DFN-CERT

deutsches forschungsnetz

Neues aus dem DFN-CERT

82. Betriebstagung | 25.03.2025

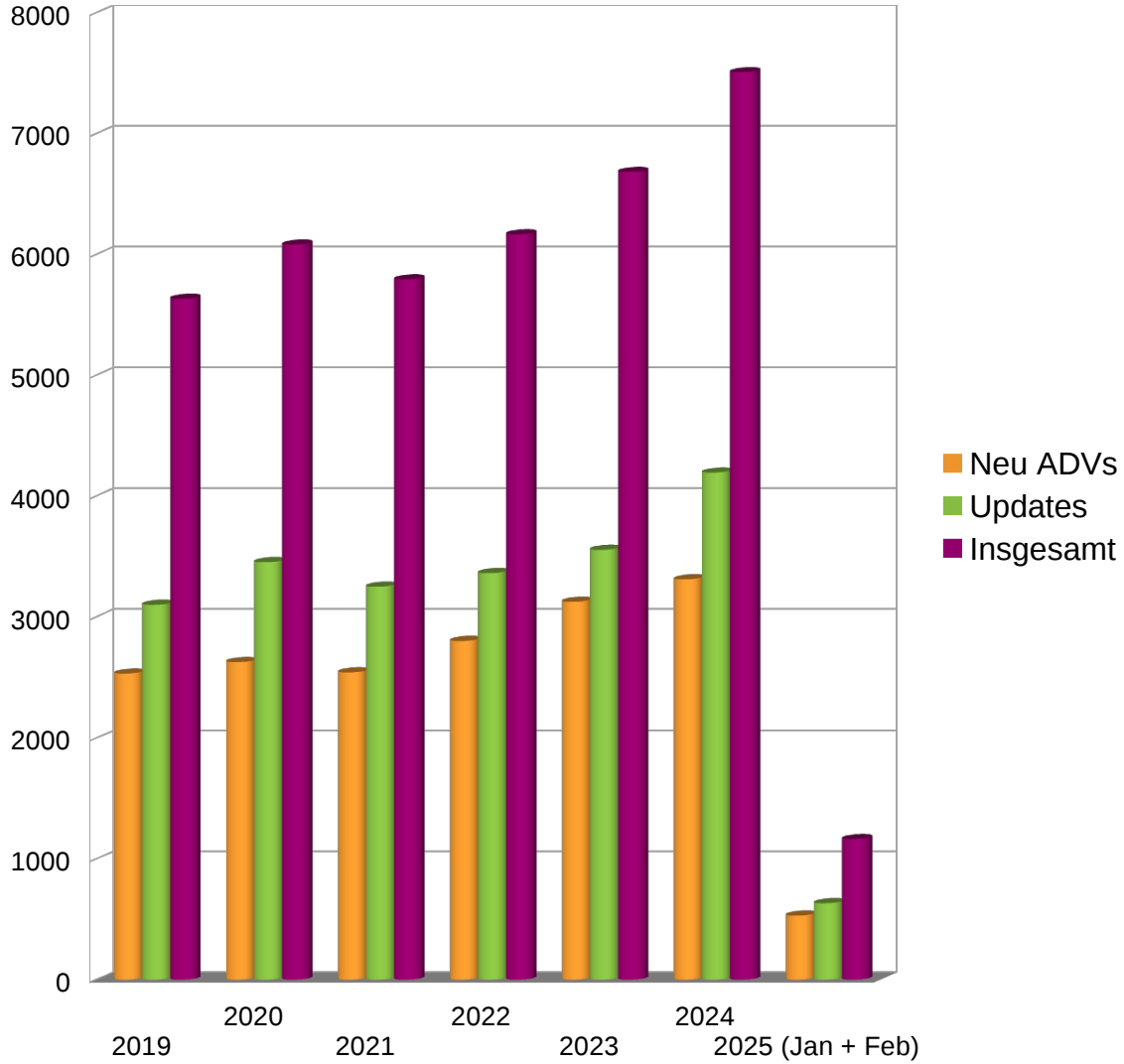
Christine Kahl

Agenda

1. Schwachstellenmeldungen
2. AW-Meldungen
3. Düt un Dat
4. Planung

Schwachstellenmeldungen

Aktuelle Advisory Zahlen



- Gesamtzahlen
  - 2024: 7509
  - Anstieg zum Vorjahr: mehr als 12%
- Prognose 2025
  - Keine Änderung des Trends absehbar
- Es skaliert nicht mehr so recht, darum denken wir nach:
  - Was können wir ändern?
  - Was erhöht eventuell sogar den Nutzen für Sie?

Unerfreulich viele kritische Schwachstellen

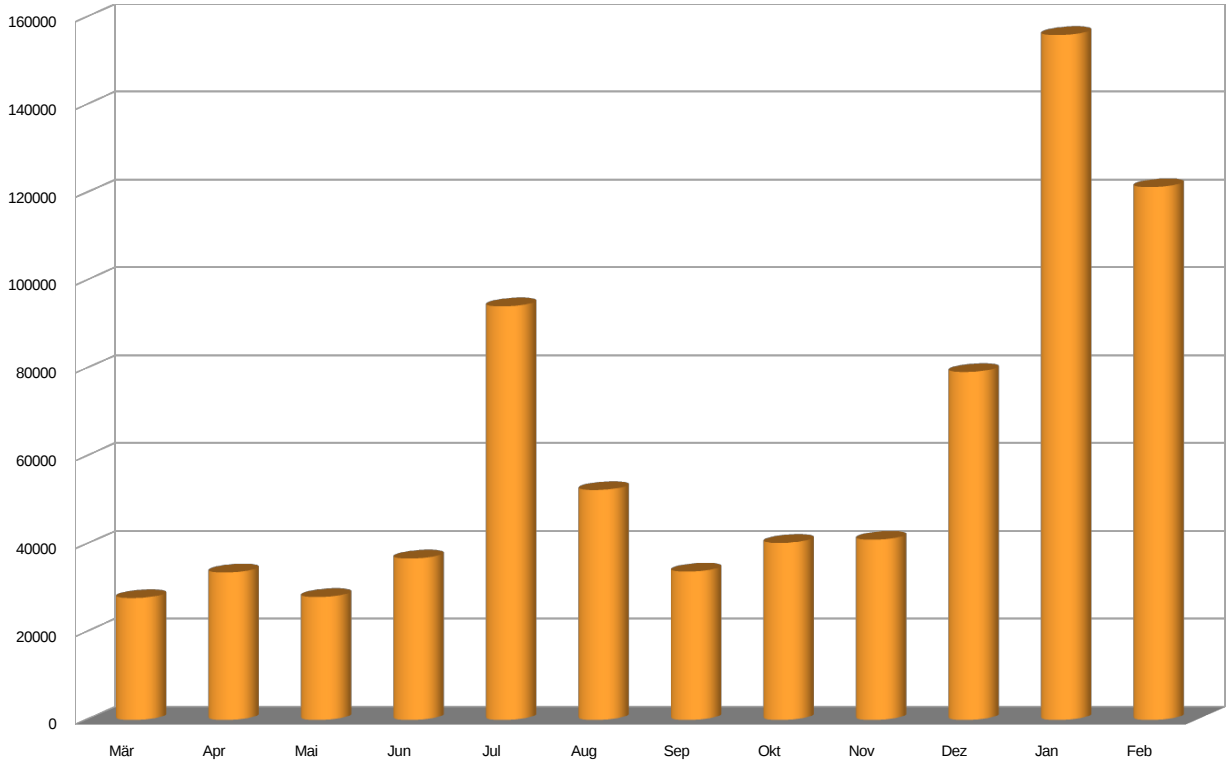
- CVSS-Score von 10.0 (zweite Jahreshälfte 2024):
  - Cisco Unified Industrial Wireless Software, CVE-2024-20418: In der webbasierten Verwaltungsoberfläche von Ultra-Reliable Wireless Backhaul (URWB) Access Points können nicht authentifizierte Angreifer aus dem Netz Befehle einschleusen, die mit Administratorrechten im Betriebssystem ausgeführt werden.
  - GitHub, CVE-2024-45409: Eine Schwachstelle in der SAML-Implementierung erlaubt es, sich als beliebiger Benutzer anzumelden.
  - Zimbra, CVE-2024-45519: Eine Schwachstelle erlaubt entfernten Angreifern das Ausführen beliebigen Programmcodes.
- CVSS-Score 9.8 oder 9.9 (zweite Jahreshälfte 2024):
  - Veeam Service Provider Console, CVE-2024-42448, CVSS 9.9
  - Android, CVE-2024-43091, CVSS 9.8
  - Microsoft Windows, CVE-2024-38063, CVE-2024-43468, CVE-2024-49112; alle CVSS 9.8
  - Aruba Access Points, CVE-2024-42505, CVE-2024-42506, CVE-2024-42507, CVE-2024-42509; alle CVSS 9.8
  - …

Unerfreulich viele kritische Schwachstellen

- CVSS-Score 10.0 (2025):
  - IBM AIX, CVE-2024-56346: Aufgrund unzureichender Prozesskontrollen ist das Ausführen beliebigen Programmcodes aus der Ferne möglich.
- CVSS-Score von mindestens 9.8 (2025):
  - FortiSwitch, CVE-2023-37936, CVSS 9.8
  - Oracle WebLogic Server, CVE-2025-21535, CVSS 9.8
  - Cisco Meeting Management, CVE-2025-20156, CVSS 9.9
  - Apple iPadOS, MacOS, CVE-2025-24137, CVSS 9.8
  - Cisco Identity Services Engine, CVE-2025-20124, CVSS 9.9
  - curl, libcurl, Meinberg LANTIME, CVE-2025-0665, CVSS 9.8
  - ...
- Schwachstellen sind nach gestohlenen Credentials (47%) das zweithäufigste Einfallstor (29%) für Ransomwareangriffe (nach Cyber Threat Index 2025 von Coalition Security)

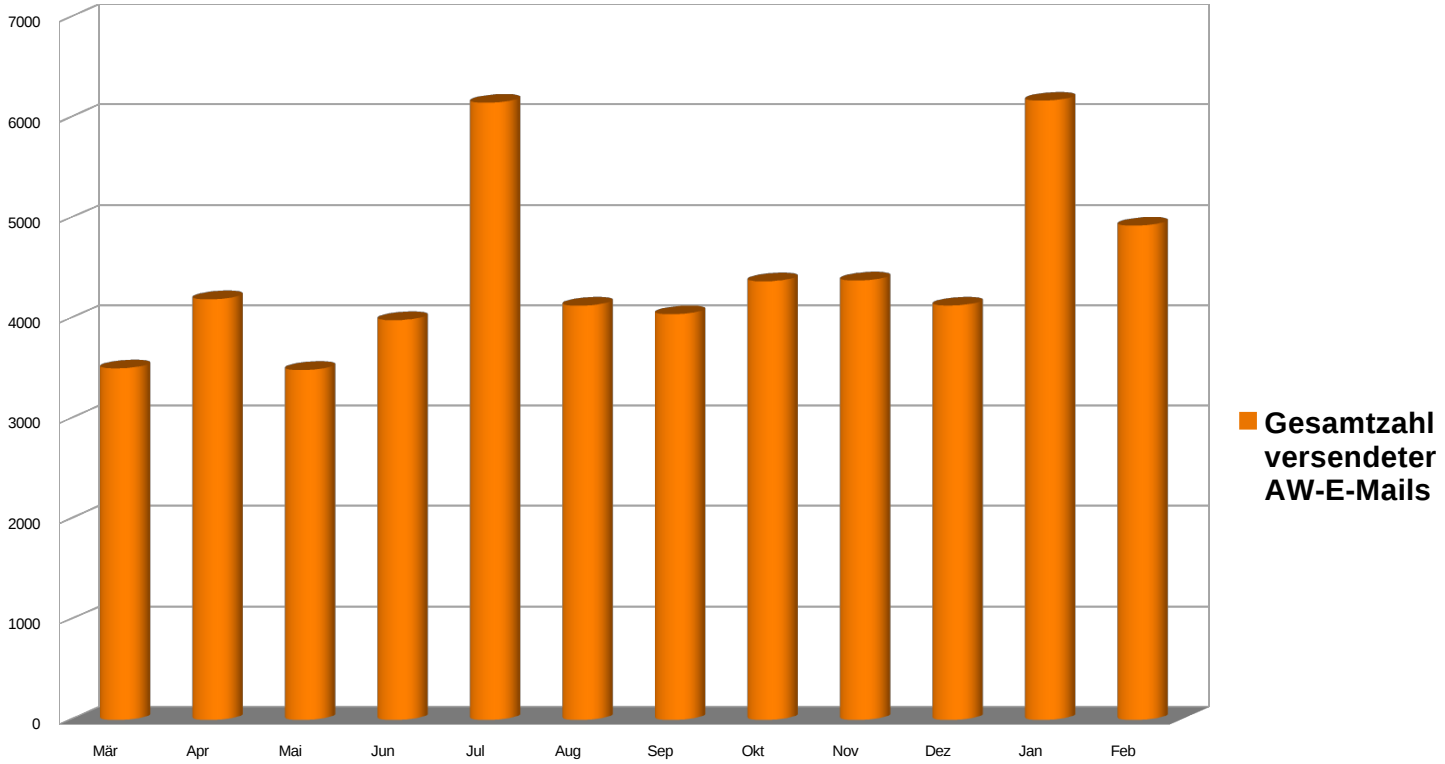
AW-Meldungen

Automatische Warnmeldungen - Events



- Die drei größten Abweichungen nach oben, ergeben sich durch die, mittlerweile hoffentlich bekannte, zeitlich begrenzte Versendung von Warnmeldungen bestimmter Kategorien, die sonst aufgrund hoher ‚false positive'-Werte oder gewünscht offener Systeme nicht weitergegeben werden. Diese sogenannten ‚Inventarscans' erfolgen etwa halbjährlich, stets mit vorheriger Ankündigung, welche Informationen in welcher Woche prozessiert werden.
- Die hier gezeigte Statistik umfasst auch Daten, die durch Teilnehmer an der Logdatenanalyse in unsere Systeme eingehen. Hier ergaben sich Schwankungen insbesondere durch gestiegene Einlieferungen von Windows-Events und DNS-RPZ-Logdaten (Dezember).

Automatische Warnmeldungen - E-Mails



- Die Peaks der versendeten E-Mails sind, aufgrund unterschiedlich starker Aggregation, nicht komplett in Übereinstimmung mit den Peaks der versendeten Events, aber auch hier sind die ‚Inventarscans' im Juli und Januar und etwas geringer im Februar sichtbar.
- Insgesamt ist zu beachten, dass die Zahlen immer etwas unscharf ist, da wir zur Systemüberwachung Events erzeugen und E-Mails versenden lassen, so etwa 30 Mails pro Woche, plus ‚echte' Events, die wir im Rahmen des Dienstmerkmals DNS-RPZ provozieren.

AW-Meldungen - Vorfälle

- Dauerbrenner
  - Kompromittierte Accounts über die Spam versendet wird und/oder Phishing-Kampagnen stattfinden.
  - Kompromittierte Systeme, die für DoS-Angriffe missbraucht werden und DoS-Angriffe, die gegen Einrichtungen gerichtet sind.
- Erwähnenswert
  - Im Januar zum ersten Mal von uns im DFN gesehen: Phishing- Kampagne bei der erbeutete Credentials über Telegram-Bots an öffentliche Kanäle geschickt wurden. Telegram-Bots werden seit etwa einem Jahr verstärkt in Phishing-Kampagnen eingesetzt.
  - In den letzten Monaten: Zunahme von Brute-Force-Angriffen auf VPN-Dienste mit ständig wechselnden IP-Adressen, wodurch eine Abwehr durch Sperrung erschwert wird.
  - Wenig größere Ransomware-Vorfälle, je einer (eher klein) im November und einer im Januar.
- Check-Point: Cyber Security Bericht für 2024
  - Größter Zuwachs von Angriffen (+75%) im Bereich Education.
  - Gefolgt von Zuwächsen im Bereich ‚Government' und ‚Healthcare & Medical'.

Düt un Dat

Düt un Dat (Plattdütsk bliff lebennig)

- DFN-Security Challenge
  - Schön war’s, insbesondere auch die Vorschläge für neue/erweiterte Usecases, die wir heiß diskutiert haben.
  - Anstrengend war’s auch, da eine ganze Reihe von Dingen manuell getrackt werden mussten.
  - Als Erfolge verbuchen wir:
    - Insgesamt 48 Teilnehmer an der Challenge haben zusammen 27.822 Punkte erzielt.
    - Es wurde eine Anbindung an die Logdatenanalyse für wazuh (Open Source Sicherheitsplattform) entwickelt und der Community zur Verfügung gestellt.
    - Mehrere Vorschläge für neue Usecases oder die Erweiterung bestehender Usecases wurden eingereicht. Dreimal haben wir die volle Punktzahl für neue und relevante Vorschläge vergeben.
    - Die DNS-RPZ Community-Zone erfreut sich an sieben regelmäßig Daten einliefernden Teilnehmern.
  - Auch wenn es von uns keine Punkte mehr gibt, bleiben sie am Ball!
- Haben Sie Ideen für Maßnahmen/wollen selbst was machen? Melden Sie sich!

Düt un Dat

- Lageberichte
  - Teilnehmer an den DFN-Security Basisleistungen erhalten von uns zweimal jährlich einen Lagebericht.
  - Aktuell werden diese an unsere Kontakte für die Dienstvereinbarung gesendet.
  - Hier wird es Änderungen geben, die werden gerade definiert.
- Aktive Usecases
  - Aktuelles Dokument zu den aktiven Usecases und damit Daten, die in der Logdatenanalyse verarbeitet werden, finden Sie auf der DFN-CERT Webseite → Leistungen → Security Operations → Logdatenanalyse
  - https://www.dfn-cert.de/documents/110/DFN-Security-Logbasierte-Usecases.pdf
  - Weiterhin nehmen sehr gerne Vorschläge zu Usecases von Ihnen an.
  - Auch interessieren uns Ihre Erfahrungen im Bezug auf Windows-Events.

Planung

Planung

- Schwachstellenmeldungen
  - Bisher nur grobe Ideen Richtung Automatisierungen und Fokussierung auf die schwerwiegenderen Schwachstellen.
  - Alles was da an Änderung ansteht wird natürlich im Vorwege kommuniziert.
  - Eventuell versuchen wir da auch strukturiert Feedback von Ihnen einzusammeln.
  - Wir sind für Vorschläge/Wünsche offen.
  - Dieser Dienstbestandteil soll Ihren Bedarf decken, lassen Sie uns gern wissen wie der genau aussieht.
- DNS-RPZ
  - Wir schauen kontinuierlich nach weiteren Listen und Daten, die angeboten oder eingebunden werden können.(In Vorbereitung: Threatfox RPZ)
  - Weiterhin bleibt aber ein wichtiges Ziel von uns, ‚false positives' zu vermeiden, daher arbeiten wir auch an Änderungen der Allow-Listen.

Planung

- Netzwerkprüfer
  - Steht seit ewigen Zeiten auf unserer ToDo-Liste.
  - Wir haben sehr lange darauf gewartet, dass über GÉANT und den Security-Task ein Schwachstellenfeed bereitgestellt wird. Leider ist jetzt aber klar, dass es den so nicht geben wird.
  - Wir nehmen jetzt noch mal neu Anlauf.
- Logdatenanalyse
  - Natürlich immer Arbeit an den Usecases.
  - Zusätzliches Augenmerk in diesem Jahr: Monitoring und Reporting.

Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie Fragen?

- DFN-CERT Hotline
  - cert@dfn-cert.de
  - 040 / 808 077-590

Dienst DFN-Security, Security-Portal

portal-contact@dfn-cert.de

DNS-RPZ

dns-rpz@dfn-cert.de

- Weitere Informationen: https://www.security.dfn.de/

https://www.dfn-cert.de/leistungen/security-operations/