

Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250205



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 Private video	12
5 Cyberangriffe: (Feb)	13
6 Ransomware-Erpressungen: (Feb)	13
7 Quellen	13
7.1 Quellenverzeichnis	13
8 Impressum	14

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

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](#)

—

Schadcode-Schlupfloch in Dell NetWorker geschlossen

Angreifer können an mehreren Sicherheitslücken in Dells Backuplösung NetWorker ansetzen. Sicherheitsupdates stehen zum Download bereit.

- [Link](#)

Zoho ManageEngine Applications Manager: Sicherheitslücke verschafft Admin-Rechte

Zohocorp warnt vor einer Schwachstelle in ManageEngine Applications Manager. Angreifer können sich Admin-Rechte verschaffen.

- [Link](#)

VMware Aria Operations: Angreifer können Zugangsdaten auslesen

Broadcom warnt vor Sicherheitslücken in VMware Aria Operations, durch die Angreifer etwa Zugangsdaten ausspähen können. Updates stehen bereit.

- [Link](#)

Warten auf Patch: Das Admin-Interface Voyager für Laravel-Apps ist verwundbar

Sicherheitsforscher warnen vor möglichen Attacken auf Voyager. Bislang haben sich die Entwickler zu den Sicherheitslücken nicht geäußert.

- [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	0.994110000	Link
CVE-2024-9463	0.961860000	0.996660000	Link
CVE-2024-8963	0.967990000	0.998000000	Link
CVE-2024-7593	0.971650000	0.999000000	Link
CVE-2024-6893	0.938390000	0.993630000	Link
CVE-2024-6670	0.910490000	0.991370000	Link
CVE-2024-5910	0.962890000	0.996890000	Link
CVE-2024-55956	0.967520000	0.997860000	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	0.996110000	Link
CVE-2024-4358	0.925270000	0.992430000	Link
CVE-2024-41713	0.954370000	0.995450000	Link
CVE-2024-40711	0.963400000	0.996990000	Link
CVE-2024-4040	0.969020000	0.998290000	Link
CVE-2024-38856	0.942880000	0.994080000	Link
CVE-2024-36401	0.952840000	0.995220000	Link
CVE-2024-3400	0.964000000	0.997100000	Link
CVE-2024-3273	0.937410000	0.993530000	Link
CVE-2024-32113	0.914790000	0.991650000	Link
CVE-2024-28995	0.965000000	0.997300000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-28987	0.961930000	0.996670000	Link
CVE-2024-27348	0.960260000	0.996380000	Link
CVE-2024-27198	0.968000000	0.998000000	Link
CVE-2024-24919	0.959630000	0.996270000	Link
CVE-2024-23897	0.973540000	0.999550000	Link
CVE-2024-23692	0.964470000	0.997200000	Link
CVE-2024-21893	0.957440000	0.995930000	Link
CVE-2024-21887	0.973220000	0.999480000	Link
CVE-2024-20767	0.966770000	0.997730000	Link
CVE-2024-1709	0.957220000	0.995880000	Link
CVE-2024-1212	0.937140000	0.993490000	Link
CVE-2024-0986	0.955530000	0.995640000	Link
CVE-2024-0195	0.962680000	0.996840000	Link
CVE-2024-0012	0.969980000	0.998520000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 04 Feb 2025

[UPDATE] [hoch] libxml2: Schwachstelle ermöglicht remote Code Execution

Ein lokaler Angreifer kann eine Schwachstelle in libxml2 ausnutzen, um einen Code auszuführen.

- [Link](#)

—

Tue, 04 Feb 2025

[NEU] [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](#)

—

Tue, 04 Feb 2025

[NEU] [hoch] Google Android: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen,, um seine Privilegien zu erweitern, einen Denial-of-Service-Zustand zu erzeugen oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Tue, 04 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](#)

—

Tue, 04 Feb 2025

[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um Informationen offenzulegen, beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Tue, 04 Feb 2025

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Tue, 04 Feb 2025

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Tue, 04 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](#)

—

Tue, 04 Feb 2025

[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, Daten zu manipulieren oder vertrauliche Informationen preiszugeben.

- [Link](#)

—

Tue, 04 Feb 2025

[UPDATE] [kritisch] Apache Struts: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache Struts ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Tue, 04 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](#)

—

Tue, 04 Feb 2025

[UPDATE] [hoch] Red Hat Enterprise Linux (Advanced Cluster Management): Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux Advanced Cluster Management ausnutzen, um Sicherheitsmaßnahmen zu umgehen und einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Mon, 03 Feb 2025

[UPDATE] [hoch] Splunk Enterprise: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Splunk Enterprise ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, um Code auszuführen und um nicht näher spezifizierte Auswirkungen zu erzielen.

- [Link](#)

—

Mon, 03 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](#)

—

Mon, 03 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](#)

—

Mon, 03 Feb 2025

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

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

- [Link](#)

—

Mon, 03 Feb 2025

[UPDATE] [hoch] Dovecot: Mehrere Schwachstellen

Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in Dovecot ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Mon, 03 Feb 2025

[UPDATE] [hoch] Apache Maven: Schwachstelle ermöglicht Manipulation von Dateien oder Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache Maven ausnutzen, um Dateien zu manipulieren oder Informationen offenzulegen.

- [Link](#)

—

Mon, 03 Feb 2025

[UPDATE] [hoch] SonicWall SonicOS: Mehrere Schwachstellen

Ein lokaler oder entfernter anonymer Angreifer kann diese Schwachstellen ausnutzen, um Root-Rechte zu erlangen, beliebigen Code auszuführen, vertrauliche Informationen preiszugeben, die Authentifizierung zu umgehen oder einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Mon, 03 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](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/3/2025	[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.10 : Netdata vulnerabilities (USN-7250-1)]	critical
2/3/2025	[SUSE SLES15 / openSUSE 15 Security Update : google-osconfig-agent (SUSE-SU-2025:0302-1)]	critical
2/3/2025	[Fedora 41 : buku (2025-e035838041)]	high
2/3/2025	[Fedora 40 : buku (2025-df3432c3ee)]	high
2/3/2025	[SUSE SLES12 Security Update : libxml2 (SUSE-SU-2025:0300-1)]	high
2/3/2025	[SUSE SLES15 / openSUSE 15 Security Update : buildah (SUSE-SU-2025:0301-1)]	high
2/3/2025	[SUSE SLES15 / openSUSE 15 Security Update : iperf (SUSE-SU-2025:0291-1)]	high
2/3/2025	[Cisco IOS XR Software Network Convergence System DoS (cisco-sa-l2services-2mvHdNuC)]	high
2/3/2025	[Ubuntu 16.04 LTS / 18.04 LTS : libndp vulnerability (USN-7248-1)]	high
2/3/2025	[openSUSE 15 Security Update : SDL2_sound (openSUSE-SU-2025:0037-1)]	high

Datum	Schwachstelle	Bewertung
2/3/2025	[CentOS 9 : kernel-5.14.0-559.el9]	high
2/3/2025	[SUSE SLES15 / openSUSE 15 Security Update : libxml2 (SUSE-SU-2025:0303-1)]	high
2/3/2025	[openSUSE 15 Security Update : stb (openSUSE-SU-2025:0039-1)]	high
2/3/2025	[openSUSE 15 Security Update : chromium (openSUSE-SU-2025:0036-1)]	high
2/3/2025	[Ubuntu 20.04 LTS / 22.04 LTS : HarfBuzz vulnerability (USN-7251-1)]	high
2/3/2025	[SUSE SLES15 Security Update : buildah (SUSE-SU-2025:0320-1)]	high
2/3/2025	[SUSE SLES15 / openSUSE 15 Security Update : ignition (SUSE-SU-2025:0299-1)]	high
2/3/2025	[SUSE SLES15 / openSUSE 15 Security Update : apptainer (SUSE-SU-2025:0313-1)]	high
2/3/2025	[SUSE SLES15 Security Update : kernel (SUSE-SU-2025:0289-1)]	high
2/3/2025	[SUSE SLES15 / openSUSE 15 Security Update : govulncheck-vulndb (SUSE-SU-2025:0297-1)]	high
2/3/2025	[Ubuntu 16.04 LTS : Linux kernel (Azure) vulnerabilities (USN-7233-3)]	high
2/3/2025	[SUSE SLES15 Security Update : buildah (SUSE-SU-2025:0319-1)]	high
2/3/2025	[RHEL 8 : rsync (RHSA-2025:0884)]	high
2/3/2025	[RHEL 9 : tuned (RHSA-2025:0879)]	high
2/3/2025	[RHEL 9 : libsoup (RHSA-2025:0882)]	high
2/3/2025	[RHEL 8 : libsoup (RHSA-2025:0889)]	high
2/3/2025	[RHEL 8 : tuned (RHSA-2025:0880)]	high
2/3/2025	[RHEL 8 : libsoup (RHSA-2025:0903)]	high
2/3/2025	[RHEL 8 : rsync (RHSA-2025:0885)]	high

4 Die Hacks der Woche

mit Martin Haunschmid

4.0.1 Private video

Vorschaubild [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

6 Ransomware-Erpressungen: (Feb)

Datum	Opfer	Ransomware-Gruppe	Webseite
-------	-------	-------------------	----------

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.