

Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250302



Inhaltsverzeichnis

1 Editorial	2
2 Security-News	3
2.1 Heise - Security-Alert	3
3 Sicherheitslücken	3
3.1 EPSS	3
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit	3
3.2 BSI - Warn- und Informationsdienst (WID)	5
3.3 Sicherheitslücken Meldungen von Tenable	8
4 Die Hacks der Woche	11
4.0.1 Private video	11
5 Cyberangriffe: (Mär)	12
6 Ransomware-Erpressungen: (Mär)	12
7 Quellen	12
7.1 Quellenverzeichnis	12
8 Impressum	13

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	0.997950000	Link
CVE-2024-9474	0.974700000	0.999830000	Link
CVE-2024-9465	0.939910000	0.993870000	Link
CVE-2024-9463	0.961860000	0.996720000	Link
CVE-2024-8963	0.966400000	0.997710000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-7593	0.967500000	0.997930000	Link
CVE-2024-6670	0.904230000	0.991190000	Link
CVE-2024-5910	0.967810000	0.997980000	Link
CVE-2024-55956	0.968970000	0.998290000	Link
CVE-2024-53704	0.960740000	0.996510000	Link
CVE-2024-5217	0.948330000	0.994780000	Link
CVE-2024-50623	0.969520000	0.998440000	Link
CVE-2024-50603	0.924330000	0.992520000	Link
CVE-2024-4879	0.952210000	0.995230000	Link
CVE-2024-4577	0.951770000	0.995190000	Link
CVE-2024-4358	0.921450000	0.992340000	Link
CVE-2024-41713	0.957210000	0.995930000	Link
CVE-2024-40711	0.964240000	0.997220000	Link
CVE-2024-4040	0.967700000	0.997960000	Link
CVE-2024-38856	0.941790000	0.994040000	Link
CVE-2024-36401	0.961880000	0.996720000	Link
CVE-2024-3400	0.962560000	0.996850000	Link
CVE-2024-3273	0.935040000	0.993390000	Link
CVE-2024-32113	0.938440000	0.993710000	Link
CVE-2024-28995	0.969950000	0.998560000	Link
CVE-2024-28987	0.965400000	0.997460000	Link
CVE-2024-27348	0.960910000	0.996530000	Link
CVE-2024-27198	0.970470000	0.998740000	Link
CVE-2024-24919	0.963920000	0.997120000	Link
CVE-2024-23897	0.973580000	0.999570000	Link
CVE-2024-2389	0.908530000	0.991420000	Link
CVE-2024-23692	0.964810000	0.997340000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-21893	0.956970000	0.995880000	Link
CVE-2024-21887	0.973690000	0.999600000	Link
CVE-2024-20767	0.964870000	0.997350000	Link
CVE-2024-1709	0.957060000	0.995890000	Link
CVE-2024-1212	0.946600000	0.994570000	Link
CVE-2024-0986	0.954890000	0.995590000	Link
CVE-2024-0195	0.962680000	0.996880000	Link
CVE-2024-0012	0.970250000	0.998640000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 28 Feb 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](#)

—

Fri, 28 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](#)

—

Fri, 28 Feb 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](#)

—

Fri, 28 Feb 2025

[NEU] [hoch] Infoblox NIOS: Mehrere Schwachstellen

Ein Angreifer kann diese Schwachstellen ausnutzen, um beliebigen Code auszuführen, sich erhöhte Rechte zu verschaffen und Daten zu manipulieren.

- [Link](#)

—

Fri, 28 Feb 2025

[NEU] [hoch] Linux Kernel: Mehrere Schwachstellen

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

- [Link](#)

—

Fri, 28 Feb 2025

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

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

- [Link](#)

—

Fri, 28 Feb 2025

[NEU] [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](#)

—

Fri, 28 Feb 2025

[NEU] [hoch] IBM MQ: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in IBM MQ und der MQ Console ausnutzen, um Informationen offenzulegen, einen Denial of Service auszulösen oder beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 28 Feb 2025

[NEU] [hoch] DrayTek Vigor: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in DrayTek Vigor ausnutzen, um vertrauliche Informationen preiszugeben, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand auszulösen und beliebigen Code auszuführen.

- [Link](#)

—

Fri, 28 Feb 2025

[NEU] [hoch] Rancher: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentifzierter Angreifer kann mehrere Schwachstellen in Rancher ausnutzen, um Dateien zu manipulieren, administrative Rechte zu erlangen und einen Denial-of-Service-Zustand auszulösen.

- [Link](#)

—

Fri, 28 Feb 2025

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

Ein entfernter anonymer 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](#)

—

Fri, 28 Feb 2025

[UPDATE] [hoch] bzip2: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit den Rechten des Dienstes

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in bzip2 ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen.

- [Link](#)

—

Fri, 28 Feb 2025

[UPDATE] [hoch] zlib: Schwachstelle ermöglicht nicht spezifizierten Angriff

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in zlib ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Fri, 28 Feb 2025

[UPDATE] [hoch] IBM Informix: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in IBM Informix ausnutzen, um beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Fri, 28 Feb 2025

[UPDATE] [hoch] GNU Emacs: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in GNU Emacs ausnutzen, um beliebigen Programmcode auszuführen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Fri, 28 Feb 2025

[UPDATE] [hoch] less: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in less ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 28 Feb 2025

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

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

- [Link](#)

—

Fri, 28 Feb 2025

[UPDATE] [hoch] Apache Camel und mehrere Red Hat Produkte: Mehrere Schwachstellen

Ein entfernter anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Apache Camel und in mehreren Red Hat-Produkten ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen preiszugeben und beliebigen Code auszuführen.

- [Link](#)

—

Fri, 28 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](#)

—

Fri, 28 Feb 2025

[UPDATE] [hoch] Apache Tomcat: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache Tomcat ausnutzen, um beliebigen Programmcode auszuführen und einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/1/2025	[Amazon Linux 2 : firefox (ALASFIREFOX-2025-035)]	critical
3/1/2025	[SUSE SLES15 / openSUSE 15 Security Update : azure-cli (SUSE-SU-2025:0751-1)]	critical
3/1/2025	[Fedora 41 : xen (2025-20f63c4273)]	critical
3/1/2025	[Debian dla-4075 : ata-modules-5.10.0-29-armmp-di - security update]	critical
2/28/2025	[Mattermost Server 9.11.x < 9.11.8 / 10.2.x < 10.2.3 / 10.3.x < 10.3.3 / 10.4.x < 10.4.2 (MMSA-2025-00430)]	critical
2/28/2025	[Ubuntu 24.04 LTS : Linux kernel vulnerabilities (USN-7310-1)]	critical
2/28/2025	[Ubuntu 22.04 LTS / 24.04 LTS : Linux kernel vulnerabilities (USN-7311-1)]	critical
3/1/2025	[Oracle Linux 9 : emacs (ELSA-2025-1915)]	high
3/1/2025	[Amazon Linux 2023 : bpftool, kernel, kernel-devel (ALAS2023-2025-802)]	high
3/1/2025	[Fedora 41 : xorg-x11-server (2025-b40b12a89e)]	high
3/1/2025	[Fedora 40 : cutter-re / rizin (2025-6f77f6c77a)]	high
3/1/2025	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : libX11 (SUSE-SU-2025:0739-1)]	high
3/1/2025	[openSUSE 15 Security Update : postgresql13 (SUSE-SU-2025:0737-1)]	high
3/1/2025	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : libxml2 (SUSE-SU-2025:0746-1)]	high
3/1/2025	[SUSE SLES15 Security Update : libX11 (SUSE-SU-2025:0757-1)]	high
3/1/2025	[SUSE SLES15 / openSUSE 15 Security Update : openvswitch3 (SUSE-SU-2025:0742-1)]	high
3/1/2025	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : tiff (SUSE-SU-2025:0753-1)]	high

Datum	Schwachstelle	Bewertung
3/1/2025	[SUSE SLES12 Security Update : libxml2 (SUSE-SU-2025:0747-1)]	high
3/1/2025	[SUSE SLES15 Security Update : ovmf (SUSE-SU-2025:0752-1)]	high
3/1/2025	[Fedora 41 : chromium (2025-25ab311510)]	high
3/1/2025	[Fedora 40 : webkitgtk (2025-57805565ad)]	high
3/1/2025	[Fedora 41 : wireshark (2025-08e73d463e)]	high
3/1/2025	[Fedora 40 : wireshark (2025-04475838f9)]	high
3/1/2025	[Fedora 40 : chromium (2025-eeba8bf9d8)]	high
3/1/2025	[Fedora 41 : nodejs22 (2025-e97e5c6ce3)]	high
3/1/2025	[Fedora 41 : cutter-re / rizin (2025-1290a47fff)]	high
3/1/2025	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : libxkbfile (SUSE-SU-2025:0758-1)]	high
3/1/2025	[SUSE SLES12 Security Update : libX11 (SUSE-SU-2025:0740-1)]	high
3/1/2025	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : wireshark (SUSE-SU-2025:0754-1)]	high
3/1/2025	[SUSE SLES15 Security Update : libxml2 (SUSE-SU-2025:0748-1)]	high
3/1/2025	[openSUSE 15 Security Update : u-boot (SUSE-SU-2025:0755-1)]	high
3/1/2025	[RHEL 8 / 9 : Red Hat Ansible Automation Platform 2.5 Product Security and Bug Fix Update (Important) (RHSA-2025:1954)]	high
3/1/2025	[Debian dla-4076 : linux-config-6.1 - security update]	high
2/28/2025	[Cisco Nexus 3000 9000 Series Switches Health Monitoring Diagnostics DoS (cisco-sa-n3kn9k-healthdos-eOqSWK4g)]	high
2/28/2025	[Debian dsa-5872 : xnest - security update]	high
2/28/2025	[Debian dla-4072 : xdmx - security update]	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
-------	-------	------	-------------

6 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-01	[germancentre.sg]	incransom	Link
2025-03-01	[breakawayconcretecutting.com]	incransom	Link
2025-03-01	[JEFFREYCOURT.COM]	clon	Link
2025-03-01	[APTEAN.COM]	clon	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.