CISO Sprechstunde

07.05.2025

Aktuelles aus der FAU

Einbruch im Sprachenzentrum

4 Laptops wurden gestohlen

Risikomanagement:

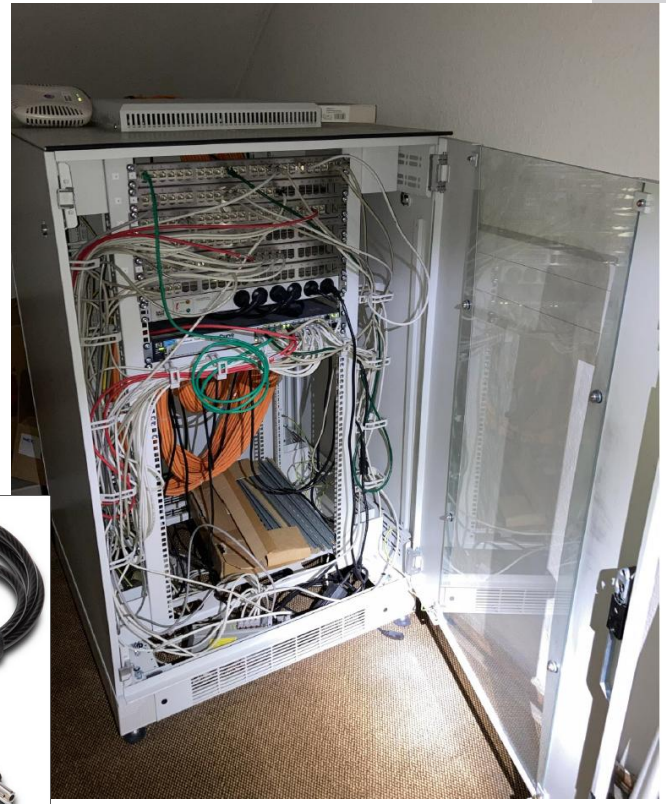
Datenverlust

➔ Festplattenverschlüsselung mit PIN

➔ backup, backup, backup

Geräteverlust

➔ Mobile Geräte bitte immer wegschließen oder Kensington Schloss (4,95 €) verwenden



Aktuelles

Betrug

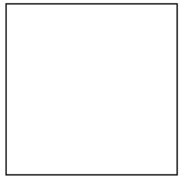
Shopping im Namen der FAU

Von: [redacted]@haushalt-fau.de>
Gesendet: Mittwoch, 16. April 2025 14:57
An: info@dualoptik.de
Betreff: Lieferzeit der Ware

Guten Tag. Im Rahmen des Programms, neue Mitarbeiter mit Ausrüstung zu versorgen und die Startausrüstung im Jahr 2025 zu aktualisieren, kauft unser Institut verschiedene Waren an.
In diesem Zusammenhang möchte ich wissen, ob Sie auf Lager sind und wie lange die Lieferung des nächsten Artikels dauern wird:

DJI Matrice 4T Wärmebild-Drohne

Mit freundlichen Grüßen



[redacted], Organisation: Abteilung H - Haushalt
Abteilung: Referat H6 - Zentrale Auftragsvergabe

Freyeslebenstraße 1 91058 Erlangen
Telefon: +49 9181 85-26701
Telefax: +49 9181 85-25913

Email: [redacted]@haushalt-fau.de
URL: http://www.fau.de

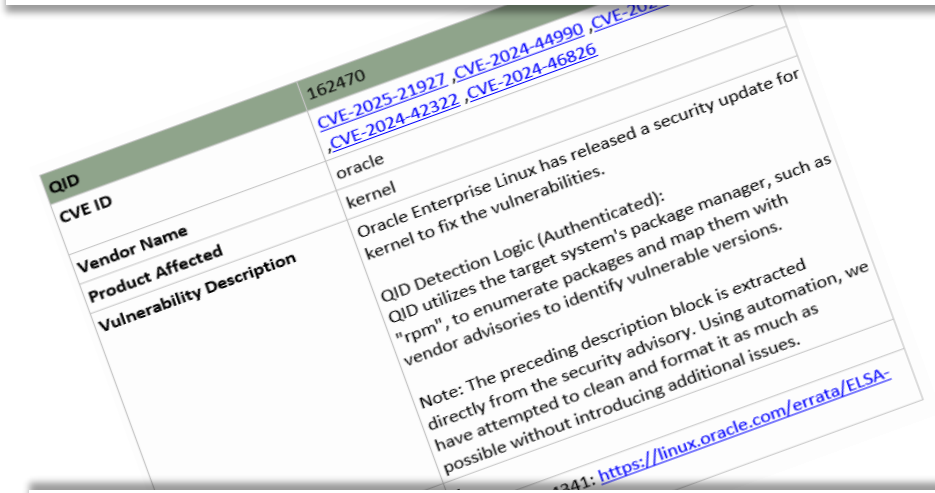
Aktuelles aus der Welt

Aktuelles

Finanzierung MITRE Corporation und CVEs

US-Kürzungen: CVE-Liste könnte sofort stoppen

Die CVE-Liste ist zentral für koordinierte Maßnahmen gegen gefährliche Bugs. Die US-Regierung entzieht die Finanzierung. Per sofort.



QID	162470
CVE ID	CVE-2025-21927 ,CVE-2024-44990 ,CVE-2024-42322 ,CVE-2024-46826
Vendor Name	oracle
Product Affected	kernel
Vulnerability Description	Oracle Enterprise Linux has released a security update for kernel to fix the vulnerabilities. QID Detection Logic (Authenticated): QID utilizes the target system's package manager, such as "rpm", to enumerate packages and map them with vendor advisories to identify vulnerable versions. Note: The preceding description block is extracted directly from the security advisory. Using automation, we have attempted to clean and format it as much as possible without introducing additional issues. ...241: https://linux.oracle.com/errata/ELSA-

CVE-Aus abgewendet, Schwachstellendatenbank der EU geht an den Start

Entscheidung in letzter Minute - offenbar geht der Vertrag zwischen CISA und MITRE in die Verlängerung. Mehrere Initiativen präsentieren derweil Alternativen.

MITRE

16.04.25 02:16 Uhr heise.de

Die Mutter aller Schwachstellendatenbanken, die **Common Vulnerabilities and Exposures (CVEs)** der **MITRE Corporation**, könnte in den nächsten Stunden offline gehen. Denn die US-Regierung verlängert die Finanzierung nicht. CVE ist elementar für Kooperation im Bereich IT-Sicherheit. Dank CVE erhalten gemeldete Sicherheitslücken eine eindeutige Nummer, anhand der alle Beteiligten sicherstellen können, dass sie vom selben Problem sprechen.

CISA will Auswirkungen "mildern„, ist allerdings selbst von erheblichen Kürzungen und Chaos dank Elon Musks DOGE betroffen.

https://www.cisa.gov/

Friedrich-Alexander-Universität
Erlangen-Nürnberg

FAU

Ransomware

Welche Fehler sind zu vermeiden?

1. Ungepatchte Sicherheitslücken

Ziele von Cyberkriminellen:

- Weit verbreitete Systeme (z.B. Microsoft)
- Zu späte oder fehlende Patches (Zero-Day-Exploits)

Präventionsmaßnahmen:

- Monitoring
- Patch-Management
- Asset-Management
- Nicht patchbare Systeme isolieren

Foto von Bill Eccles auf Unsplash

Quelle: https://www.security-insider.de/10-typische-fehler-ransomware-angriffe-a-f4d609c5b29bea15014ddf1f1c279f85/?cmp=nl-ede617ce-bb32-418b-8967-bc79e3a81876&uuid=337D99CC-15A9-4E87-B643-1C288539C55F, abgerufen am 22.04.2025

2. Schwache Passwörter

Problematische Praktiken:

- Passwörter sind zu kurz
- zu einfach
- mehrfach verwendet

Präventionsmaßnahmen:

- Konsequente Passwortrichtlinie
- Multi-Faktor-Authentifizierung (MFA)

Foto von rc.xyz NFT gallery auf Unsplash

Quelle: https://www.security-insider.de/10-typische-fehler-ransomware-angriffe-a-f4d609c5b29bea15014ddf1f1c279f85/?cmp=nl-ede617ce-bb32-418b-8967-bc79e3a81876&uuid=337D99CC-15A9-4E87-B643-1C288539C55F, abgerufen am 22.04.2025

3. Mangelnde Account-Hygiene

Problematische Praktiken:

- Administratoren melden sich mit domänen-administrativen Rechten auf Arbeitsplatzrechnern an, wobei höchstprivilegierte Log-ins lokal zwischengespeichert werden
- Passwort-Hashes können so aus dem Arbeitsspeicher ausgelesen werden --> Angreifer nutzen kompromittierte lokale Administratorkonten

Präventionsmaßnahmen:

- Klare Account-Trennung
- Einsatz des Tiering-Modells:
  - Systeme in Sicherheitsstufen (Tiers) unterteilen
  - Für jede Stufe ein eigenes Administratorkonto verwenden
  - Schutz vor Kompromittierung „höherer“ Systeme durch „niedrigere“

Foto von John Cameron auf Unsplash

Quelle: https://www.security-insider.de/10-typische-fehler-ransomware-angriffe-a-f4d609c5b29bea15014ddf1f1c279f85/?cmp=nl-ede617ce-bb32-418b-8967-bc79e3a81876&uuid=337D99CC-15A9-4E87-B643-1C288539C55F, abgerufen am 22.04.2025

4. Fehlende Netzwerksegmentierung

Problematische Praktiken:

- Viele Unternehmen betreiben flache, unsegmentierte Netzwerke, in welchen sich Kriminelle einfach ausbreiten können.
- Gut gemacht: An der FAU gibt es viele Subnetze

Präventionsmaßnahmen z.B.:

- Trennung von Server- und Client-Netzwerken
- Trennung von Operational Technology (OT) und IT
- Separates Netzsegment für Management-Schnittstellen, auf das nur Admin-Accounts über ein VPN mit MFA Zugriff haben

Foto von John Cameron auf Unsplash

Quelle: https://www.security-insider.de/10-typische-fehler-ransomware-angriffe-a-f4d609c5b29bea15014ddf1f1c279f85/?cmp=nl-ede617ce-bb32-418b-8967-bc79e3a81876&uuid=337D99CC-15A9-4E87-B643-1C288539C55F, abgerufen am 22.04.2025

5. Unzureichende Backups

Problematische Praktiken:

- Fehlende Backup-Strategie
- Backups sind zu leicht zu finden und können so von Angreifern mitverschlüsselt werden

Präventionsmaßnahmen:

- Backups sollten vom normalen LAN und vom Internet isoliert sein
- Unterbringung in einem separaten Netzsegment
- Funktionsfähigkeit und Einspielen regelmäßig testen
- „3-2-1-Prinzip“: 3 Backup-Kopien auf 2 Medien, davon eine off-site verwahrt

Foto von John Cameron auf Unsplash

Quelle: https://www.security-insider.de/10-typische-fehler-ransomware-angriffe-a-f4d609c5b29bea15014ddf1f1c279f85/?cmp=nl-ede617ce-bb32-418b-8967-bc79e3a81876&uuid=337D99CC-15A9-4E87-B643-1C288539C55F, abgerufen am 22.04.2025

6. Überlastetes IT-Personal

Problematische Praktiken:

- Unterbesetzte IT-Abteilungen --> Sicherheit wird zur Nebensache

Präventionsmaßnahmen:

- Ausreichend viele und fachkundige Personen in der IT beschäftigen
- Dedizierte Fachkräfte für IT-Sicherheit (ISB)
- Wettbewerbsfähige Vergütung

Foto von Maximalfocus auf Unsplash

Quelle: https://www.security-insider.de/10-typische-fehler-ransomware-angriffe-a-f4d609c5b29bea15014ddf1f1c279f85/?cmp=nl-ede617ce-bb32-418b-8967-bc79e3a81876&uuid=337D99CC-15A9-4E87-B643-1C288539C55F, abgerufen am 22.04.2025

7. Probleme mit IT-Dienstleistern

Problematische Praktiken:

- Unzureichende Vertragsgestaltung und fehlende Kontrolle der IT-Dienstleister

Präventionsmaßnahmen:

- Klare Service-Level-Agreements mit definierten Reaktionszeiten
- 24/7 Erreichbarkeit vereinbaren
- Regelmäßige Überprüfung der Sicherheitsstrategie, einschließlich der Infrastruktur des Dienstleisters, z.B. durch Pen-Tests
- Gemeinsame Notfallübungen

Foto von charlesdeluvio auf Unsplash

Quelle: https://www.security-insider.de/10-typische-fehler-ransomware-angriffe-a-f4d609c5b29bea15014ddf1f1c279f85/?cmp=nl-ede617ce-bb32-418b-8967-bc79e3a81876&uuid=337D99CC-15A9-4E87-B643-1C288539C55F, abgerufen am 22.04.2025

8. Fehlendes Security Monitoring

Problematische Praktiken:

- Warnmeldungen aus Security-Lösungen werden übersehen, gehen in einer Flut irrelevanter Meldungen unter oder werden aufgrund fehlenden Fachwissens falsch interpretiert.

Präventionsmaßnahmen:

- Dediziertes Personal für IT-Sicherheit oder Managed Security Services wie MXDR oder Managed SOC
- Klare Meldeketten
- Regelmäßige Überprüfung der Sicherheitsstrategie

Foto von Vidi Drone auf Unsplash

Quelle: https://www.security-insider.de/10-typische-fehler-ransomware-angriffe-a-f4d609c5b29bea15014ddf1f1c279f85/?cmp=nl-ede617ce-bb32-418b-8967-bc79e3a81876&uuid=337D99CC-15A9-4E87-B643-1C288539C55F, abgerufen am 22.04.2025

9. Technische Schulden

Problematische Praktiken:

- Veraltete IT-Infrastrukturen

Präventionsmaßnahmen:

- Fokus nicht nur auf neue Systeme oder Sicherheitsprodukte legen, sondern technische Schulden regelmäßig abarbeiten

Foto von Matt Benson auf Unsplash

Quelle: https://www.security-insider.de/10-typische-fehler-ransomware-angriffe-a-f4d609c5b29bea15014ddf1f1c279f85/?cmp=nl-ede617ce-bb32-418b-8967-bc79e3a81876&uuid=337D99CC-15A9-4E87-B643-1C288539C55F, abgerufen am 22.04.2025

10. Panik im Ernstfall

Problematische Praktiken:

- „Headless Chicken Mode“ nach der Entdeckung einer schwerwiegenden Attacke

Präventionsmaßnahmen:

- Im Vorfeld erstellter Notfallplan, offline verfügbar und nicht auf einem verschlüsselten Server
- System-Priorisierung
- Idealerweise haben die Verantwortlichen bereits im Vorfeld Kontakt zu den Fachleuten (Incident-Response-Team) hergestellt und einen Incident-Response-Retainer-Vertrag abgeschlossen

Foto von Finja Petersen auf Unsplash

Quelle: https://www.security-insider.de/10-typische-fehler-ransomware-angriffe-a-f4d609c5b29bea15014ddf1f1c279f85/?cmp=nl-ede617ce-bb32-418b-8967-bc79e3a81876&uuid=337D99CC-15A9-4E87-B643-1C288539C55F, abgerufen am 22.04.2025

Ihre Fragen?

Ihre Wünsche?