DFN CERT

deutsches forschungsnetz

Neues aus dem DFN-CERT

79. Betriebstagung | 17.10.2023

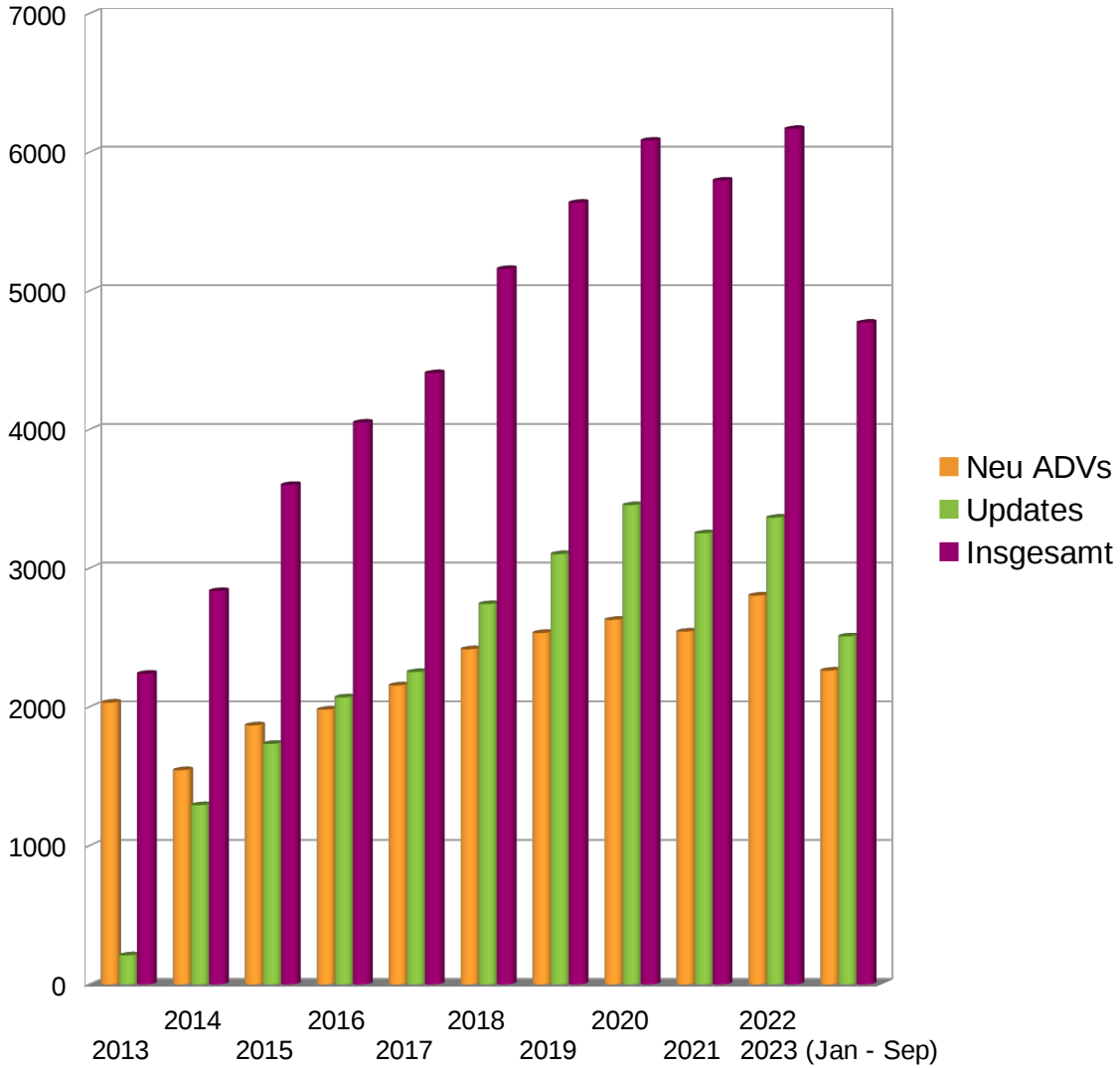
Christine Kahl

Agenda

1. Advisory Statistik
2. Schwachstellen
3. Automatische Warnmeldungen
4. Vorfälle
5. Security Operations

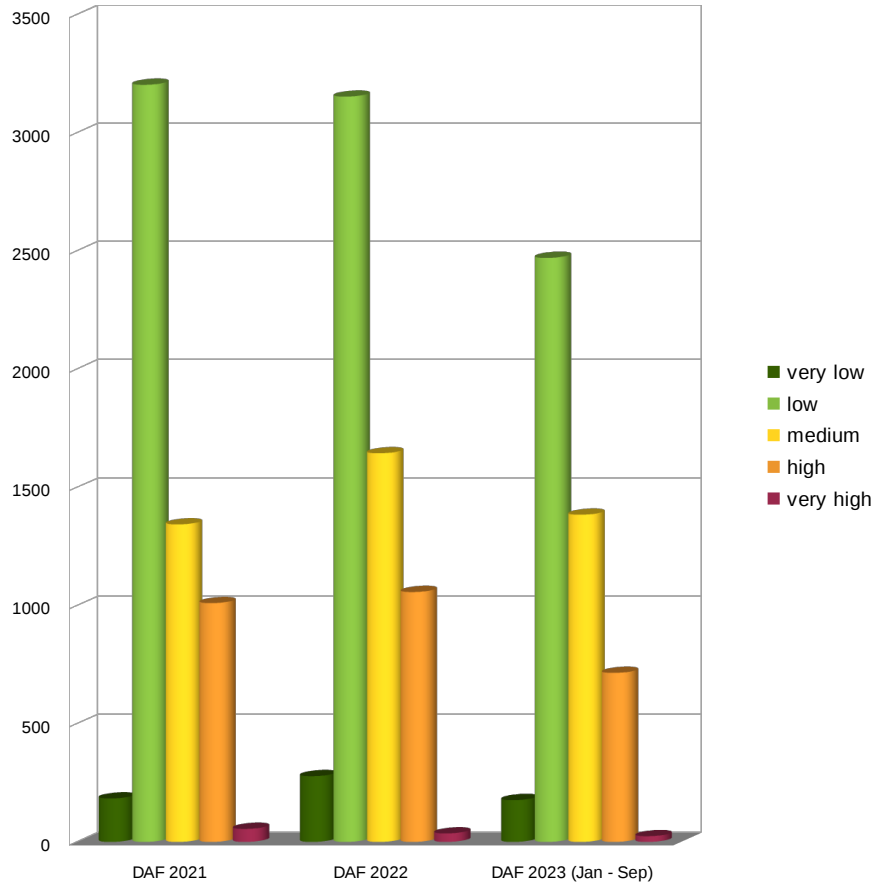
Advisory Statistik

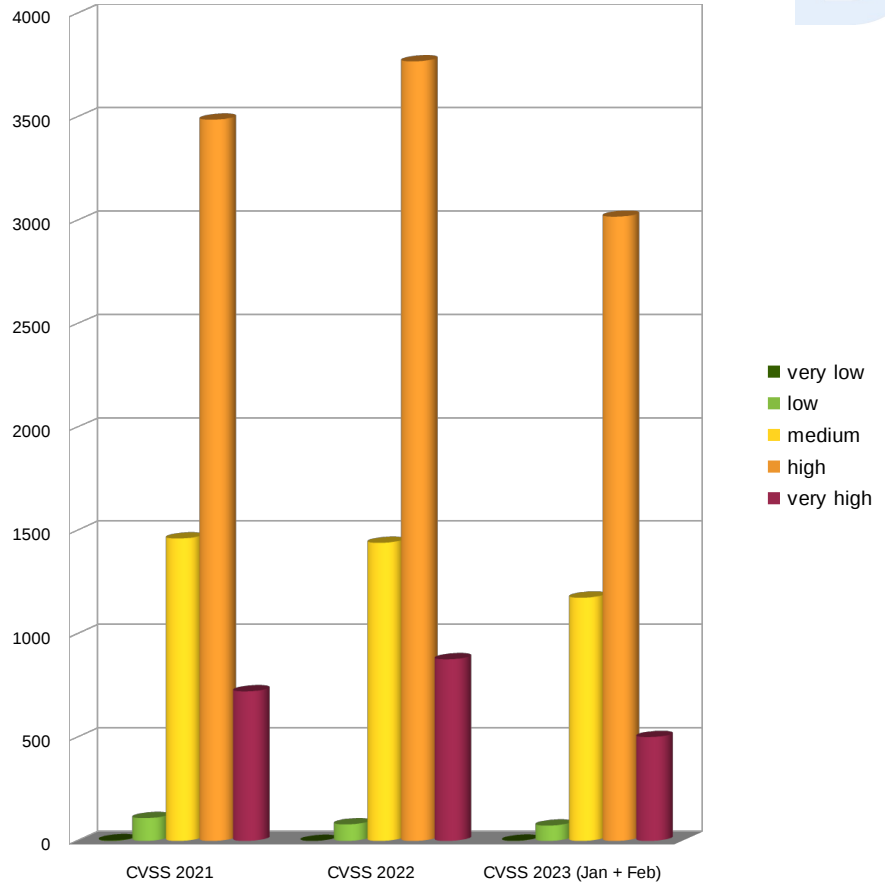
Aktuelle Advisory Zahlen



- Gesamtzahlen
  - 2013: 2240
  - 2023: Hochrechnung 6360
- In 10 Jahren
  - Über den Daumen: Verdreifachung der Meldungszahlen
  - Geschätzt 1000 Meldungen durch neue Produkte, Rest ist Anstieg im Bereich der unterstützten Systeme
  - Kein Ende / keine Umkehr des Trends zu erkennen: Denken Sie über Automatisierungen nach

ADVs nach Schweregrad – DAF – CVSS



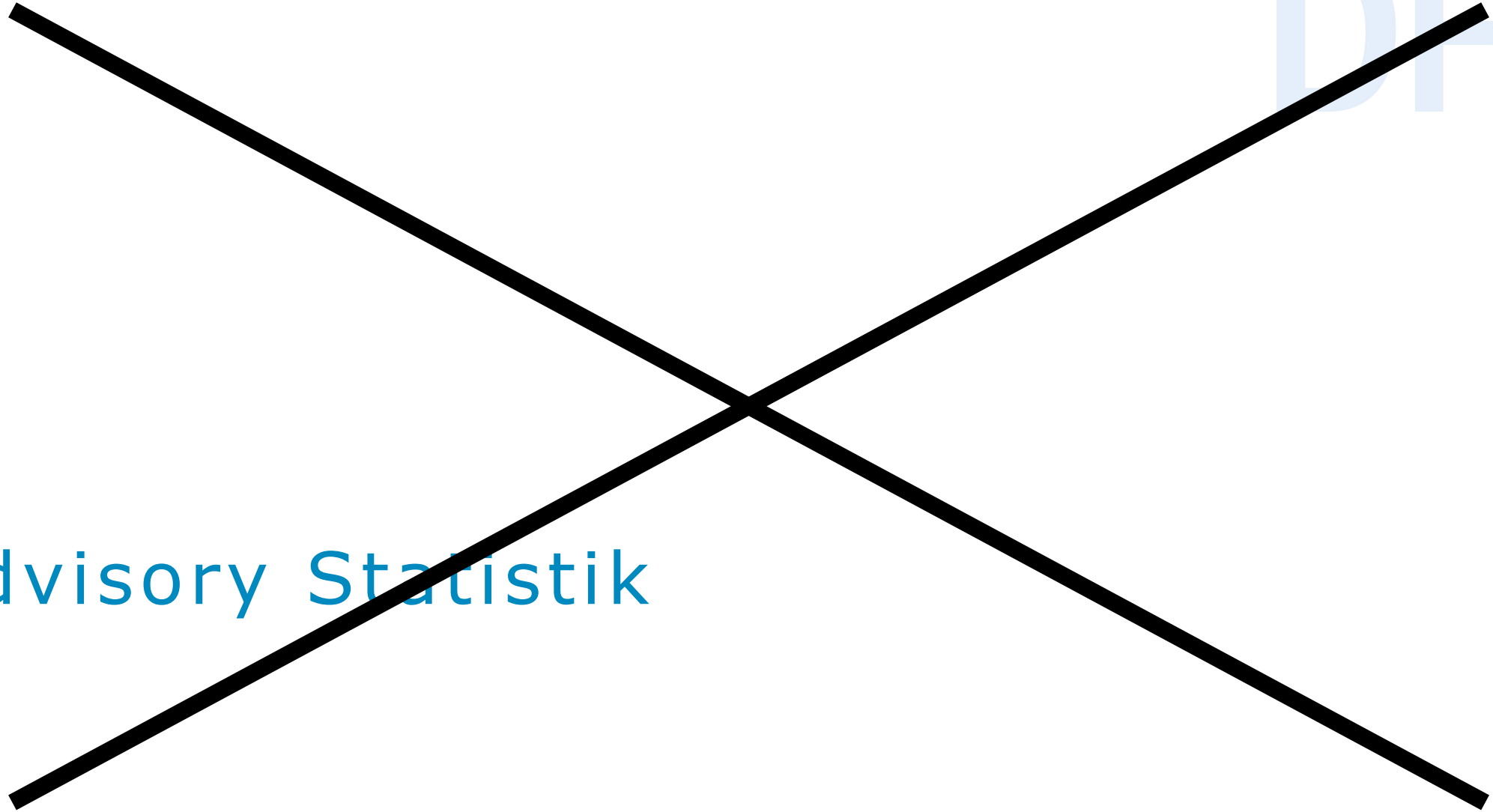


DAF und CVSS seit 2021:

- Keine bemerkenswerten Verschiebungen, gleichbleibende Unterschiede in den Bewertungen
- DAF ist tot, es lebe CVSS. Aktuell ist CVSS 3.1 und wird von uns in den Meldungen genutzt.
- CVSS 4.0 war für knapp 2 Monate kommentierbar (Juni + Juli) und soll Ende Oktober veröffentlicht werden.

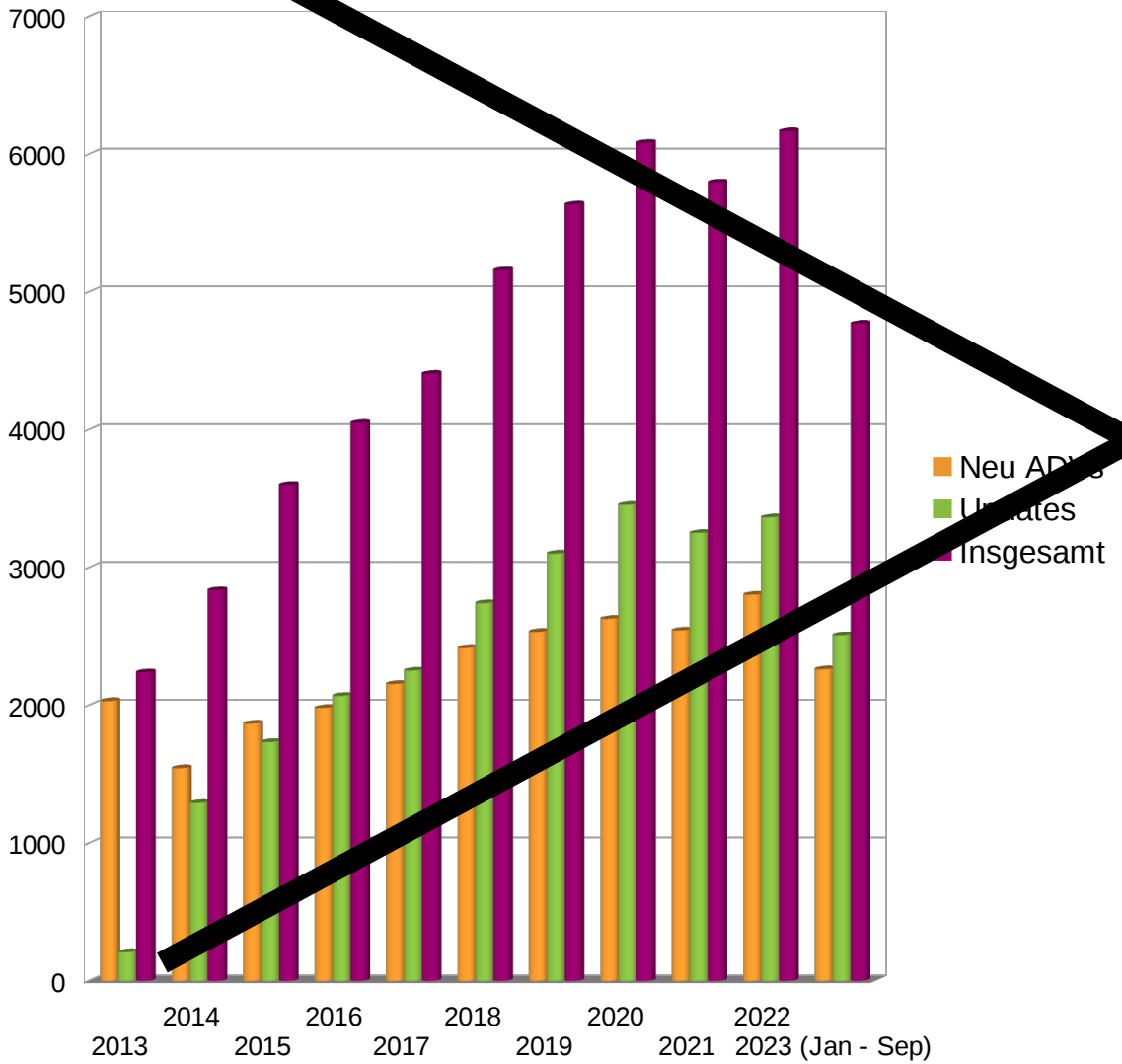
Agenda

1. Advisory Statistik
2. Schwachstellen
3. Automatische Warnmeldungen
4. Vorfälle
5. Security Operations



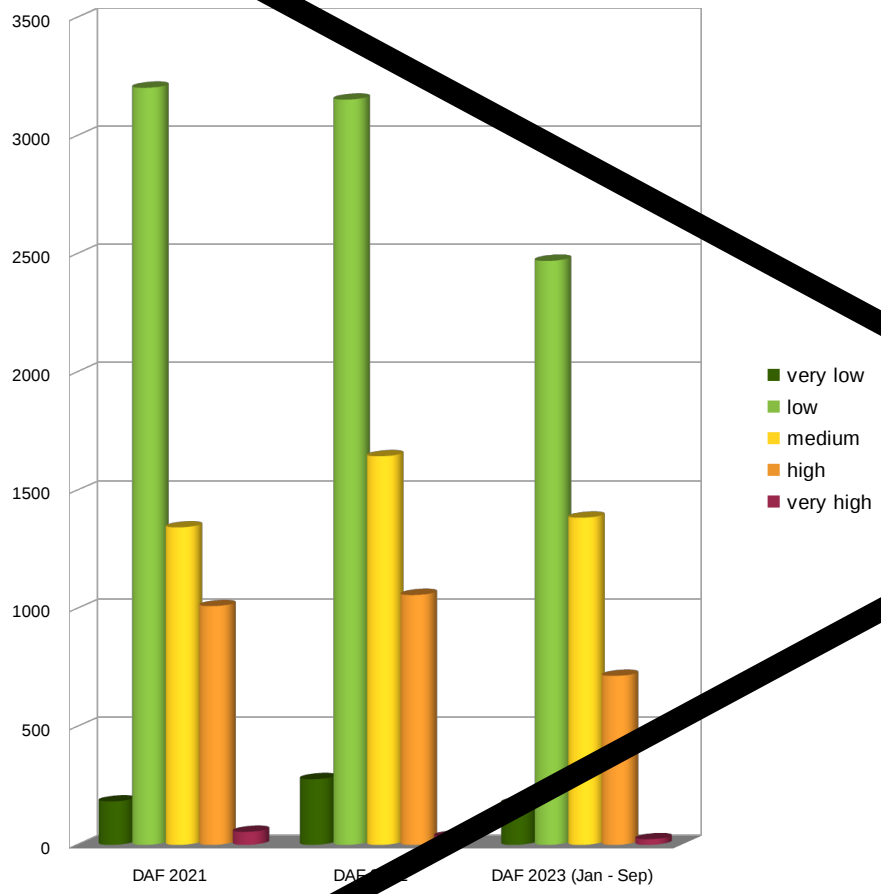
Advisory Statistik

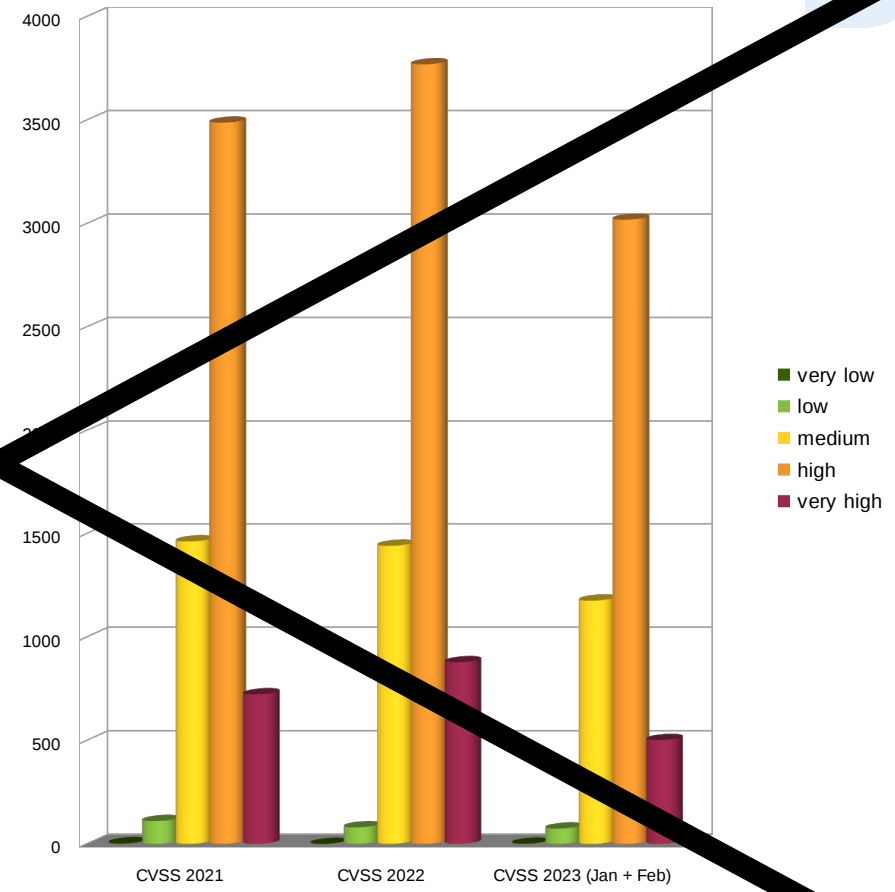
Aktuelle Advisory Zahlen



- Gesamtzahlen
  - 2013: 2240
  - 2023: Hochrechnung 6360
- In 10 Jahren
  - Über den Daumen: Verdreifachung der Meldungszahlen
  - Geschätzt 1000 Meldungen durch neue Produkte, Rest ist Anstieg im Bereich der unterstützten Systeme
  - Kein Ende / keine Umkehr des Trends zu erkennen: Denken Sie über Automatisierungen nach

ADVs nach Schweregrad – DAF – CVSS





DAF und CVSS seit 2021:

- Keine bemerkenswerten Verschiebungen, gleichbleibende Unterschiede in den Bewertungen
- DAF ist tot, es lebe CVSS. Aktuell ist CVSS 3.1 und wird von uns in den Meldungen genutzt.
- CVSS 4.0 war für knapp 2 Monate kommentierbar (Juni + Juli) und soll Ende Oktober veröffentlicht werden.

Lassen Sie uns mal Tacheles reden.

Wir haben ein Problem!

In Form von 19 größeren Vorfällen im letzten Jahr.

19 ist nicht nur eine Zahl, sondern steht für:

- XX1
- XX2
- XX3
- XX4
- XX5
- XX6
- XX7
- XX8
- XX9
- XX10
- XX11
- XX12
- XX13
- XX14
- XX15
- XX16
- XX17
- XX18
- XX19
- **Bitte kein weiterer Eintrag!**

Unsere Unterstützung durch DFN.Security

DFN.Security

- Schwachstellenmeldungen > 6000 pro Jahr
  - Windows, Red Hat, SUSE, Oracle, Juniper, Cisco usw.
  - Aufbereitung zur schnellen Verarbeitung durch Sie
- Netzwerkprüfer zur Überwachung des eigenen Netzes auf offen erreichbare Dienste
- Gezielte Überwachung ausgewählter Server durch ein aktives Dienstemonitoring
- DoS-Basisschutz
- Automatische Warnmeldungen
  - IP-Adress-basiert und Domain-basiert
  - Zustellung an definierte Kontakte
  - Aggregation eingesammelter Daten und kontinuierliche Anpassung an aktuelle Entwicklungen

DFN.Security - Logdatenanalyse

- Usecases für Windows- und Linux-Systeme
- Basisleistungen
  - Definierte Einlieferungswege, https://www.dfn-cert.de/leistungen/secops.html
  - Limitierung auf 1tsd Zeilen pro Sekunde
  - Keine zusätzlichen Kosten!
- Erweiterte Leistungen
  - Dateneinlieferung ensprechend Ihrer Bedürfnisse
  - Kein definiertes Limit für das Datenvolumen
  - Überschaubare zusätzliche Kosten, festgelegt über die Mitgliederversammlung
  - Möglichkeit der Einflußnahme auf die Weiterentwicklung des Dienstes

DFN.Security – aktuelle Daten

- Seit Mitte letzten Jahres haben wir ein eigenes Team (CTI = Cyber Threat Intelligence), dass sich mit der Beschaffung aktueller Daten befasst:
  - Laufende Angriffswellen
  - Aktuelle IoCs (Indicators of Compromise)
  - Datenveröffentlichungen aus Angriffen ...
- Geschwindigkeit ist ein wichtiger Faktor für die erfolgreiche Prävention und manche Daten sind nur kurze Zeit gültig/nutzbar

DFN.Security - **ABER**

- **Ohne Ihre Mithilfe bleiben unsere Maßnahmen wirkungslos**
- Seit Juni können die Verträge für die DFN.Security Basisleistungen oder erweiterten Leistungen geschlossen werden, Stand eingegangene Verträge am 13.10.23:
  - Basisleistungen: 17
  - Erweiterte Leistungen: 2
- Lassen Sie die vornehme Zurückhaltung fallen und schließen Sie zumindest den Vertrag für die Basisleistungen ab!
- Sorgen Sie dafür, dass Sie Zugang zum DFN.Security-Portal haben und dass in diesem aktuelle Kontaktinformationen von Ihnen hinterlegt sind
- Fragen zur Portalnutzung? → 5 freie Plätze für das morgige Training von 14:30 – 16:30 Uhr

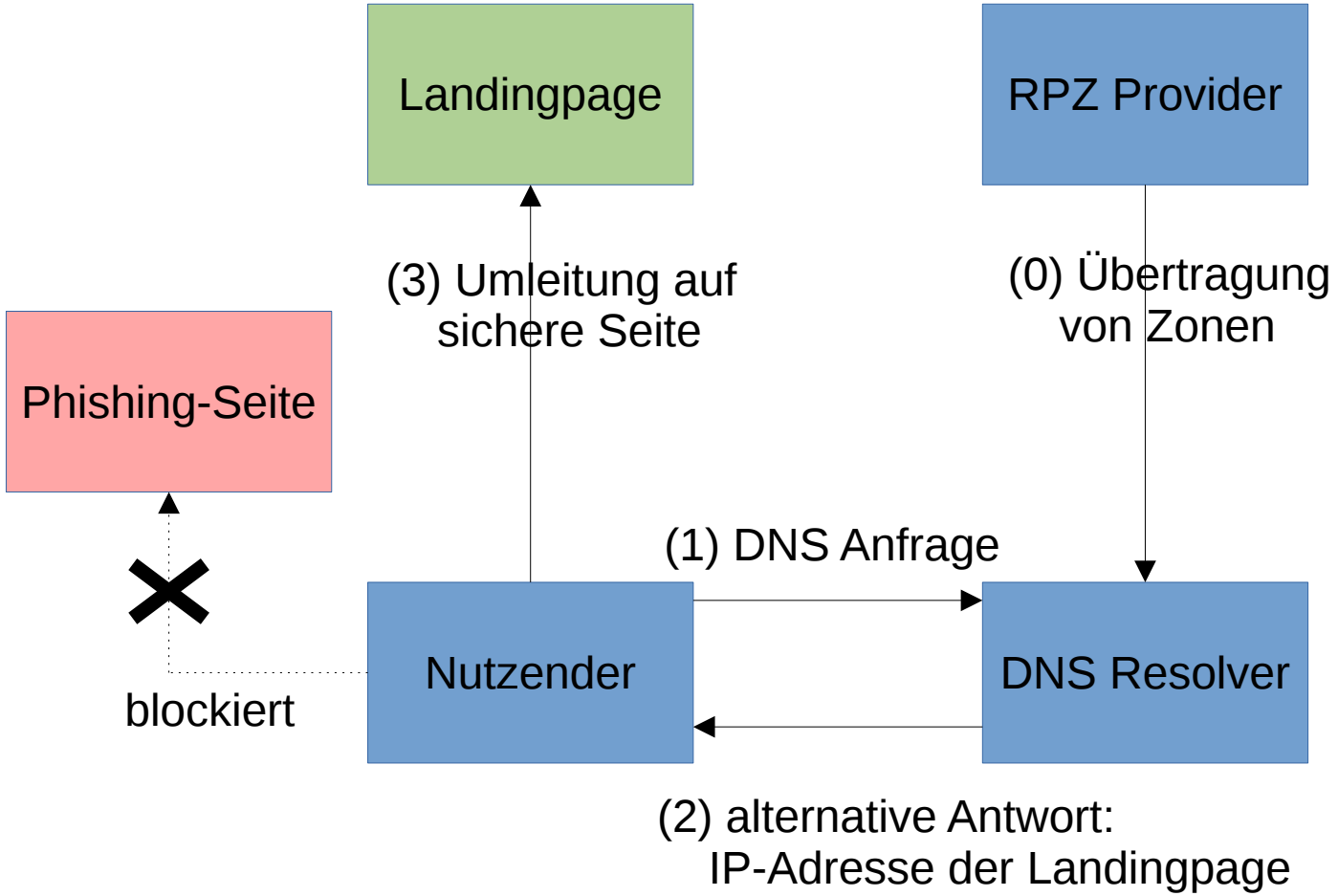
DFN.Security – Beachtenswertes

- Wir versuchen alle Erweiterungen des Dienstens allen Teilnehmern zur Verfügung zu stellen, aber es gibt Kostentreiber (HW + manuelle Aufwände), die uns limitieren, darum stehen manche Dienstmerkmale nur oder zunächst in den erweiterten Leistungen bereit.
- Wenn Sie Kollegen haben, die für die Beschaffung zuständig sind und nicht ausreichend über den Dienst informiert sind oder Sie selbst noch nicht genug wissen: Kein Problem!
  - Nächste Informationsveranstaltung am 05.12.23 in der Zeit von 9:30 – 12:30 Uhr
  - Einfach einwählen: https://dfn.zoom.us/j/66277930054?pwd=R3hnRGNPdFdaN0ZpaDFtRC9qNk1MUT09

Nächste Erweiterung: DNS-RPZ

- DNS-RPZ = Domain Name System Response Policy Zone
- Verfahren, um bei der Namensauflösung durch rekursive Resolver mittels eigener Richtlinien einzugreifen
- Letztlich dient das dazu, Zugriff auf bestimmte Domains zu unterbinden
- Aktive Gefahrenabwehr insbesondere von Phishingangriffen
- Auch hier: Die Verfügbarkeit guter und aktueller Daten ist ein entscheidendes Erfolgskriterium
- Um dieses Dienstmerkmal zügig bereitstellen zu können, kooperieren wir mit der Schweizer Stiftung SWITCH
  - Diese betreibt einen solchen Dienst seit Jahren u. a. für die Schweizer Hochschulen
  - Zunächst werden wir primär die SWITCH Zone anbieten

Nächste Erweiterung: DNS-RPZ



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/