

DFN-CERT

deutsches forschungsnetz



Neues aus dem DFN-CERT

83. Betriebstagung | 07.10.2025

Christine Kahl

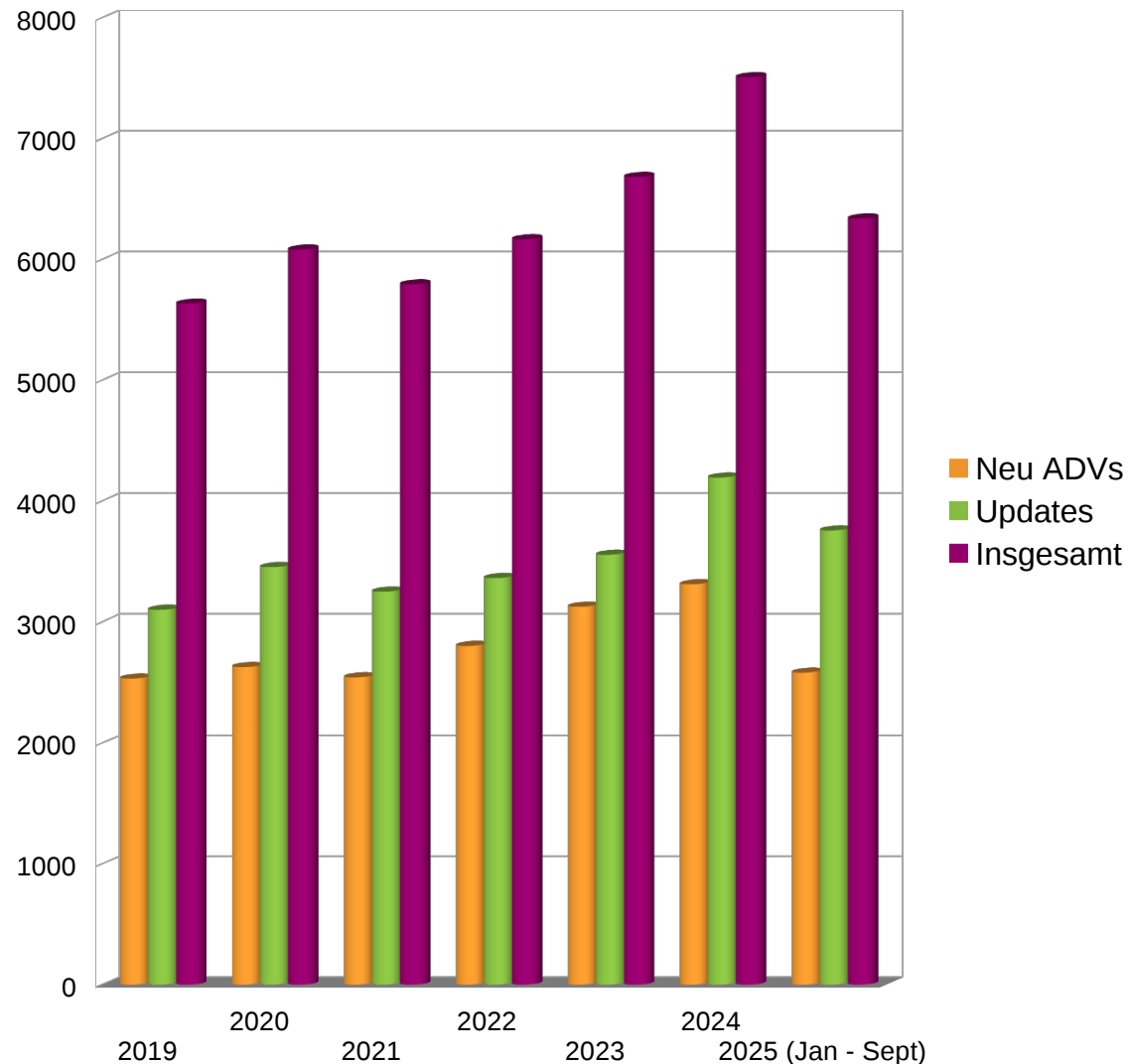
Agenda

DFN

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

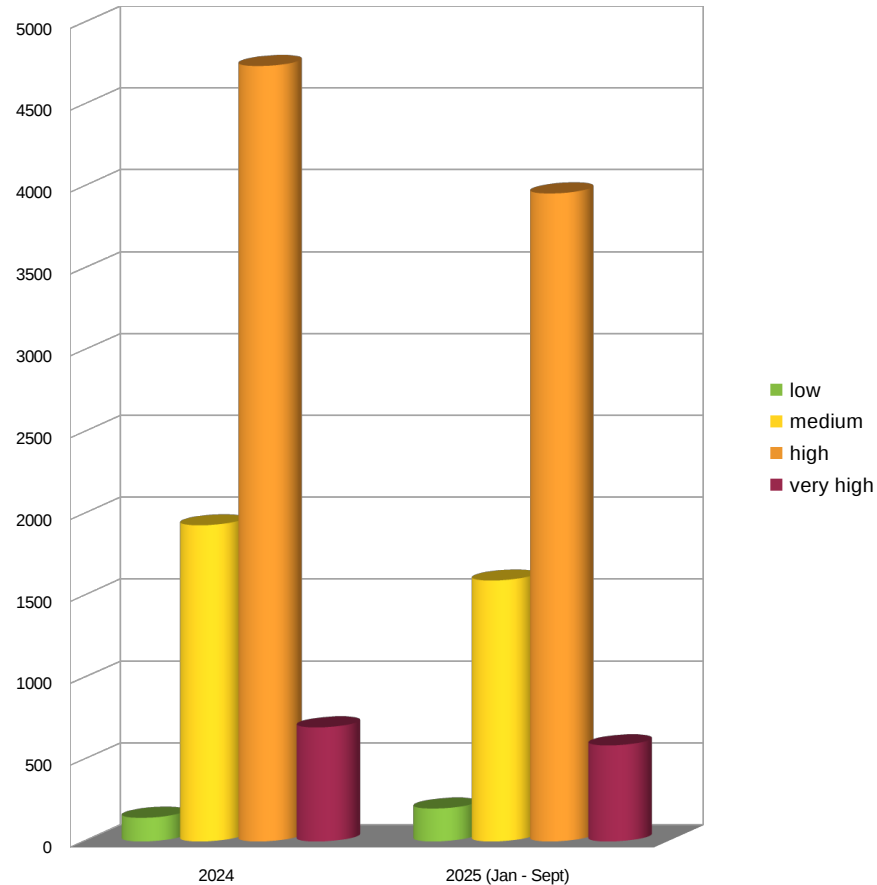
Schwachstellenmeldungen

Aktuelle Advisory Zahlen



- ▶ Gesamtzahlen
 - ▷ 2024: 7509
 - ▷ Anstieg zum Vorjahr: mehr als 12%
- ▶ Prognose 2025
 - ▷ Zahlen weiter steigend
 - ▷ Wahrscheinlich mehr als 8 Tausend Meldungen
- ▶ Es skaliert nicht mehr, darum müssen wir unsere Arbeitsweise anpassen
 - ▷ Generelle Anpassungen in den nächsten Jahren
 - ▷ Einzelmaßnahmen kurzfristig und angekündigt über das Security-Portal

ADVs nach CVSS Schweregrad – 2024 & 2025



▶ CVSS Version 3.1:

- ▶ Low = 0.1 – 3.9
- ▶ Medium = 4.0 – 6.9
- ▶ High = 7.0 – 8.9
- ▶ Very high = 9.0 – 10.0

▶ Very high Meldungen

- ▶ 2024 = 697, ca. 58 pro Monat
- ▶ 2025 = 587, ca. 65 pro Monat

► Situation

- ▶ Seit Mitte Februar 2024 ist das Kernel-Projekt als CVE Numbering Authority (CNA) für Schwachstellen im Linux-Kernel akzeptiert und ist damit die autoritäre Stelle für die Vergabe von CVE-IDs.
- ▶ Aufgrund der Einschätzung der dort Verantwortlichen, dass auf dieser Betriebssystemebene alle Programmfehler sicherheitsrelevant sein können, werden seitdem massenhaft CVE-IDs für den Kernel vergeben.
- ▶ Im Juli 2025 konnten wir einen neuen Rekord beobachten, da für den ‚Unbreakable Enterprise Kernel‘ für Oracle Linux 9 und 10 Sicherheitsupdates veröffentlicht wurden, die insgesamt 1.345 ‚Schwachstellen‘ adressieren.

► Unsere Einschätzung

- ▶ Bei einem Großteil der ‚Schwachstellen‘ lassen sich keine schadhaften Auswirkungen erkennen, weshalb sie in den Schwachstellenmeldungen des DFN-CERT nicht weiter berücksichtigt werden.
- ▶ Wenngleich das obige ein Extremfall ist, nimmt die Zahl an Meldungen, die sehr viele Schwachstellen beheben, zu.
- ▶ Wir erkennen darin keine Verschärfung der Sicherheitslage für den Kernel.

Mehr Schwachstellen – Mehr Patches – Auswirkungen auf den Dienst

- ▶ Meldungen mit einer Vielzahl behobener Schwachstellen
 - ▷ Es geht viel Aufwand in die Bewertung und Beschreibung einzelner Schwachstellen.
 - ▷ Gerade wenn viele und sehr schwerwiegende Schwachstellen mit einem Patch behoben werden, ist die Beschreibung einer jeden Einzelschwachstelle im Detail – nach unserer Einschätzung – für Sie nicht so relevant, wie die Gesamtbewertung des Sicherheitsupdates.
 - ▷ Wir versuchen hier mit Automatisierungen Aufwände zu sparen.
 - ▷ Zur Zeit wird aber alles noch manuell kontrolliert.
- ▶ Das Datenvolumen macht Änderungen notwendig
 - ▷ Bereiten Sie sich mental darauf vor, dass wir den Schwachstellendienst anpassen müssen, um die bekannte Produktpalette weiter zu bedienen.
 - ▷ Wir werden frühzeitig über generelle Änderungen informieren.

Kritische Schwachstellen mit CVSS 10.0

(seit der letzten BT)



- ▶ IBM DB2 (CVE-2025-1726): Pufferüberlauf im Datenbank-Server ermöglicht Ausführen beliebigen Programmcodes mit Systemrechten.
- ▶ Cisco Identity Services Engine (CVE-2025-1708): Die Schwachstelle ermöglicht ohne Authentifizierung das Ausführen beliebigen Programmcodes auf dem Netzwerk-Policy-Server und so die Kompromittierung zentraler Zugriffsregeln.
- ▶ Cisco Identity Services Engine (CVE-2025-20281, CVE-2025-20282, CVE-2025-20337): Die Schwachstellen ermöglichen das Ausführen beliebigen Programmcodes mit Administrationsrechten.
- ▶ Cisco IOS XE Wireless Controller (CVE-2025-20188): Ein hartkodiertes JSON-Web-Token auf Wireless-LAN-Controllern ermöglicht einem nicht authentifizierten Angreifer das Hochladen beliebiger Dateien.
- ▶ Cisco Unified Communications Manager (CVE-2025-20309): Hartkodierte Anmeldedaten für den Fernzugang ermöglichen das Erlangen von Administratorrechten.

Kritische Schwachstellen mit CVSS 10.0

(seit der letzten BT)



- ▶ Erlang/OTP SSH (CVE.2025-32433): Die Schwachstelle ermöglicht das Erlangen von root-Rechten.
- ▶ ADOdb-PostgreSQL-Treiber (CVE-2025-46337): Unzureichendes Escaping in der PostgreSQL-Integration der PHP-Bibliothek ADOdb erlaubt SQL Injection. Dieses Paket wird insbesondere von Moodle verwendet.
- ▶ Apache Parquet (CVE-2025-30065): Die Schwachstelle ermöglicht das Ausführen beliebigen Codes durch manipulierte Schema-Dateien.
- ▶ AMI MegaRAC (CVE-2024-54085): Ein Fehler in der Redfish-Schnittstelle ermöglicht den Zugriff auf die Management-Schnittstelle ohne Zugangsdaten.

Kritische Schwachstellen mit CVSS 10.0

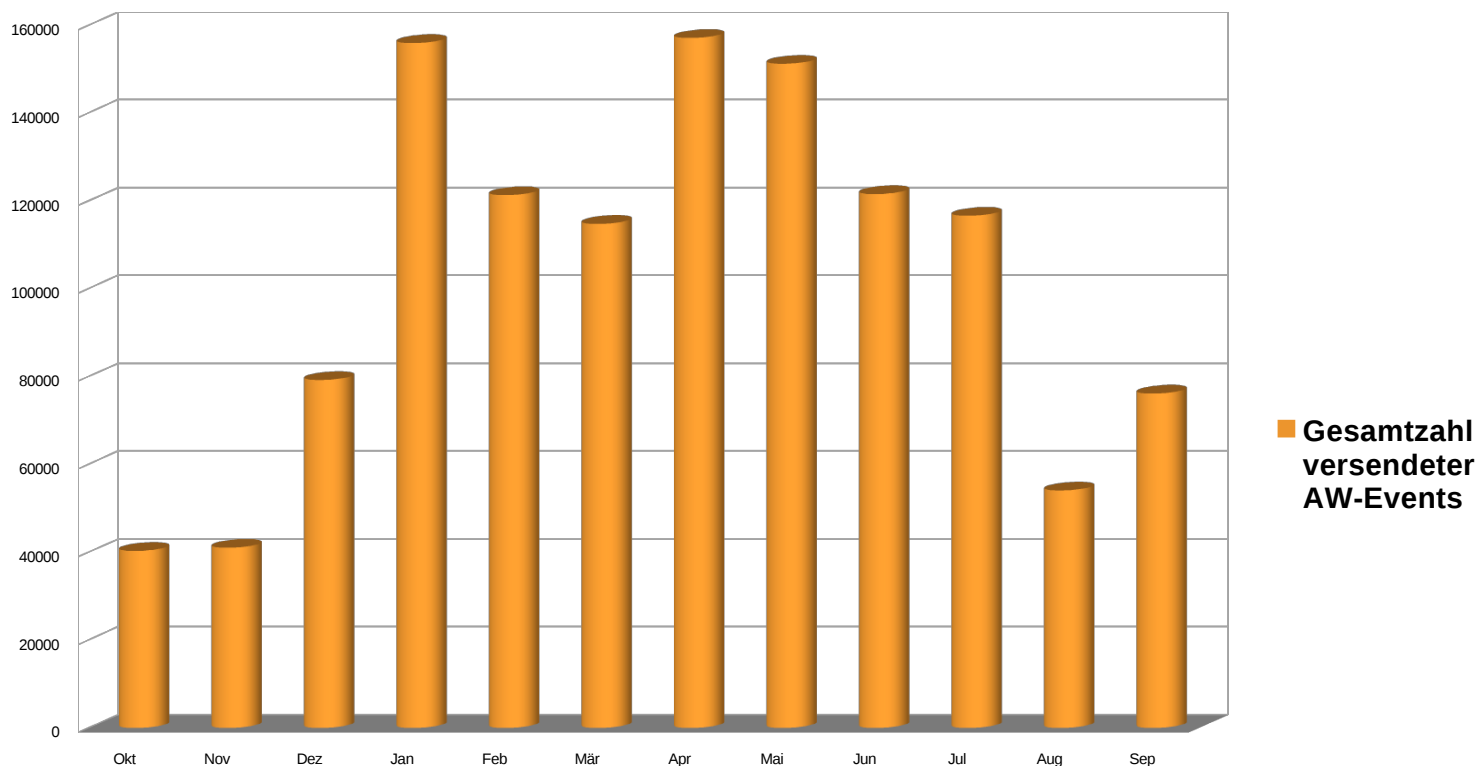
(seit der letzten BT)



- ▶ Kunbus RevolutionPI (CVE-2025-24522): Die Schwachstelle ermöglicht die Ausführung beliebigen Programmcodes.
- ▶ SAP NetWeaver Visual Composer (CVE-2025-31324): Mangelhafte Autorisierung erlaubt unberechtigte Programmcodeausführung aus der Ferne.
- ▶ Zusätzlich mehrere Schwachstellen mit einem Score von 9.8 oder 9.9
- ▶ aktuelles Beispiel: CVE-2025-20333, 9.9, Schwachstelle in Cisco Secure Firewall Adaptive Security Appliance und Threat Defense ermöglicht Ausführen beliebigen Programmcodes mit Administratorrechten → aktiv ausgenutzt

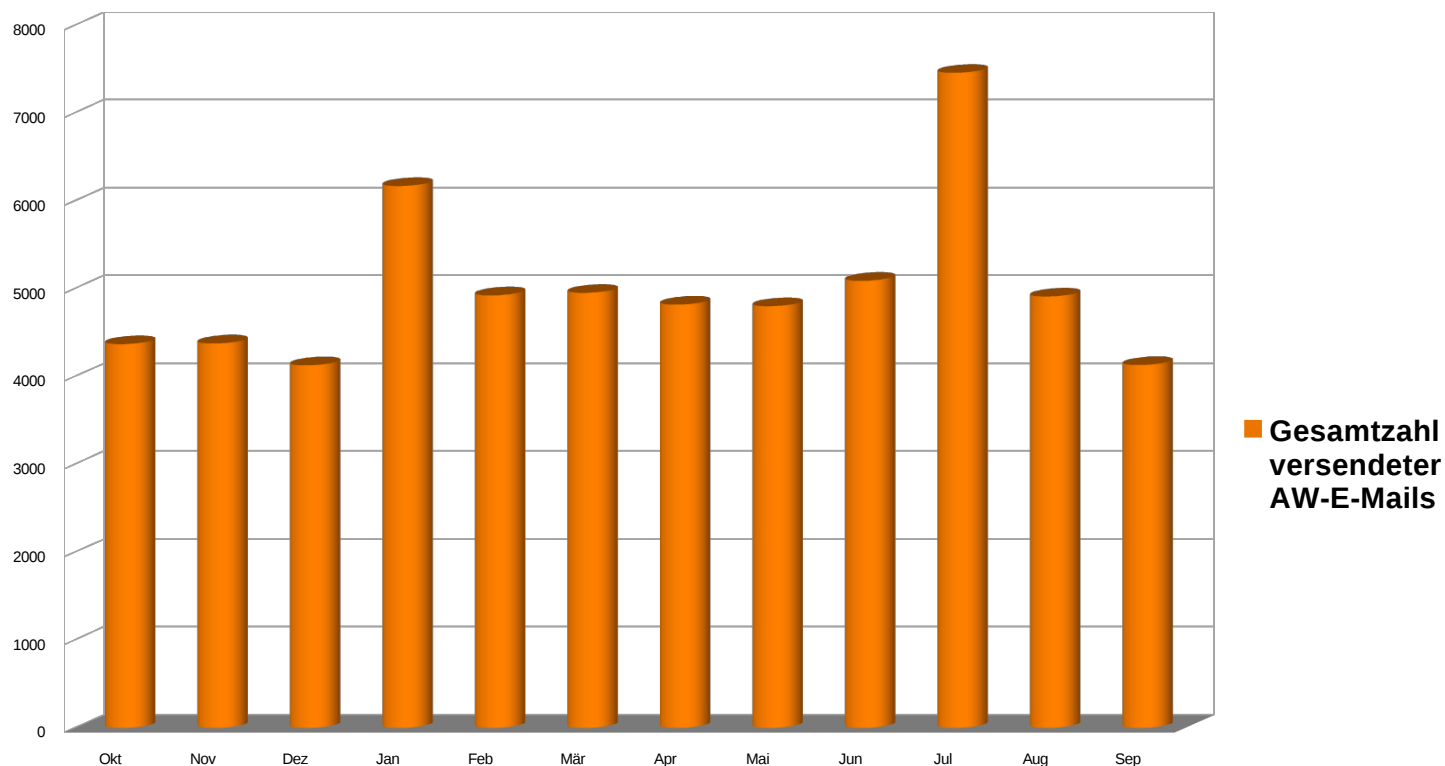
AW-Meldungen

Automatische Warnmeldungen - Events



- ▶ Die Statistik erfasst Eingangsdaten aus Datenzulieferungen, eigener Sensorik und der Logdatenanalyse.
- ▶ Im September zwei Wochen keine Daten von Shadowserver.
- ▶ Externe Zulieferungen umfassten Informationen zu Systemen, die sich auf teilw. aktiv ausgenutzte Schwachstellen beziehen (z. B. CVE-2025-53786 (MS Exchange), CVE-2025-5777, CVE-2025-6543, CVE-2025-7775 (Citrix NetScaler)). Sofern betroffene Systeme offen aus dem Netz erreichbar sind werden sie über die Warnmeldungskategorie 'Vulnerability/HTTP' gemeldet.

Automatische Warnmeldungen - E-Mails



- ▶ Deutlich sichtbar die ‚Inventarscans‘ im Januar und Juli
- ▶ Der größte Meldungsanteil im Juli mit gut 28% der Meldungen entfällt auf die Kategorie ‚Unrestricted Access‘
- ▶ Die Inventarscans sorgten weiterhin für Anstiege in den Kategorien ‚Amplifier‘, ‚Unencrypted Communication‘ und ‚Unsafe Cryptography‘

AW-Meldungen - Vorfälle

► Dauerbrenner weiterhin

- ▷ Kompromittierte Accounts über die Spam versendet wird und/oder Phishing-Kampagnen stattfinden.

► Netflowanalyse

- ▷ Von Einrichtungen gemeldete maliziöse IP-Adressen, die über unsere Netflowanalyse zu Hinweisen an andere Teilnehmer führten.

► Erwähnenswert

- ▷ Im April dominierte mit ca. 41% die Kategorie 'Access Domains' (65144 Events) die AW-Meldungen, die bei geblockten Domains im Kontext von DNS-RPZ ausgelöst werden. Die hohe Anzahl von Events ist auf eine größere Phishing-Kampagne gegen eine Einrichtung sowie eine durchgeführte Analyse der betroffenen Einrichtung zurückzuführen.
- ▷ Im Mai wurde im Zuge einer koordinierten Aktion internationaler Strafverfolgungsbehörden genannt "Operation Endgame 2.0" eine Botnet-Infrastruktur von Cyberkriminellen übernommen sowie deren Betreiber festgenommen. Dabei wurden gestohlene Anmeldedaten sichergestellt und über Spamhaus verteilt. Die Anmeldedaten konnten 24 Einrichtungen zugeordnet und an diese weitergeleitet werden.

Lageberichte

- ▶ Für Teilnehmer am Dienst DFN-Security verfügbar
- ▶ Für Sicherheitskontakte beim jeweiligen Teilnehmer (CISO, Adminstrierende von Netzbereichen, u. ä.)
- ▶ Die Berichte sind **nicht** öffentlich
- ▶ Einstufung nach dem Traffic Light Protocol (TLP)
 - ▷ TLP:CLEAR: Unbegrenzte Weitergabe
 - ▷ **TLP:GREEN**: Organisationsübergreifende Weitergabe
 - ▷ TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe
 - ▷ TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe
 - ▷ TLP:RED: Persönlich, nur für benannte Empfänger

- ▶ Verteilung mittlerweile über Mailingliste
- ▶ <https://www.listserv.dfn.de/sympa/info/dfn-cert-lageberichte>
- ▶ Berechtigung zum Erhalt der Berichte wird geprüft, bevor eine Abonnementwunsch akzeptiert wird
- ▶ Seit Mitte des Jahres monatliche Berichterstellung
- ▶ Aktuell umfasst der Bericht drei Blöcke
 - ▷ Informationen zu ausgewählten Schwachstellen
 - ▷ Erkenntnisse aus der Vorfallsbearbeitung
 - ▷ Kennzahlen
- ▶ Kontinuierliche Weiterentwicklung der Berichte

- ▶ 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 Meldungen aus dem Bereich ‚Politik & Öffentlichkeit‘

BSI Lagebericht – in Vorbereitung

- ▶ Es wird eine neue Mailingliste für den Erhalt der BSI Lageberichte eingerichtet
- ▶ Nur Informationen, die nach dem Traffic Light Protocol (TLP) als TLP:GREEN oder niedriger eingestuft sind, werden weitergegeben
- ▶ Diese Berichte sind **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
 - ▷ ...
- ▶ Wann? Noch in diesem Jahr.

Ankündigungen

Ankündigungen

- ▶ Informationsveranstaltung DFN-Security
 - ▷ Nächster Termin: 11. Dezember ab 09:30
 - ▷ Agenda wird im Laufe des Monats erstellt
 - ▷ Vorstellung der Dienstbestandteile, Security-Portal, ...

- ▶ MISP-Schulung – noch nicht terminiert, wahrscheinlich noch in diesem Jahr
 - ▷ Wir betreiben derzeit für unsere Arbeit eine Malware Information Sharing Platform (MISP)
 - ▷ Diese wird für das Teilen von Informationen mit DFN-Teilnehmer vorbereitet
 - ▷ Ob mit eigenem MISP-Server oder einem Account auf unserem Server, Basiskenntnis über MISP ist zur erfolgreichen Nutzung erforderlich
 - ▷ Wird organisiert von den Kollegen des Cyber Threat Intelligence Teams → Stefan Kelm

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/>

