

Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250529



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)	9
3.3 Sicherheitslücken Meldungen von Tenable	12
4 Die Hacks der Woche	14
4.0.1 Information Stealer. Wie funktionieren sie?	15
5 Cyberangriffe: (Mai)	16
6 Quellen	17
6.1 Quellenverzeichnis	17
7 Impressum	18

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

Warten auf Sicherheitsupdate: Versa Concerto ist schwer verwundet

Lücken bedrohen die Orchestrierungsplattform Versa Concerto. Schadcode-Attacken sind möglich. Medienberichten zufolge gibt es Updates. Der Hersteller schweigt.

- [Link](#)

—

Sicherheitsupdates Cisco: Angreifer können sich höhere Rechte erschleichen

Wichtige Updates schließen mehrere Schwachstellen in unter anderem Cisco Networks Analytics Manager und Webex Meetings Services.

- [Link](#)

—

Angreifer können mit VMware erstellte virtuelle Maschinen crashen

Broadcom hat wichtige Sicherheitsupdates für VMware ESXi, vCenter Server, Workstation und Fusion veröffentlicht.

- [Link](#)

—

Authentifizierung: Kritische Lücke in Samlify macht Angreifer zu Admins

Ein Sicherheitsupdate schließt eine Schwachstelle in der SAML-Bibliothek Samlify. Attacken sollen vergleichsweise einfach sein.

- [Link](#)

—

Mehrere Sicherheitslücken bedrohen VMware Cloud Foundation

Die Cloudlösung VMware Cloud Foundation ist verwundbar. Angreifer können unberechtigt auf Daten und Services zugreifen.

- [Link](#)

—

HCL-Domino-Add-on Leap gegen mögliche Attacken abgesichert

Das Anwendungsentwicklungssystem HCL Domino ist über Schwachstellen im Add-on Leap attackierbar.

- [Link](#)

—

Firefox: Mozilla schließt Sicherheitslücken aus Pwn2Own-Hacker-Wettbewerb

Der Webbrowser Firefox ist in verschiedenen Ausgaben verwundbar. Die Entdecker der Lücken kassierten 100.000 US-Dollar Prämie.

- [Link](#)

Angreifer können Verbindungen von Sonicwall SMA1000 manipulieren

Die Fernzugriffslösung Secure Mobile Access (SMA) der 1000er-Serie von Sonicwall ist verwundbar.

- [Link](#)

Sicherheitspatches Palo Alto: Firewalls mit PAN-OS sind verwundbar

Das IT-Sicherheitsunternehmen Palo Alto Networks schließt mehrere Lücken in unter anderem PAN-OS und Prisma Access Browser.

- [Link](#)

Warnung vor Angriffen auf neue SAP-Netweaver-Lücke, Chrome und Draytek-Router

Die US-amerikanische IT-Sicherheitsbehörde CISA warnt vor Angriffen auf eine neue SAP-Netweaver-Lücke sowie auf Chrome und Draytek-Router.

- [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-2025-3248	0.926020000	0.997270000	Link
CVE-2025-29927	0.931560000	0.997810000	Link
CVE-2025-24893	0.921650000	0.996900000	Link
CVE-2025-24813	0.936280000	0.998270000	Link
CVE-2025-0282	0.923560000	0.997080000	Link
CVE-2025-0108	0.940390000	0.998830000	Link
CVE-2024-9989	0.911880000	0.996200000	Link
CVE-2024-9935	0.928150000	0.997460000	Link
CVE-2024-9474	0.942830000	0.999270000	Link
CVE-2024-9465	0.942440000	0.999180000	Link
CVE-2024-9463	0.942640000	0.999240000	Link
CVE-2024-9264	0.920720000	0.996820000	Link
CVE-2024-9234	0.925020000	0.997190000	Link
CVE-2024-9047	0.926090000	0.997270000	Link
CVE-2024-9014	0.923220000	0.997030000	Link
CVE-2024-8963	0.943250000	0.999390000	Link
CVE-2024-8856	0.919220000	0.996700000	Link
CVE-2024-8504	0.923140000	0.997010000	Link
CVE-2024-8503	0.930440000	0.997690000	Link
CVE-2024-8190	0.928890000	0.997550000	Link
CVE-2024-7954	0.937810000	0.998470000	Link
CVE-2024-7928	0.915540000	0.996420000	Link
CVE-2024-7593	0.943990000	0.999670000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-7120	0.915170000	0.996390000	Link
CVE-2024-6911	0.927560000	0.997410000	Link
CVE-2024-6782	0.936240000	0.998270000	Link
CVE-2024-6781	0.934260000	0.998060000	Link
CVE-2024-6670	0.944670000	0.999930000	Link
CVE-2024-6646	0.921240000	0.996870000	Link
CVE-2024-5932	0.941040000	0.998940000	Link
CVE-2024-5910	0.908210000	0.995980000	Link
CVE-2024-5806	0.907610000	0.995930000	Link
CVE-2024-57727	0.935860000	0.998240000	Link
CVE-2024-56145	0.930390000	0.997680000	Link
CVE-2024-55956	0.921000000	0.996860000	Link
CVE-2024-55591	0.940360000	0.998820000	Link
CVE-2024-53704	0.934710000	0.998120000	Link
CVE-2024-53677	0.918050000	0.996610000	Link
CVE-2024-5217	0.941960000	0.999090000	Link
CVE-2024-51567	0.942610000	0.999230000	Link
CVE-2024-51378	0.939560000	0.998690000	Link
CVE-2024-5084	0.907680000	0.995930000	Link
CVE-2024-50623	0.939920000	0.998740000	Link
CVE-2024-50603	0.943350000	0.999420000	Link
CVE-2024-50498	0.924360000	0.997140000	Link
CVE-2024-4956	0.939760000	0.998710000	Link
CVE-2024-48914	0.909810000	0.996070000	Link
CVE-2024-4885	0.942780000	0.999260000	Link
CVE-2024-4879	0.943360000	0.999420000	Link
CVE-2024-48307	0.926310000	0.997310000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-48248	0.935290000	0.998180000	Link
CVE-2024-47575	0.912740000	0.996230000	Link
CVE-2024-47176	0.916890000	0.996510000	Link
CVE-2024-46938	0.919470000	0.996730000	Link
CVE-2024-4577	0.943760000	0.999560000	Link
CVE-2024-45519	0.941500000	0.999010000	Link
CVE-2024-45388	0.915030000	0.996380000	Link
CVE-2024-45216	0.939010000	0.998620000	Link
CVE-2024-45195	0.940810000	0.998900000	Link
CVE-2024-4443	0.933810000	0.998000000	Link
CVE-2024-44000	0.920120000	0.996770000	Link
CVE-2024-4358	0.942540000	0.999210000	Link
CVE-2024-43451	0.910720000	0.996110000	Link
CVE-2024-42640	0.907720000	0.995940000	Link
CVE-2024-4257	0.922930000	0.997000000	Link
CVE-2024-41713	0.939140000	0.998630000	Link
CVE-2024-41107	0.931620000	0.997820000	Link
CVE-2024-4040	0.944120000	0.999730000	Link
CVE-2024-40348	0.916690000	0.996490000	Link
CVE-2024-39914	0.926650000	0.997330000	Link
CVE-2024-38856	0.943660000	0.999530000	Link
CVE-2024-38816	0.927560000	0.997410000	Link
CVE-2024-38475	0.924010000	0.997100000	Link
CVE-2024-38112	0.913840000	0.996300000	Link
CVE-2024-37032	0.919920000	0.996760000	Link
CVE-2024-36991	0.907880000	0.995950000	Link
CVE-2024-36412	0.938060000	0.998500000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-36401	0.944180000	0.999760000	Link
CVE-2024-36104	0.938050000	0.998500000	Link
CVE-2024-3552	0.932020000	0.997860000	Link
CVE-2024-3495	0.932990000	0.997940000	Link
CVE-2024-34470	0.932220000	0.997890000	Link
CVE-2024-34102	0.941360000	0.998970000	Link
CVE-2024-3400	0.943450000	0.999450000	Link
CVE-2024-3273	0.944050000	0.999690000	Link
CVE-2024-3272	0.934330000	0.998070000	Link
CVE-2024-32651	0.913070000	0.996240000	Link
CVE-2024-32113	0.934460000	0.998080000	Link
CVE-2024-31982	0.941580000	0.999020000	Link
CVE-2024-31849	0.904420000	0.995730000	Link
CVE-2024-31848	0.928750000	0.997530000	Link
CVE-2024-31750	0.924280000	0.997130000	Link
CVE-2024-3116	0.906820000	0.995890000	Link
CVE-2024-30269	0.917990000	0.996610000	Link
CVE-2024-30255	0.918430000	0.996650000	Link
CVE-2024-29973	0.936960000	0.998350000	Link
CVE-2024-29972	0.915290000	0.996400000	Link
CVE-2024-29895	0.927360000	0.997390000	Link
CVE-2024-29824	0.943410000	0.999430000	Link
CVE-2024-2961	0.923580000	0.997090000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 26 May 2025

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um Sicherheitsvorkehrungen zu umgehen, einen Denial-of-Service auszulösen, Dateien zu manipulieren oder Informationen offenzulegen.

- [Link](#)

—

Mon, 26 May 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

—

Mon, 26 May 2025

[NEU] [UNGEPATCHT] [kritisch] Microsoft Windows Server 2025: Schwachstelle ermöglicht Privilegieneskalation

Ein Angreifer kann eine Schwachstelle in Microsoft Windows Server 2025 ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Mon, 26 May 2025

[UPDATE] [hoch] Mozilla Firefox / Thunderbird: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox / Thunderbird ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial-of-Service auszuführen.

- [Link](#)

—

Mon, 26 May 2025

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PHP ausnutzen, um vertrauliche Informationen preiszugeben, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu erzeugen und einen Spoofing-Angriff durchzuführen.

- [Link](#)

—

Mon, 26 May 2025

[UPDATE] [kritisch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programmcode auszuführen, Informationen preiszugeben und andere nicht spezifizierte Angriffe durchzuführen.

- [Link](#)

—

Mon, 26 May 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service Angriff durchzuführen, seine Privilegien eskalieren oder einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Mon, 26 May 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um einen Denial of Service Angriff und weitere nicht spezifizierte Angriffe durchzuführen.

- [Link](#)

—

Mon, 26 May 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 oder einen unspezifischen Angriff durchzuführen.

- [Link](#)

—

Mon, 26 May 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

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

- [Link](#)

—

Mon, 26 May 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

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

- [Link](#)

—

Mon, 26 May 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um nicht spezifizierte Auswirkungen zu erzeugen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Mon, 26 May 2025

[UPDATE] [hoch] VMware Aria Operations, VMware Aria Operations for Logs und VMware Cloud Foundation:: Mehrere Schwachstellen

Ein entfernter authentisierter Angreifer kann mehrere Schwachstellen in VMware Aria Operations for Logs, VMware Aria Operations und VMware Cloud Foundation ausnutzen, um Informationen preiszugeben, erhöhte Berechtigungen zu erlangen und einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

—

Mon, 26 May 2025

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

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

- [Link](#)

—

Mon, 26 May 2025

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen preiszugeben, einen Denial-of-Service-Zustand herbeizuführen oder nicht näher spezifizierte Angriffe zu starten.

- [Link](#)

—

Fri, 23 May 2025

[NEU] [hoch] Microsoft Edge: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle in Microsoft Edge ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Fri, 23 May 2025

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

Ein Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service Zustand herbeizuführen und um nicht näher beschriebene Auswirkungen zu verursachen.

- [Link](#)

—

Fri, 23 May 2025

[UPDATE] [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, 23 May 2025

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglichen nicht spezifizierten Angriff

Ein lokaler Angreifer kann eine Schwachstelle im Linux-Kernel ausnutzen, um einen nicht näher spezifizierten Angriff zu starten.

- [Link](#)

—

Fri, 23 May 2025

[UPDATE] [hoch] Checkmk: Mehrere Schwachstellen

Ein entfernter authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Checkmk ausnutzen, um Dateien zu manipulieren und vertrauliche Informationen preiszugeben.

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
5/23/2025	[Oracle Linux 9 : nginx (ELSA-2025-7402)]	critical
5/23/2025	[Oracle Linux 9 : ghostscript (ELSA-2025-7586)]	critical
5/23/2025	[Fortinet FortiVoice Stack-based Buffer Overflow (FG-IR-25-254)]	critical
5/23/2025	[Oracle Linux 9 : php:8.3 (ELSA-2025-7418)]	critical
5/25/2025	[Fedora 41 : dotnet8.0 (2025-d62bbb5261)]	high
5/25/2025	[Photon OS 3.0: Runc PHSA-2022-3.0-0405]	high
5/24/2025	[Oracle Linux 9 : redis (ELSA-2025-7438)]	high
5/24/2025	[Fedora 41 : thunderbird (2025-ee55907675)]	high

Datum	Schwachstelle	Bewertung
5/24/2025	[SUSE SLES15 Security Update : kernel (Live Patch 17 for SLE 15 SP5) (SUSE-SU-2025:01692-1)]	high
5/24/2025	[SUSE SLES15 Security Update : kernel (Live Patch 4 for SLE 15 SP6) (SUSE-SU-2025:01682-1)]	high
5/24/2025	[SUSE SLES12 Security Update : python-setuptools (SUSE-SU-2025:01695-1)]	high
5/24/2025	[SUSE SLES15 Security Update : kernel (Live Patch 13 for SLE 15 SP5) (SUSE-SU-2025:01676-1)]	high
5/24/2025	[SUSE SLED15 / SLES15 Security Update : python-tornado6 (SUSE-SU-2025:01649-2)]	high
5/24/2025	[SUSE SLES12 Security Update : python36-setuptools (SUSE-SU-2025:01693-1)]	high
5/24/2025	[SUSE SLES15 Security Update : kernel (Live Patch 3 for SLE 15 SP6) (SUSE-SU-2025:01683-1)]	high
5/24/2025	[SUSE SLES15 Security Update : kernel (Live Patch 20 for SLE 15 SP5) (SUSE-SU-2025:01677-1)]	high
5/23/2025	[Oracle Linux 9 : gvisor-tap-vsock (ELSA-2025-7416)]	high
5/23/2025	[Oracle Linux 9 : kernel (ELSA-2025-7903)]	high
5/23/2025	[Oracle Linux 9 : firefox (ELSA-2025-8049)]	high
5/23/2025	[Oracle Linux 9 : gimp (ELSA-2025-7417)]	high
5/23/2025	[Atlassian Confluence 7.13.x < 8.5.22 / 8.6.x < 9.2.4 / 9.3.x < 9.4.1 (CONFSERVER-99686)]	high
5/23/2025	[SOLIDWORKS eDrawings 2025 <= 2025 SP1.2 Multiple Vulnerabilities]	high
5/23/2025	[SonicWall SMA 1000 Series < 12.4.3-02963 SSRF (SNWLID-2025-0010)]	high
5/23/2025	[Atlassian Jira Service Management Data Center and Server 5.11.3 < 5.12.20 / < 5.12.22 / 5.13.x < 10.3.5 / 10.4.x < 10.6.0 (JSDSERVER-16207)]	high
5/23/2025	[Atlassian Confluence 2.2.x < 8.5.21 / 8.6.x < 9.2.2 / 9.3.x < 9.3.2 (CONFSERVER-99568)]	high

Datum	Schwachstelle	Bewertung
5/23/2025	[Python Library Tornado 6.5.0 DoS]	high
5/23/2025	[BeyondTrust Privilege Management for Windows < 25.2 Privilege Escalation (BT25-01)]	high
5/23/2025	[Oracle Linux 9 : nodejs:22 (ELSA-2025-7433)]	high
5/23/2025	[Oracle Linux 9 : redis:7 (ELSA-2025-7429)]	high

4 Die Hacks der Woche

mit Martin Haunschmid

4.0.1 Information Stealer. Wie funktionieren sie?



[Zum Youtube Video](#)

5 Cyberangriffe: (Mai)

Datum	Opfer	Land	Information
2025-05-24	Arcona-Hotels	[DEU]	Link
2025-05-22	Landratsamt Bodenseekreis	[DEU]	Link
2025-05-22	Choksi Laboratories Limited	[IND]	Link
2025-05-20	Département des Hauts-de-Seine	[FRA]	Link
2025-05-20	Kettering Health	[USA]	Link
2025-05-19	Maison d'Accueil les Quatre Vents - Nivelles	[BEL]	Link
2025-05-18	La Maison Liégeoise	[BEL]	Link
2025-05-18	MathWorks	[USA]	Link
2025-05-15	Arla Foods	[DEU]	Link
2025-05-15	Peter Green Chilled	[GBR]	Link
2025-05-14	Central Point School District 6	[USA]	Link
2025-05-14	Morgan County 911	[USA]	Link
2025-05-14	Cellcom	[USA]	Link
2025-05-13	Nucor Corporation	[USA]	Link
2025-05-12	Drogarias Globo	[BRA]	Link
2025-05-10	Alabama	[USA]	Link
2025-05-09	Hessischen Apothekerverband	[DEU]	Link
2025-05-09	Tiffany & Co.	[KOR]	Link
2025-05-08	Roma Tre	[ITA]	Link
2025-05-07	Uttar Haryana Bijli Vitran Nigam Limited (UHBVNL)	[IND]	Link
2025-05-06	West Lothian Council	[GBR]	Link
2025-05-06	Terre d'Oc	[FRA]	Link
2025-05-05	Global Crossing Airlines Group Inc.	[USA]	Link
2025-05-04	South African Airways	[ZAF]	Link
2025-05-04	Promosfera	[ITA]	Link

Datum	Opfer	Land	Information
2025-05-03	Coweta County School System	[USA]	Link
2025-05-02	Outwood Academy Acklam	[GBR]	Link
2025-05-01	Harrods	[GBR]	Link
2025-05-01	Framlingham College	[GBR]	Link
2025-05-01	Legal Aid Agency	[GBR]	Link
2025-05-01	Breton S.p.A.	[ITA]	Link

6 Quellen

6.1 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>

7 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.