DFN CERT

deutsches forschungsnetz

Neues aus dem DFN-CERT

78. Betriebstagung | 28.03.2023

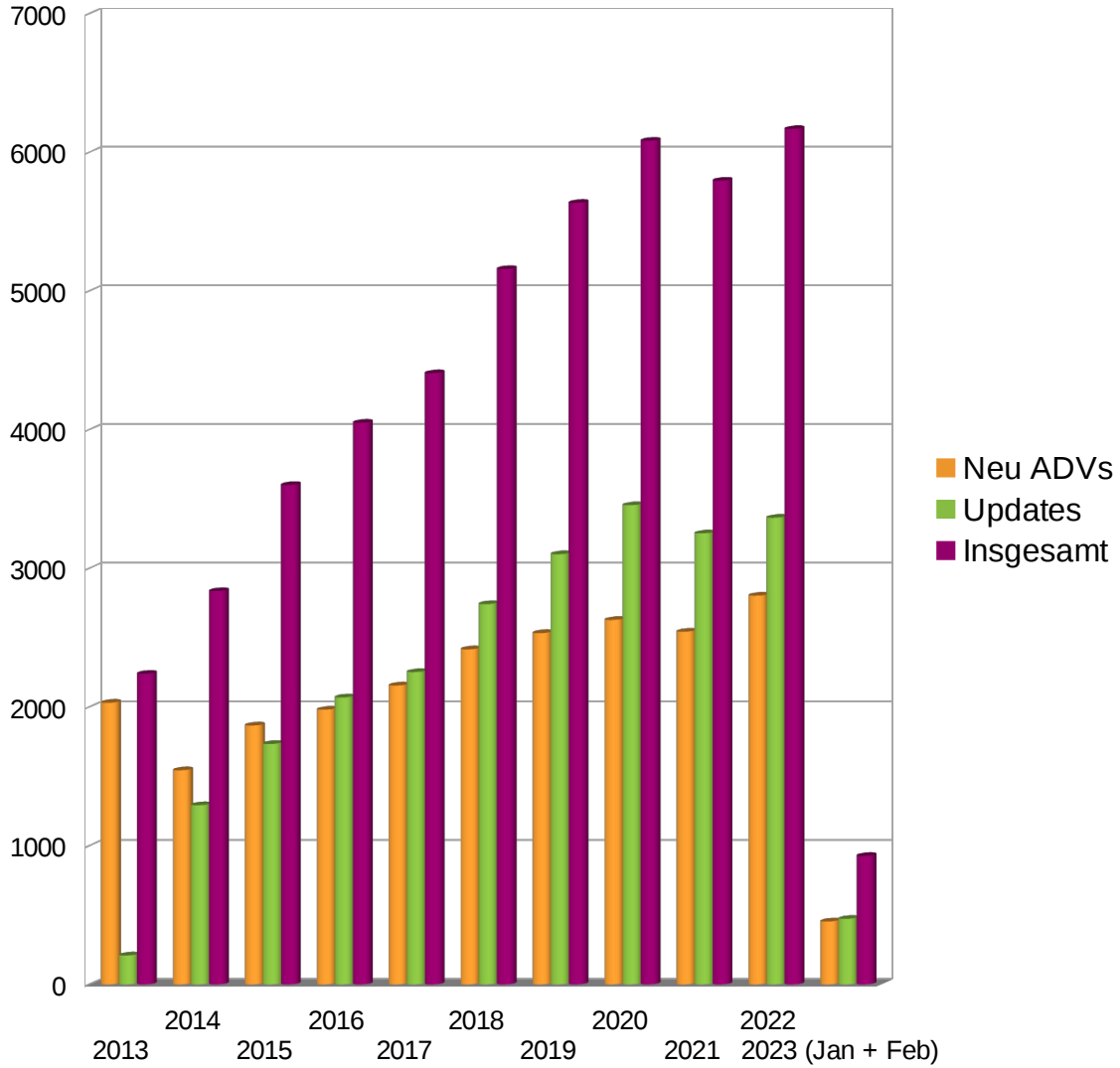
Christine Kahl

Agenda

1. Advisory Statistik
2. Automatische Warnmeldungen
3. Vorfälle – richtig übel und richtig viele
4. Security Operations

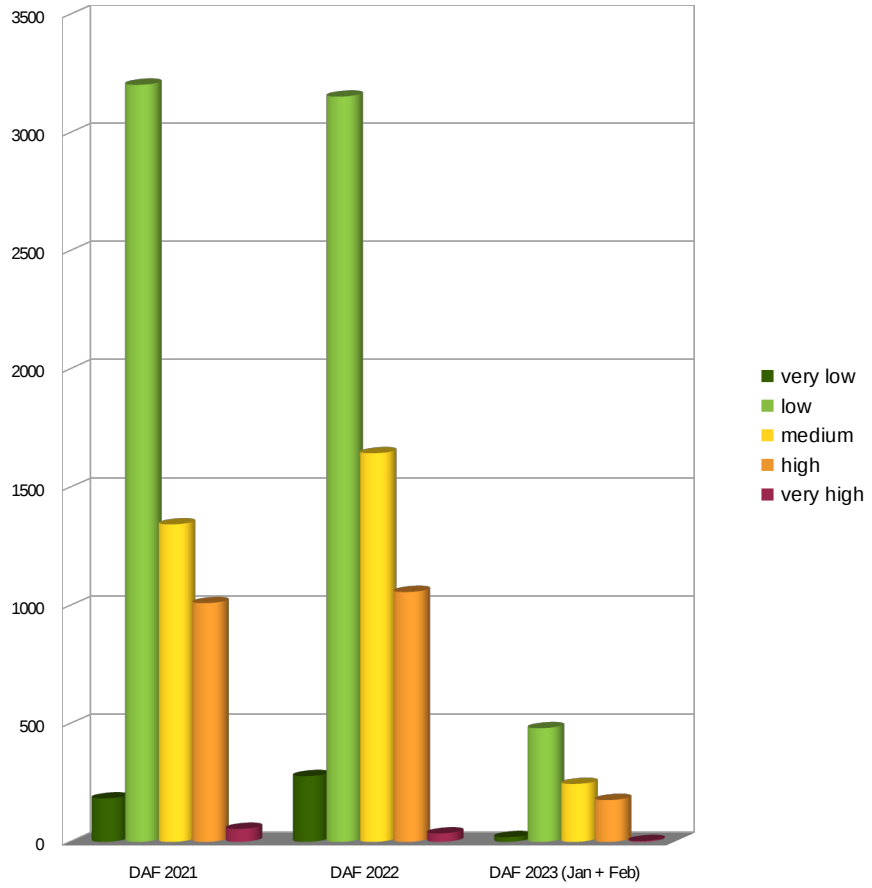
Advisory Statistik

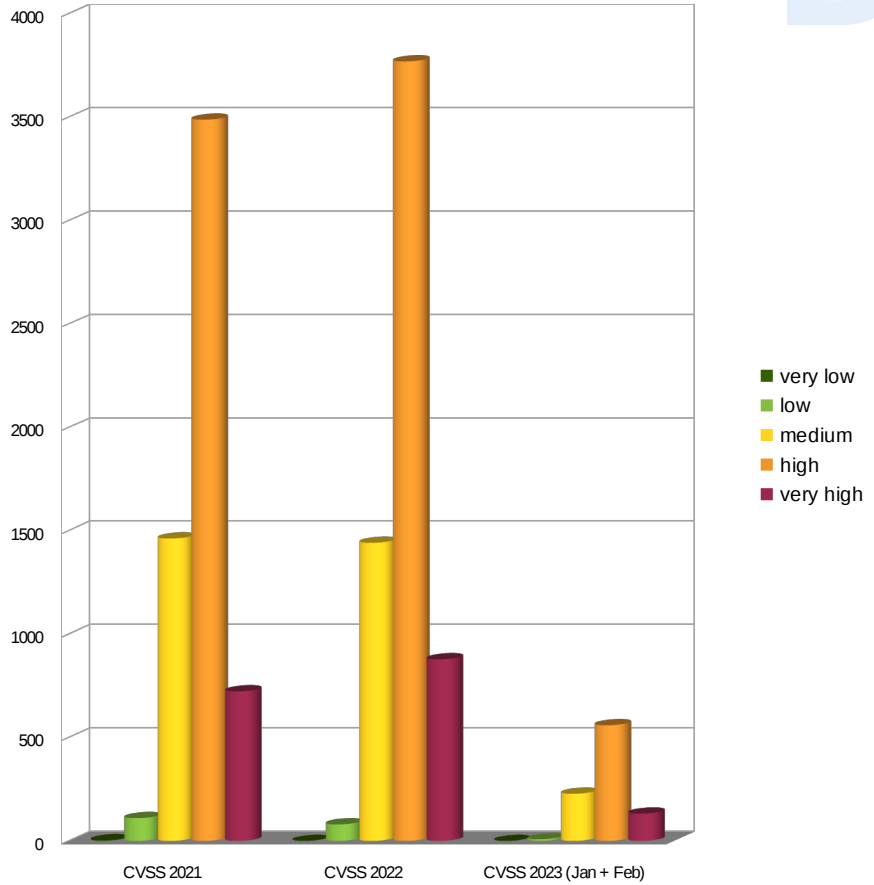
Aktuelle Advisory Zahlen



- Gesamtzahlen
  - 2013: 2240
  - 2020: 6083 (Anstieg um ~8%)
  - 2021: 5795 (Rückgang um ~5%)
  - 2022: 6168 (Anstieg um gut 6%)
- Prognose 2023
  - Zahlen entsprechen bisher ziemlich denen von 2022

ADVs nach Schweregrad – DAF – CVSS



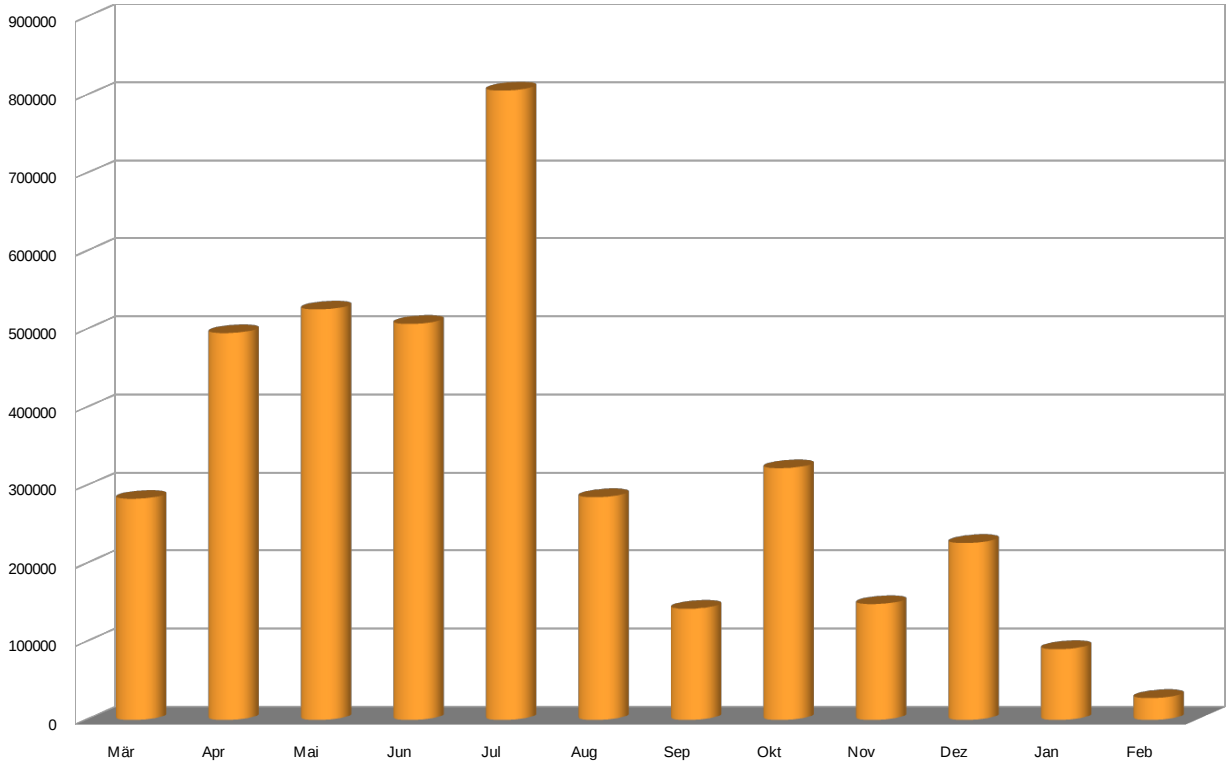


DAF und CVSS seit 2021:

- DAF und CVSS für sich betrachtet: Keine hervortretenden Änderungen
- DAF und CVSS zueinander: Die Diskrepanz zwischen den Volumina im Bereich von ‚very high' wird größer, da DAF dort noch weniger (trotz gestiegener Meldungszahlen) und CVSS mehr (stärker Anstieg als nach dem Plus der Meldungszahlen) einordnet

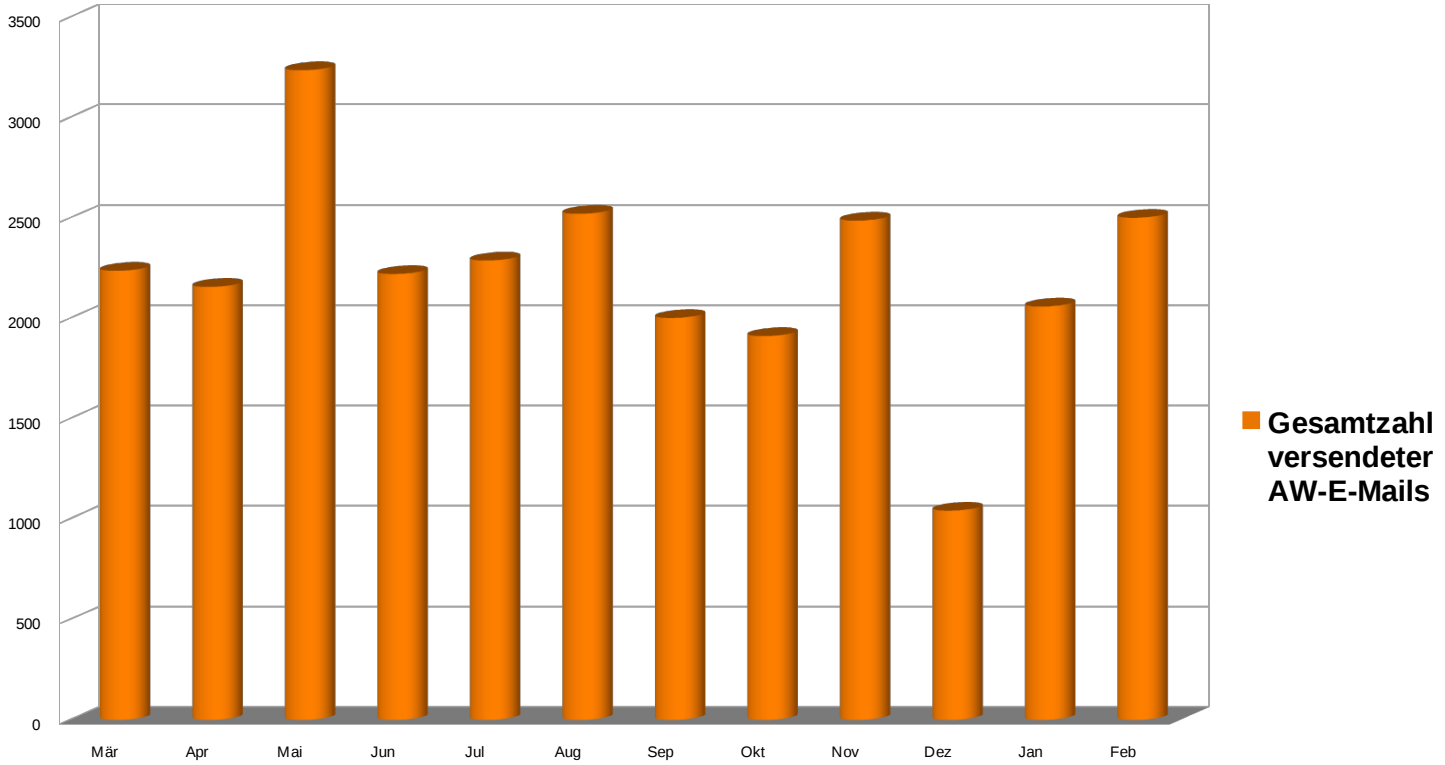
AW-Meldungen

Automatische Warnmeldungen - Events



- Im Oktober stieg die Anzahl ausgelieferter Events im Vergleich zum Vormonat wieder deutlich → erhöhte Scan-Aktivitäten (wie im Juli)
- Zusätzlich wurden im Oktober Informationen zu Verwundbarkeiten bzgl. zweier Zero-Day-Schwachstellen in MS Exchange und einer aktiv ausgenutzten Schwachstelle in der Zimbra E-Mail-Software verteilt
- Der Rückgang ausgelieferter Daten im November → Rückgang der Scans → alle anderen Kategorien verzeichnen Zuwächse, insbesondere Vorfälle im Bereich ‚Bot' zum Vormonat vervierfacht
- Bereinigt man die Dezember-Zahlen um Veränderungen im Scan-Bereich ergeben sich wenig Änderungen zum Vormonat
- Der Rückgang versendeter E-Mails im Dezember → leider nur ein Problem bei der Datenverteilung

Automatische Warnmeldungen - E-Mails



- Im Januar sank die Anzahl exportierter Events aufgrund der Deaktivierung der Weitergabe von hochfrequent scannenden Systemen → (in Absprache mit den hauptsächlich Betroffenen), geringer Mehrwert der Informationen, nehmen aber den Blick auf das Wesentliche
- Wesentlich sind u. a. Kommunikationsversuche zu C&C-Servern über die durch die Verfügbarkeit neuer Datenquellen (begrenzte Anzahl Flows) im Kontext des SecOps-Projektes seit Januar informiert wird
- Im Februar gab es eine bemerkenswert geringe Anzahl von Scans, Anstiege ergaben sich im Bereich ‚Amplifier', ‚Unrestricted Access' und ‚Vulnerability'

Vorfälle – richtig übel und richtig viele

Vorfälle – richtig übel und richtig viele

- Ende 2022 und Anfang 2023 Häufung von größeren Sicherheitsvorfällen
- In gut zwei Monaten, zehn größere Vorfälle mit zum Teil verheerenden Folgen für die betroffenen Einrichtungen
  - Royal Ransomware
  - Vice Society – scheinbar besonderes Interesse am Bildungssektor
  - Gezielte Datenexfiltration und Verschlüsselung von Backups
  - Erpresst wird, wer erpresst werden kann
- Initialer Zugang häufig über kompromittierte Anmeldeinformationen, aber auch über die Ausnutzung bekannter Schwachstellen
- Wenn Sie noch Argumente suchen, warum Investitionen in
  - Prävention und
  - Reaktion auf Sicherheitsmeldungen

notwendig sind: Es sind diese Zahlen und u. a. diese Akteure!

Vorfälle – richtig übel und richtig viele

- Und selbst wenn Sie richtig gut im Bereich Sicherheit aufgestellt sind: Bereiten Sie sich darauf vor ein Opfer zu werden.
  - Dessen Kommunikationsinfrastruktur wegbricht
  - Von dem jeder wissen will was los ist
  - …
- Stichwort: Notfallmanagement
- Wenn Sie dafür Pläne aufstellen, vergessen Sie nicht:
  - -1: Nicht in Panik verfallen
  - 0: Kontakt zum DFN-CERT aufnehmen
  - 1: Chef informieren
  - 2: ...

Security Operations

Basisleistungen: Logdateneinlieferung

- Technisch: System ist in Betrieb
  - Limit: 1.000 Logzeilen pro Sekunde
- Unterstützung für die Dateneinlieferung: SOC-Connector
- Vertraglich
  - DFN-Rahmenvertrag
  - Dienstvereinbarung DFN.Security
  - Rahmen-Auftragsverarbeitungsvereinbarung
  - Anhang DFN.Security

DFN.Security Online Informationsveranstaltung am 14.04.23 9:30 – 12:30

Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie Fragen?

- DFN-CERT Hotline
  - cert@dfn-cert.de
  - 040 / 808 077-590
- Weitere Informationen: https://www.cert.dfn.de/