2025

[UPDATE] [hoch] Jenkins Plugins: Mehrere Schwachstellen

Ein entfernter authentisierter Angreifer oder ein anonymer Angreifer kann mehrere Schwachstellen in Jenkins ausnutzen, um Dateien zu manipulieren, vertrauliche Informationen preiszugeben, beliebigen Code auszuführen, sich erhöhte Rechte zu verschaffen und einen Cross-Site-Scripting-Angriff

durchzuführen.

- Link

—

Wed, 05 Mar 2025

[UPDATE] [hoch] Jenkins: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Jenkins ausnutzen, um Sicherheitsmaßnahmen zu umgehen, einen Cross-Site-Scripting-Angriff durchzuführen und einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Wed, 05 Mar 2025

[UPDATE] [hoch] Red Hat Enterprise Linux (Podman und Buildah): Schwachstelle ermöglicht Manipulation von Dateien

Ein lokaler Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um Dateien zu manipulieren.

- Link

—

Wed, 05 Mar 2025

[UPDATE] [hoch] VMware ESXi: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in VMware ESXi, VMware Workstation, VMware Fusion und VMware Cloud Foundation ausnutzen, um beliebigen Code auszuführen, erhöhte Rechte zu erlangen und vertrauliche Informationen preiszugeben.

- Link

—

Tue, 04 Mar 2025

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

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

- Link

—

Tue, 04 Mar 2025

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

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

- Link

—

Tue, 04 Mar 2025

[UPDATE] [hoch] WebKit (GTK und WPE): Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in WebKit ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen preiszugeben und einen Denial-of-Service-Zustand zu erzeugen.
- Link

—

Tue, 04 Mar 2025

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

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

—

Tue, 04 Mar 2025

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht SQL Injection und Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um eine SQL Injection durchzuführen und in der Folge beliebigen Programmcode auszuführen.
- Link

—

Tue, 04 Mar 2025

[UPDATE] [hoch] Red Hat Enterprise Linux (Quarkus): Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Quarkus auf Red Hat Enterprise Linux ausnutzen, um Informationen offenzulegen, oder einen Denial of Service auszulösen.
- Link

—

Tue, 04 Mar 2025

[NEU] [hoch] Android Patchday März 2025: Mehrere Schwachstellen

Ein Angreifer kann diese Schwachstellen ausnutzen, um seine Privilegien zu erweitern, einen Denial-of-Service-Zustand zu erzeugen, beliebigen Code auszuführen oder vertrauliche Informationen preiszugeben.
- Link

—

Tue, 04 Mar 2025

[NEU] [hoch] ESRI ArcGIS: Mehrere Schwachstellen

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in ESRI ArcGIS ausnutzen, um Dateien zu manipulieren, Cross-Site-Scripting durchzuführen, Informationen offenzulegen oder Sicherheitsvorkehrungen zu umgehen.
- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/5/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-10229]	high
3/5/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-2174]	high
3/5/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-29509]	high
3/5/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-2698]	high
3/5/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-26882]	high
3/5/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-26996]	high
3/5/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-30156]	high
3/5/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-0841]	high
3/5/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-25744]	high
3/5/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-10488]	high
3/5/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-1135]	high
3/5/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-27322]	high
3/5/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-3159]	high
3/5/2025	[Linux Distros Unpatched Vulnerability : CVE-2024-0806]	high

4 Die Hacks der Woche

mit Martin Haunschmid

4.0.1 Private video

Vorschaubild Zum Youtube Video

5 Cyberangriffe: (Mär)

Datum	Opfer	Land	Information
2025-03-04	Unikorn Semiconductor Corp.	[TWN]	Link
2025-03-04	Stadtwerke Schwerte	[DEU]	Link
2025-03-03	Whitman Hospital and Medical Clinics	[USA]	Link
2025-03-02	HomeTeamNS	[SGP]	Link
2025-03-02	POLSA (Polish Space Agency)	[POL]	Link
2025-03-02	Adval Tech Group	[CHE]	Link
2025-03-02	Penn-Harris-Madison school district	[USA]	Link
2025-03-02	Ivinhema	[BRA]	Link

6 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-03-06	[Elite Advanced Laser Corporation]	akira	Link
2025-03-05	[1X Internet]	fog	Link
2025-03-05	[Bizcode]	fog	Link
2025-03-05	[Manning Publications Co.]	fog	Link
2025-03-05	[Engikam]	fog	Link
2025-03-05	[FHNW]	fog	Link
2025-03-05	[Aeonsparx]	fog	Link
2025-03-05	[Flightsim studio]	fog	Link
2025-03-05	[Neopoly]	fog	Link
2025-03-05	[Kr3m]	fog	Link
2025-03-05	[InfoReach]	fog	Link
2025-03-05	[Euranova]	fog	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-03-05	[Inelmatic]	fog	Link
2025-03-05	[Kotliva]	fog	Link
2025-03-05	[Blue Planet]	fog	Link
2025-03-05	[Eumetsat]	fog	Link
2025-03-05	[Melexis]	fog	Link
2025-03-06	[City government office in Van (Turkey) - van.bel.tr]	skira	Link
2025-03-06	[Law Diary (USA)]	skira	Link
2025-03-06	[Carruth Compliance Consulting]	skira	Link
2025-03-06	[CCL Products India]	skira	Link
2025-03-06	[Krisala Developer (India)]	skira	Link
2025-03-05	[The 19 biggest gitlabs]	fog	Link
2025-03-05	[willms-fleisch.de]	safepay	Link
2025-03-05	[Pervedant]	lynx	Link
2025-03-05	[SCOLARO FETTER GRIZANTI & McGOUGH, P.C. (scolaro.com)]	fog	Link
2025-03-05	[www.black-star.fr]	ransomhub	Link
2025-03-05	[Adrenalina]	akira	Link
2025-03-05	[Cyncly Company]	akira	Link
2025-03-05	[City Plumbing & Electric Supply Co]	akira	Link
2025-03-03	[www.japanrebuilt.jp]	ransomhub	Link
2025-03-04	[www.sunsweet.com]	ransomhub	Link
2025-03-05	[Best Collateral, Inc.]	rhysida	Link
2025-03-04	[Chicago Doorways, LLC]	qilin	Link
2025-03-05	[Schmiedetechnik Plettenberg GmbH & Co KG]	lynx	Link
2025-03-04	[365labs - Security Corp]	monti	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-03-04	[PFS Grupo - Plan de igualdad, Sostenibilidad]	qilin	Link
2025-03-04	[Pampili (pampili.com.br)]	fog	Link
2025-03-04	[Keystone Pacific Property Management LLC]	bianlian	Link
2025-03-04	[Mosley Glick O'Brien, Inc.]	bianlian	Link
2025-03-04	[FANTIN group]	akira	Link
2025-03-04	[Grupo Baston Aerossol (baston.com.br)]	fog	Link
2025-03-04	[Ray Fogg Corporate Properties]	akira	Link
2025-03-04	[goencon.com]	ransomhub	Link
2025-03-04	[Seabank Group]	lynx	Link
2025-03-04	[Tata Technologies]	hunters	Link
2025-03-04	[Wendy Wu Tours]	killsec	Link
2025-03-04	[rockhillwc.com]	qilin	Link
2025-03-04	[bpmmicro.com]	qilin	Link
2025-03-04	[peruzzi.com]	qilin	Link
2025-03-04	[IOVATE.COM]	clop	Link
2025-03-04	[Legal Aid Society of Salt Lake]	bianlian	Link
2025-03-04	[Ewald Consulting]	bianlian	Link
2025-03-04	[Netcom-World]	apos	Link
2025-03-04	[InternetWay]	apos	Link
2025-03-04	[cimenyan.desa.id]	funksec	Link
2025-03-03	[familychc.com]	ransomhub	Link
2025-03-03	[andreyevengineering.com]	ransomhub	Link
2025-03-03	[drvitenas.com]	kairos	Link
2025-03-03	[usarice.com]	kairos	Link
2025-03-03	[Sunnking SustainableSolutions]	akira	Link
2025-03-03	[LINKGROUP]	arcusmedia	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-03-03	[Openreso]	arcusmedia	Link
2025-03-03	[Itapeseg]	arcusmedia	Link
2025-03-03	[logic insectes]	arcusmedia	Link
2025-03-03	[RJ IT Solutions]	arcusmedia	Link
2025-03-03	[Grafitec]	arcusmedia	Link
2025-03-03	[synaptic.co.tz]	arcusmedia	Link
2025-03-03	[quigleyeye.com]	cactus	Link
2025-03-03	[La Unión]	lynx	Link
2025-03-03	[Central McGowan (centralmcgowan.com)]	fog	Link
2025-03-03	[Klesk Metal Stamping Co (kleskmetalstamping.com)]	fog	Link
2025-03-03	[Forstenlechner Installationstechnik]	akira	Link
2025-03-03	[ceratec.com]	abyss	Link
2025-03-02	[Pre Con Industries]	play	Link
2025-03-02	[IT-IQ Botswana]	play	Link
2025-03-02	[North American Fire Hose]	play	Link
2025-03-02	[Couri Insurance Agency]	play	Link
2025-03-02	[Optometrics]	play	Link
2025-03-02	[International Process Plants]	play	Link
2025-03-02	[Ganong Bros]	play	Link
2025-03-02	[FM.GOB.AR]	monti	Link
2025-03-02	[gruppocogesi.org]	lockbit3	Link
2025-03-02	[Bell Ambulance]	medusa	Link
2025-03-02	[Workforce Group]	killsec	Link
2025-03-01	[germancentre.sg]	incransom	Link
2025-03-01	[breakawayconcretecutting.com]	incransom	Link
2025-03-01	[JEFFREYCOURT.COM]	clop	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-03-01	[APTEAN.COM]	clop	Link
2025-03-01	[Wayne County, Michigan]	interlock	Link
2025-03-01	[The Smeg Group]	interlock	Link
2025-03-01	[Newton & Associates, Inc]	rhysida	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.