DFN-CERT

deutsches forschungsnetz

Neues aus dem DFN-CERT

84. Betriebstagung | 17.03.2026

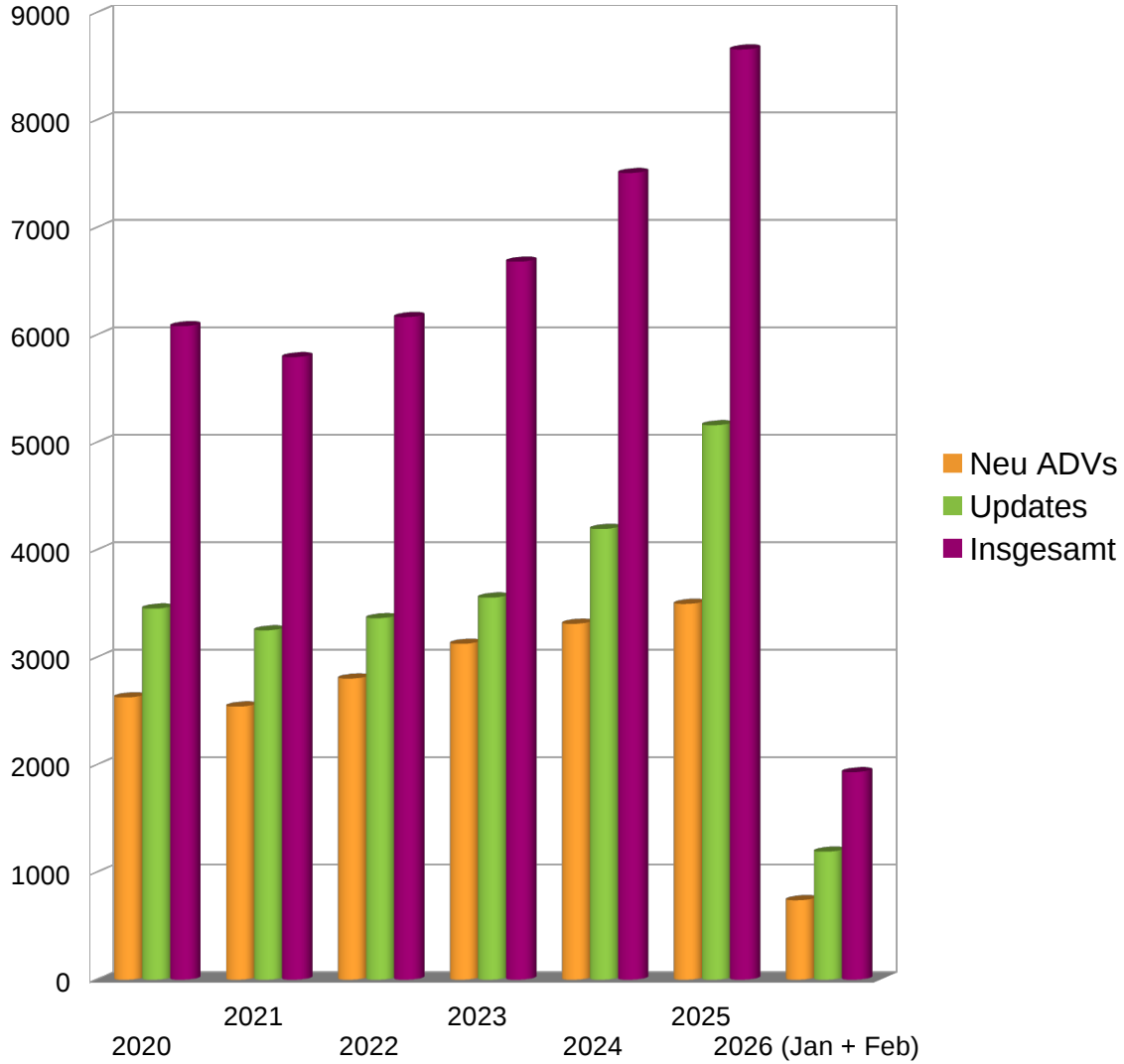
Christine Kahl

Agenda

1. Schwachstellenmeldungen
2. AW-Meldungen
3. Lageberichte
4. Ankündigungen

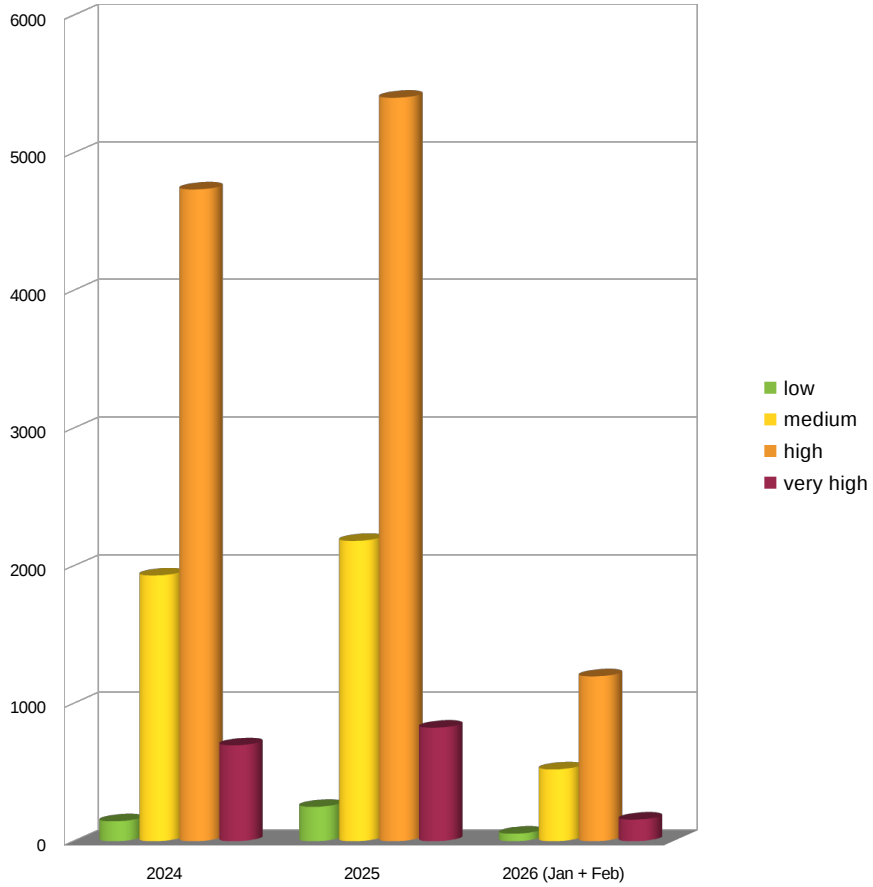
Schwachstellenmeldungen

Aktuelle Advisory Zahlen



- Gesamtzahlen
  - 2025: 8.659
  - 2024: 7.509
  - Anstieg zum Vorjahr: mehr als 15%
  - Bei 5-Tage Woche eine Verteilung auf ca. 250 Arbeitstage: 34 Meldungen pro Tag
- Prognose 2026
  - Zahlen weiterhin steigend (Jan + Feb: 1.932)

ADVs nach CVSS Schweregrad – 2024 - 2026



- Anzahl der schwerwiegenden Meldungen steigt in etwa gleichem Umfang, wie die Anzahl der Meldungen insgesamt
- High Meldungen
  - 2024 = 4736, ca. 395 pro Monat
  - 2025 = 5402, ca. 450 pro Monat
  - Jan+Feb 26 = 1198, 599 pro Monat
- Very high Meldungen
  - 2024 = 697, ca. 58 pro Monat
  - 2025 = 825, ca. 68 pro Monat
  - Jan+Feb 26 = 157, 78,5 pro Monat

Kritische Schwachstellen mit CVSS ab 9.8

(ausgewählt seit der letzten BT im Oktober 2025)

- Microsoft Windows Server Update Service (WSUS) (CVE-2025-59287, CVSS 9.8): Deserialisierung von nicht vertrauenswürdigen Daten ohne ausreichende Prüfung ermöglicht Ausführen beliebigen Programmcodes mit ‘SYSTEM’-Privilegien. Ausnutzung beobachtet ab dem 24.10.25, adressiert im Rahmen des Oktober Patchtags 25.

- Oracle E-Business Suite (CVE-2025-61882, CVSS 9.8; CVE-2025-61884, CVSS 7.5): Die Schwachstellen ermöglichen das Ausspähen von Informationen und Ausführen beliebigen Programmcodes. Erste Angriffe wurden Wochen vor der Veröffentlichung des Sicherheitsupdates, nämlich ab dem 09.08.25 beobachtet. Über die Schwachstellen konnten teilweise erhebliche Datenmengen extrahiert werden, die für eine Erpressungskampagne einer unter dem Namen Clop agierenden Gruppe verwendet werden. (Sicherheitsupdates 06.10.25)

- Samba (CVE-2025-10230, CVSS 10.0): Schwachstelle ermöglicht das Ausführen beliebigen Programmcodes mit den Rechten des Dienstes und kann Einfluss auf andere Komponenten haben.

Kritische Schwachstellen mit CVSS ab 9.8
(ausgewählt seit der letzten BT im Oktober 2025)

- Oracle Fusion Middleware (CVE-2025-61757, CVSS 9.8): Schwachstelle aufgrund fehlender Authentifizierung für kritische Funktionen, wodurch ein Angreifer aus der Ferne Programmcode ausführen und die Kontrolle über das gesamte System übernehmen kann. Veröffentlicht mit Oktober Patchtag 25, seit Ende November im CISA Known Exploited Vulnerability Catalog enthalten.

- Fortinet FortiWeb (CVE-2025-64446, CVSS 9.8; CVE-2025-58034, CVSS 7.2): Durch die Ausnutzung können Administrationskonten auf einer Instanz erstellt und die Anwendung damit vollständig kompromittiert werden. Die erste Meldung über eine aktiv ausgenutzte Schwachstelle am 06.10.25, Patch verfügbar am 28.10.25 ohne Details, diese wurden am 14.11.25 veröffentlicht, zusammen mit Medienberichten über eine massive Ausnutzung.

Kritische Schwachstellen mit CVSS ab 9.8

(ausgewählt seit der letzten BT im Oktober 2025)

- MISP Threat Sharing (GCVE-1-2025-0010, CVSS 8.2, Umgehen von Sicherheitsvorkehrungen; GCVE-1-2025-0011, CVSS 9.9, Ausführen beliebigen Programmcodes; GCVE-1-2025-0013, CVSS 9.9, Privilegieneskalation; GCVE-1-2025-0014, CVSS 9.9, Cross-Site-Scripting-Angriff; GCVE-1-2025-0015, CVSS 9.9, Cross-Site-Scripting-Angriff): Alle vorgenannten Angriffe können Einfluss auf andere Komponenten haben.

- IBM AIX und IBM VIOS (CVE-2025-36096, CVSS 9.0, Umgehen von Sicherheitsvorkehrungen; CVE-2025-36236, CVSS 8.2, Manipulation von Dateien; CVE-2025-36250, CVSS 10.0, Ausführen beliebigen Programmcodes; CVE-2025-36251, CVSS 9.6, Ausführen beliebigen Programmcodes): IBM vergibt für eine Schwachstelle den CVSS von 10.0. Abweichend vergibt NVD ‘nur’ eine 9.8, aufgrund einer anderen Einschätzung, ob die Schwachstelle Einfluss auf andere Komponenten haben kann.

- Cisco Unified Contact Center Express (CVE-2025-20354, CVSS 9.8, Ausführen beliebigen Programmcodes mit Administratorrechten; CVE-2025-20358, CVSS 9.4, Umgehen von Sicherheitsvorkehrungen): Schwachstellen basieren auf fehlender Authentifizierung für kritische Funktionen und das Hochladen oder Erstellen von beliebigen Dateien.

Kritische Schwachstellen mit CVSS ab 9.8
(ausgewählt seit der letzten BT im Oktober 2025)

- FortiGate-Firewall mit Fortinet FortiOS (CVE-2020-12812, CVSS 5.2 bei Veröffentlichung durch Hersteller, jetzt CVSS 9.8 von NVD): Ermöglicht Umgehen der Zwei-Faktor-Authentisierung für LDAP und wird jetzt aktiv ausgenutzt.

- Cisco Secure Email Gateway und Cisco Secure Email and Web Manager (CVE-2025-20393, CVSS 10.0, Schwachstelle ermöglicht das Ausführen beliebigen Programmcodes mit Administratorrechten): Aufgrund unzureichende Eingabevalidierung, Veröffentlichung am 17. Dezember, Ausnutzung mindestens seit 10. Dezember, wahrscheinlicher seit Ende Nov.

- FortiOS, FortiWeb, FortiProxy und FortiSwitchManager (CVE-2025-59718, CVSS 9.8, Umgehen von Sicherheitsvorkehrungen): Schwachstelle aufgrund einer unsachgemäßen Überprüfung der kryptografischen Signatur. Bereits drei Tage nach Veröffentlichung konnte eine aktive Ausnutzung beobachtet werden.

Kritische Schwachstellen mit CVSS ab 9.8
(ausgewählt seit der letzten BT im Oktober 2025)

- React Server Components (CVE-2025-55182, CVSS 10.0): Unsichere Deserialisierung von Nutzdaten ermöglicht Programmcodeausführung, auch React2Shell genannt, wegen Nutzung der Komponente in anderer Software, Ausnutzung startete kurz nach Veröffentlichung.
- FortiAnalyser, FortiManager und FortiOS (CVE-2026-24858, CVSS 9.8, Umgehen von Sicherheitsvorkehrungen): Schwachstellen basieren auf dem Umgehen der Authentifizierung und wurde bereits vor Veröffentlichung ausgenutzt.
- GNU InetUtils (CVE-2026-24061, CVSS 9.8, Umgehen von Sicherheitsvorkehrungen): Verwundbarkeit aufgrund des Umgehens der Remote-Authentifizierung bei aktiviertem und von außen erreichbaren telnetd. Schwachstelle existiert seit 11 Jahren und wird aktiv ausgenutzt.

Kritische Schwachstellen mit CVSS ab 9.8
(ausgewählt seit der letzten BT im Oktober 2025)

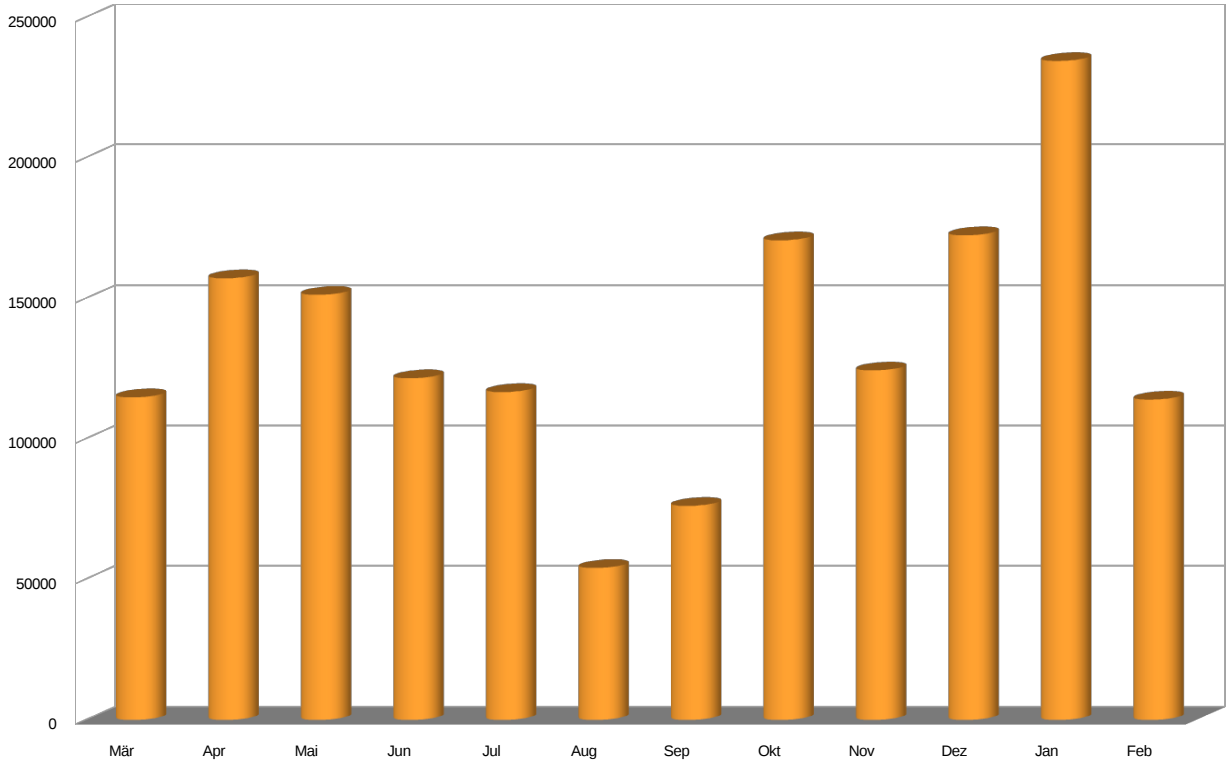
- Zimbra Collaboration Suite (CVE-2025-68645, CVSS 9.8, Ausführen beliebigen Programmcodes): Veröffentlicht im Mitte November 2025 und am 22. Januar in den Known Exploited Katalog aufgenommen. Laut CERT-Bund/BSI werden in DE 40% der Zimbra-Instanzen mit veralteter Software betrieben.
- GNU Wget2 (CVE-2025-69194, CVSS 9.8, Ausführen beliebigen Programmcodes mit Benutzerrechten): Schwachstelle ermöglicht Dateien an nicht vorgesehene Speicherorte zu schreiben.
- Apple iOS, iPadOS, macOS u. a. (CVE-2026-20700, CVSS 9.8, Ausführen beliebigen Programmcodes): Durch das Schreiben von Speicher außerhalb gültiger Puffergrenze kann beliebiger Programmcode ausgeführt werden. Schwachstelle wurde am 12.02.26 behoben und am 17.02 in der Katalog aktiv ausgenutzter Schwachstellen aufgenommen.

Kritische Schwachstellen mit CVSS ab 9.8
(ausgewählt seit der letzten BT im Oktober 2025)

- Mozilla Firefox und Thunderbird (CVE-2026-0881, CVSS 10.0, Umgehen von Sicherheitsvorkehrungen; CVE-2026-0884, CVSS 9.8, Ausführen beliebigen Programmcodes): Der Ausbruch aus der geschützten Umgebung (Sandbox Escape) kann andere Komponenten beeinträchtigen.
- OpenSSL (CVE-2025-15467, CVSS 9.8, Ausführen beliebigen Programmcodes): Pufferüberlauf auf dem Stack aufgrund des Kopierens von ‘ASN.1’-Parametern ohne vorherige Prüfung, ob das Ziel groß genug für die Daten ist.
- Juniper Junos OS Evolved (CVE-2026-21902, CVSS 9.8, Ausführen beliebigen Programmcodes mit Administratorrechten) fälschlicherweise nach außen offener Port, der nur intern zugänglich sein sollte.

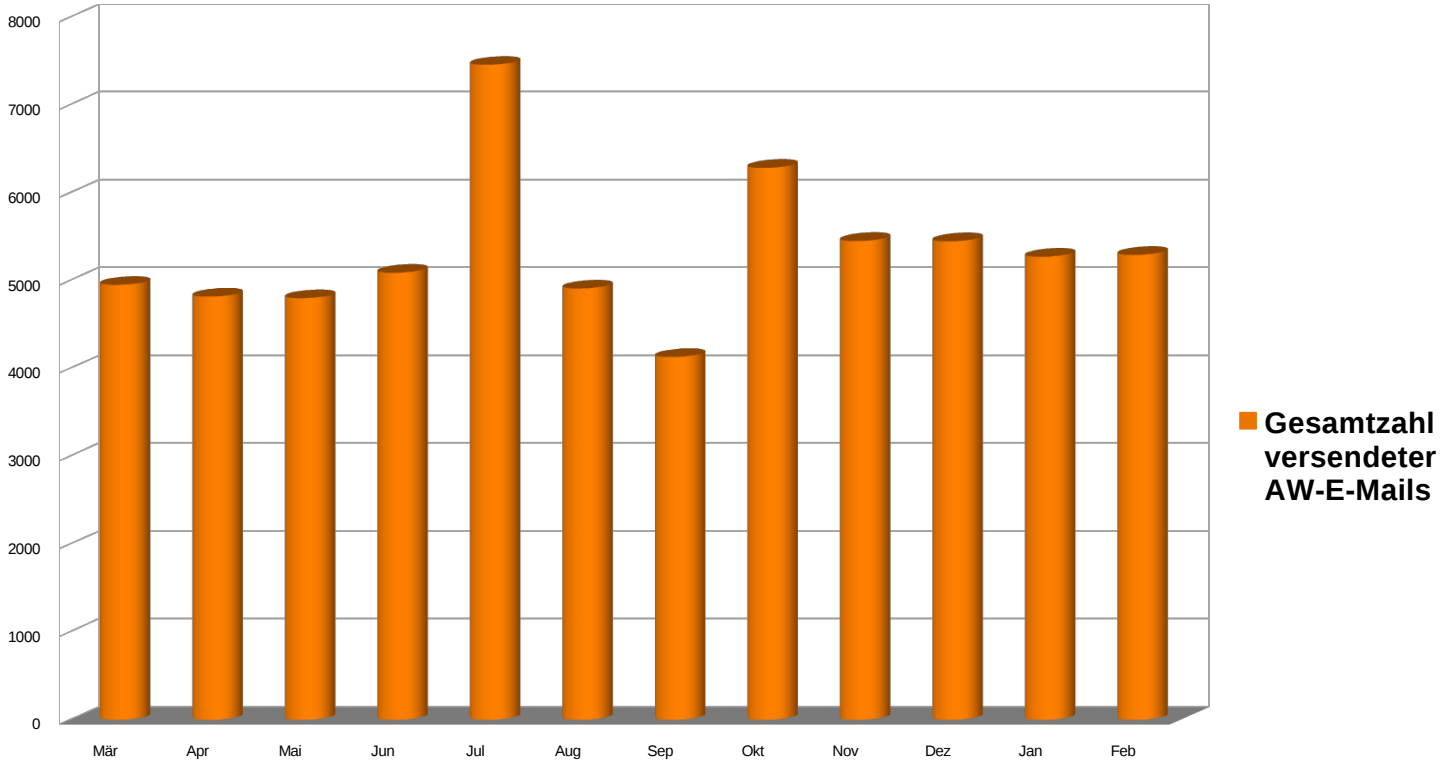
AW-Meldungen

Automatische Warnmeldungen - Events



- Oktober 25:
  - 48% der Meldungen entfallen auf die Kategorie ‘Access Domains’ (DNS-RPZ, kurzzeitig geblockte CDN-Domain)
  - Kategorie ‘Unrestricted Access’ (offen aus dem Internet erreichbare Systemen) Anzahl zu Sept verdoppelt. Großteil MS-RPC-Dienste
- November 25:
  - Änderung bei Verarbeitung der Logdaten von DFN-Mailsupport die zur Verringerung von nicht eindeutig positiven Meldungen geführt haben

Automatische Warnmeldungen - E-Mails



- Dezember 25:
  - 55% der Meldungen ‘Access Domains’ (keine Analyse, ob auch FP hier reinspielen, Analyse nur zeitnah möglich)
  - Durch Schwachstellen verwundbare Systeme, sechs neue aufgenommen u. a. React Server-Komponenten (CVE-2025-55182)
- Januar 26:
  - Durch Schwachstellen verwundbare Systeme, zehn neue aufgenommen u. a. Zimbra Collaboration Suite (CVE-2025-68645)
  - Shadowserver Report zu kompromittierten Accounts: mehr als drei Millionen Benutzerkonten aus Infostealern, 276 dieser Einträge konnten verifizierten Domains zugeordnet werden

AW-Meldungen - Vorfälle

- Februar 26:
  - Im Vergleich zum Vormonat fast halbierte Zahl an Events bei nahezu identischer Zahl versendeter E-Mails basiert auf deutlich verringerter Zahl gemeldeter Blockierungen im Dienstmerkmal DNS-RPZ.
  - Mehr als 10% der automatisch verarbeiteten Events betraf im Februar einmalige Meldungen zu kompromittierten Zugangsdaten aus Infostealer-Los. Reports von Shadowserver umfassten mehr als 120 Millionen Benutzerkonten. 15.079 dieser Einträge wurden verifizierten Domains von Teilnehmern am DFN zugeordnet und weitergemeldet.
- Dauerbrenner weiterhin
  - Kompromittierte Accounts über die Spam versendet wird
  - und/oder Phishing-Kampagnen stattfinden.
- Immer wieder werden Forschungsscanner gemeldet, deren Kommunikationsverhalten als Angriff interpretiert wird. Wer da in Vorbereitung ist, kann uns gern kontaktieren, um Vorkehrungen zu treffen, wie die Anzahl der Beschwerden reduziert werden kann.
- Zwei Einrichtungen wurden im Februar 2026 auf der Leakseite der Gruppe ‚Qilin‘ geführt. Die Gruppe ist auch international für Angriffe im Bildungssektor bekannt und aktuell neben ‚The Gentlemen‘ eine der aktiveren Gruppierungen in diesem Bereich.

Lageberichte

DFN-CERT Lagebericht – warum?

- Das was ich gerade erzählt habe, finden Sie mittlerweile auch in unseren monatlich erscheinenden Lageberichten.
- Von mir gab es, eine kleine Zusammenfassung.
- Die Berichte geben noch mehr Infos zu
  - Gerade relevanten/neuen Schwachstellen.
  - Aktuellen Reports und Anpassungen die Automatischen Warnmeldungen betreffend.
  - Und zeigen wie sich verschiedene Bereiche entwickeln (Kennzahlen).
- Und natürlich bekommen Sie das Ganze

zeitnah!

DFN-CERT Lagebericht – wie?

- Voraussetzung: Teilnehmer am Dienst DFN-Security
  - Achtung: Nur weil Sie Zugriff auf das Security Portal haben, heißt das **nicht**, dass Sie am Dienst DFN-Security teilnehmen.
  - Das tun Sie nur, wenn Sie die entsprechende Dienstvereinbarung unterschrieben haben.
- Der Bericht ist für Sicherheitskontakte beim jeweiligen Teilnehmer (CISO, Administrierende von Netzbereichen, u. ä.).
- Berechtigung zum Erhalt der Berichte wird geprüft, bevor eine Abonnementwunsch akzeptiert wird, ggf. über Handlungsberechtigte Person.
- Die Berichte sind **nicht** öffentlich!
- Mailingliste: https://www.listserv.dfn.de/sympa/info/dfn-cert-lageberichte

BSI Lagebericht – seit Januar 26

- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellt als nationales IT-Lagezentrum für Kooperationspartner und Betreiber kritischer Infrastrukturen werktäglich Lageberichte.
- Diese Berichte umfassen Informationen, wie z.B. Schwachstellen in vom DFN-CERT Schwachstellendienst nicht unterstützter Software oder Vorfälle außerhalb des DFN, die für DFN Teilnehmer interessant und hilfreich sein können.
- Das DFN-CERT hat als Mitglied im Deutschen CERT-Verbund und der Allianz für Cybersicherheit die Erlaubnis erhalten als Multiplikator die BSI Lageberichte an Teilnehmer am DFN weiterzugeben.
- Die Weitergabe wird in Auszügen geschehen, da z.B. die Kurzmeldungen mit eingeschränktem Informationsumfang zu Sicherheitsupdates vor der Weitergabe entfernt werden, wie auch einige Meldungen aus dem Bereich ‚Politik & Öffentlichkeit‘.

BSI Lagebericht – seit Januar 26

- Nur Informationen, die nach dem Traffic Light Protocol (TLP) als TLP:GREEN oder niedriger eingestuft sind, werden weitergegeben.
- Diese Berichte sind ebenfalls **nicht** öffentlich.
- Eine Nichtbeachtung des TLP kann zum Ausschluss von der Mailingliste führen, da sie zum Verlust der Multiplikatorprivilegien des DFN-CERT führen kann.
- Daher die Bitte
  - Die Lageberichte nicht auf Webseiten bereitstellen und nicht beliebig weiterleiten
  - Auch nicht automatisch bei VirusTotal hochladen
  - ...

BSI Lagebericht – seit Januar 26

- Mailingliste: https://www.listserv.dfn.de/sympa/info/dfn-bsi-tageslageberichte
- Der Bericht ist für Sicherheitskontakte beim jeweiligen Teilnehmer (CISO, Administrierende von Netzbereichen, u. ä.).
- Berechtigung zum Erhalt der Berichte wird geprüft, bevor eine Abonnementwunsch akzeptiert wird, ggf. über Handlungsberechtigte Person.
- Eine Teilnahme am Dienst DFN-Security ist für das Abonnement dieser Mailingliste nicht erforderlich (eine Teilnahme aber natürlich trotzdem sinnvoll).

Ankündigungen

Ankündigungen

- Virtuelle Informationsveranstaltung DFN-Security
  - Nächster Termin: **02.07.2026 9:30 -12:30**
  - Agenda wird ca. einen Monat vor der Veranstaltung veröffentlicht
  - Wie üblich umfasst der Termin die
    - Vorstellung der Dienstbestandteile
    - Benutzung des Security-Portals
    - Information über die neuesten Änderungen
    - …
  - https://www.dfn-cert.de/informationen/veranstaltungen/dfn-security-infoveranstaltung/

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/