DFN-CERT

deutsches forschungsnetz

Neues aus dem DFN-CERT

80. Betriebstagung | 19.03.2024

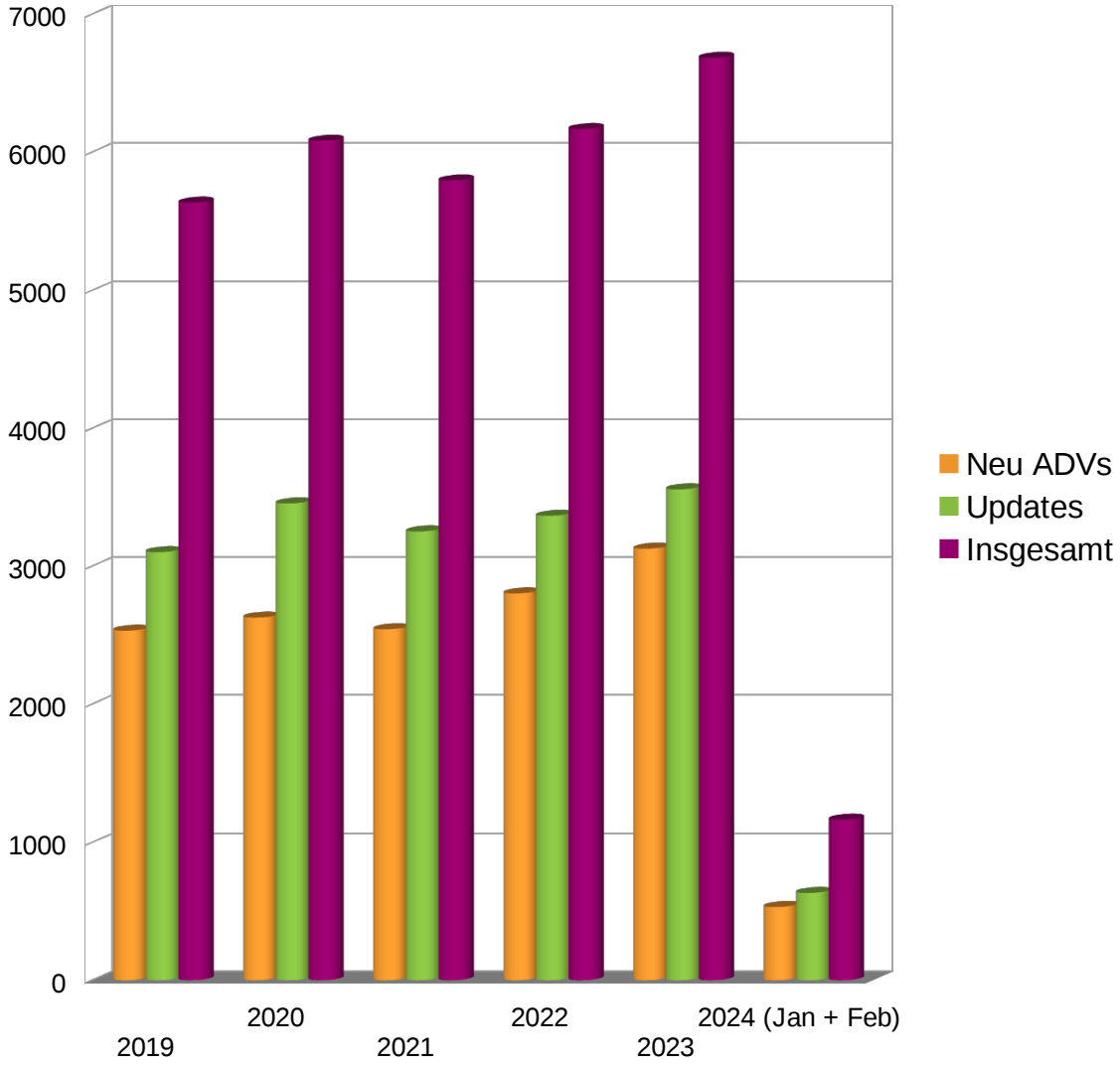
Christine Kahl

Agenda

1. Schwachstellenmeldungen
2. Ausgewählte Schwachstellen
3. Automatische Warnmeldungen
4. Logdatenanalyse
5. DNS-RPZ

Schwachstellenmeldungen

Aktuelle Advisory Zahlen



- Gesamtzahlen
  - 2019: 5635
  - 2023: 6684
  - Anstieg zum Vorjahr gute 8%
- Bei 250 Arbeitstagen sind das ~ 27 Meldungen pro Tag
- Prognose 2023
  - Weiter steigend
- Unterstützte Systeme weitgehend stabil
  - Atlassian Confluence und
  - Rocket.Chat frisch aufgenommen

Schwachstellenmeldungen verarbeiten

- Ergebnisse der Studie zur Verwendung von Security Advisories an der Friedrich-Alexander-Universität Erlangen (knapp 200 beantwortete Fragebögen, Großteil der Antwortenden kommt aus Deutschland)
  - Die meisten Teilnehmenden bekommen Sicherheitsmeldungen, die für sie nicht relevant sind
  - Viele der Probleme bei der Bearbeitung von Security Advisories können durch Vorgaben für die Struktur und Verteilungswege angegangen werden
  - Studie zielt eigentlich auf den Mehrwert von CSAF (Common Security Advisory Framework)
  - CSAF könnte einige der Probleme lösen, ist aber aktuell noch nicht bekannt oder verbreitet genug
- **ABER** auch ohne CSAF sind Optimierungen möglich:

Schwachstellenmeldungen verarbeiten

- Nutzen Sie die Filter- und Strukturierungsmöglichkeiten, die das DFN.Security-Portal liefert, z. B.
  - Richten Sie dedizierte Verteiler ein (Über: E-Mail-Kontakt anlegen),

    um nach Systemen (Plattform- oder Softwarekategorie oder CPE)

    und/oder Schweregrad (Empfehlung: CVSS) zu strukturieren (Über: Mein Profil/Kontakt bearbeiten - Abonnements)
  - Setzen Sie Präfixe für E-Mails, um richtig wichtiges schnell zu erkennen (Über: Mein Profil/Kontakt bearbeiten – E-Mail Einstellungen)
  - Hinterlegen Sie an den Systemen die genutzte Software, um Schwachstellenmeldungen den verantwortlichen Administrierenden zuzustellen (Über: Netzwerkstruktur)
- Nicht jeder Patch muss instantan installiert werden, aber manchmal kommt es auf Stunden und nicht auf Tage an

Ausgewählte Schwachstellen

Cisco mit 10

- Cisco IOS XE, CVE-2023-20198, Privilegieneskalation, 10
  - Switches und Router mit IOS XE
  - Schwachstelle in webbasierter Konfigurationsoberfläche ermöglicht vollständige Kompromittierung
- Schwachstelle war mehrere Wochen bekannt (seit mindestens 18.09.23), bevor der Hersteller ein Advisory veröffentlichte (16.10.23)
- Zunächst stellte der Hersteller nur Hinweise zur Mitigation bereit, Patches folgten erst eine Woche später
- Glimpflich davon gekommen: im DFN-Netz waren mehrere Systeme (zweistelliger Bereich) verwundbar, Hinweise auf tatsächlich Infektionen derzeit nur in zwei Fällen

Exim mit 9.8

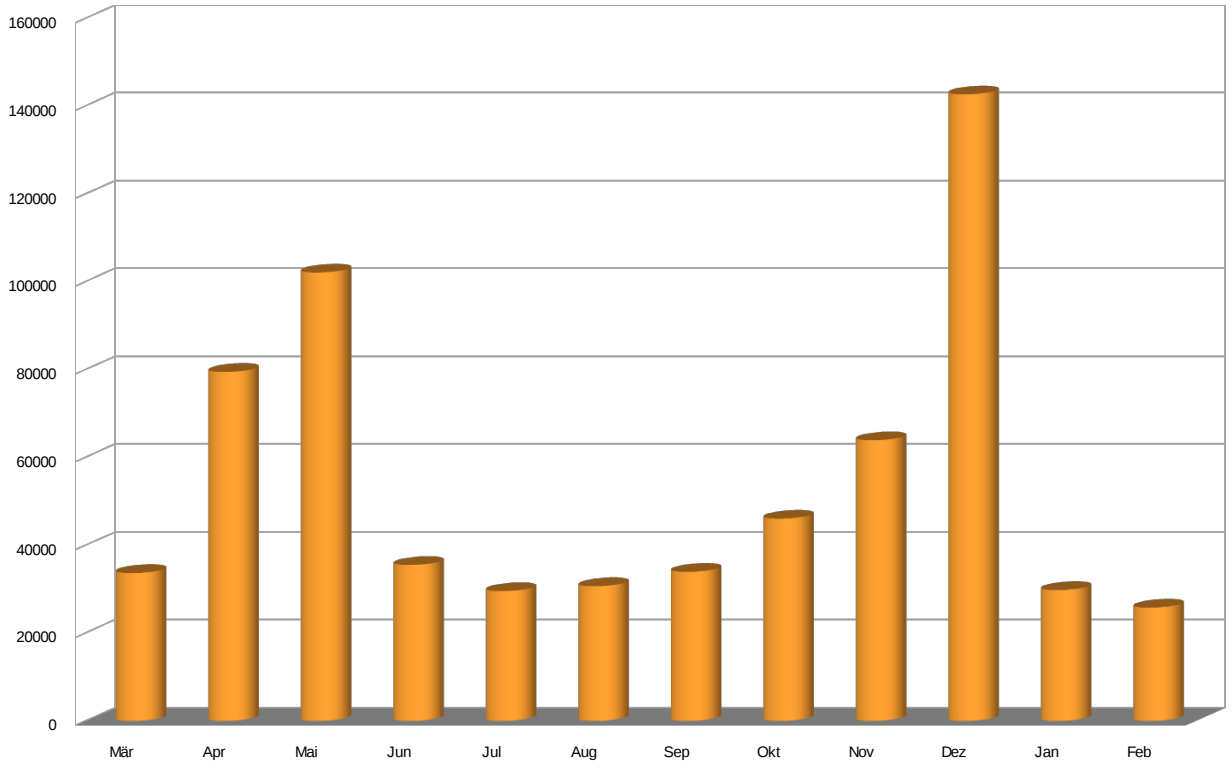
- E-Mail-Server Exim, CVE-2023-42115, RCE, 9.8
  - Schwachstelle ermöglicht das Ausführen beliebigen Programmcodes ohne Authentifizierung
  - Schadcode kann über reguläre E-Mail eingeschleust werden
- Schwachstellenbehebung erfolgte erst über 10 Monate nach dem ersten Report durch die ZDI (Zero Day Initiative), vermutlich aufgrund von Fehlern in der Kommunikation
- Nach Berichten des BSI existierten in Deutschland mehr als 100tsd verwundbare Systeme
- Konkrete Zahlen für DFN-Teilnehmer liegen uns nicht vor

Schwerwiegend und zügig ausgenutzt

- Citrix Netscaler und Gateway, CVE-2023-3519, RCE, 9.8, CVE-2023-4966, Offenlegung von Informationen, 9.4
  - Ausführen beliebigen Programmcodes und Ausspähen von Informationen ohne Authentifizierung wurde schnell von Ransomware-Gruppen ausgenutzt
  - Schwachstelle mit dem Namen ‚CitrixBleed' ermöglicht das Ausspähen von Sitzungstoken
  - Das Ausspähen der Sitzungstoken wurde als ‚It appears people are collecting session tokens like Pokemon' beschrieben
  - Mehrere Installationen im DFN verwundbar, eine Instanz gesichert kompromittiert
- Atlassian Confluence, CVE-2023-22515, Privilegieneskalation, 9.8
  - Schwachstelle ermöglicht das Anlegen von Administratorkonten ohne Authentifizierung
  - Im Netz des DFN wissen wir von vier verwundbaren Systemen

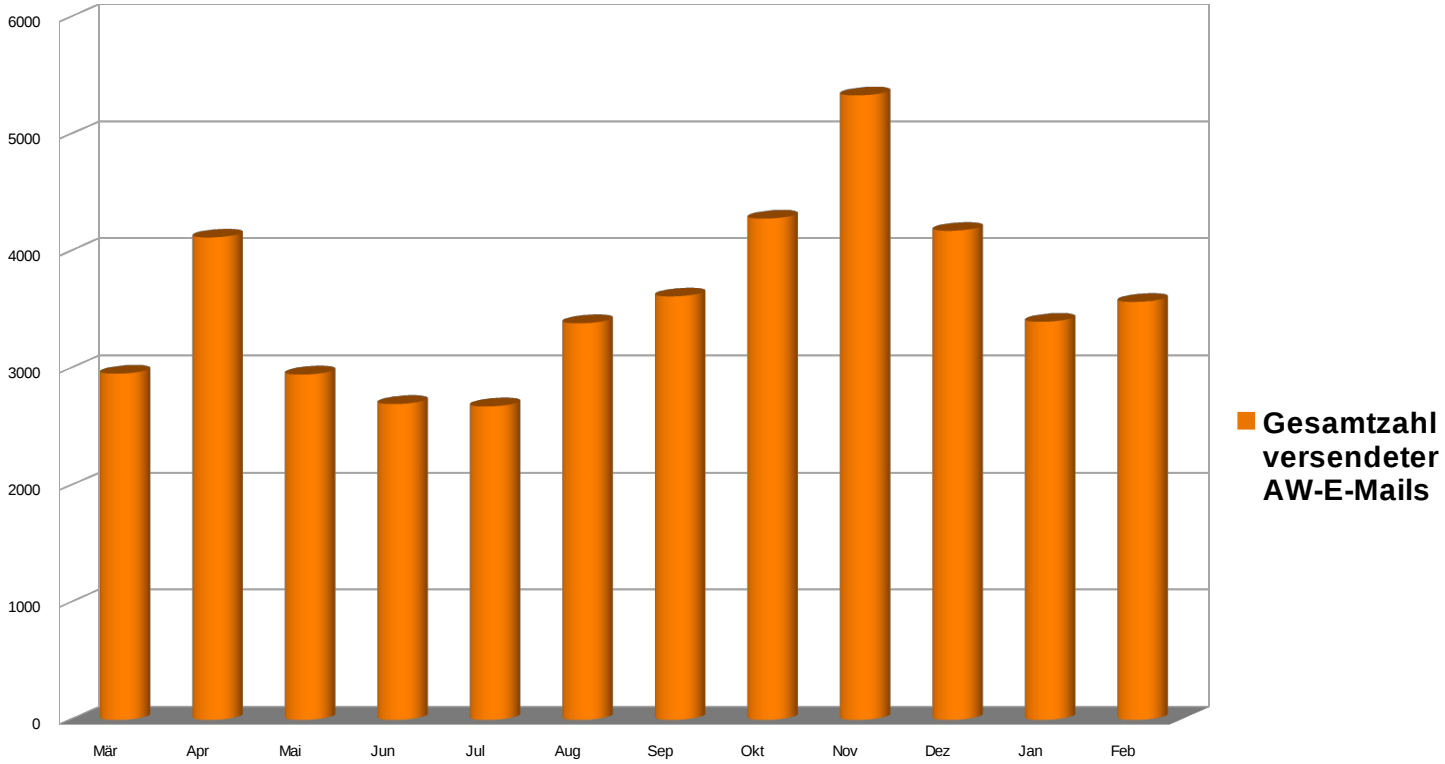
AW-Meldungen

Automatische Warnmeldungen - Events



- Im Oktober wurden drei weitere Einrichtungen Opfer größerer Sicherheitsvorfälle
- Von Mitte November bis Mitte Dezember wurden zeitlich begrenzt Warnmeldungen bestimmter Kategorien versendet, die sonst aufgrund hoher ‚false positive'-Werte oder gewünscht offener Systeme nicht weitergegeben werden
- Der Peak im Dezember lässt sich auf diese temporäre Versendung zurückführen
- Die Befürchtungen, dass das Jahresende, welches sich zumeist durch schlechte personelle Besetzung auszeichnet, besonders für Angriffe genutzt würde, bestätigte sich nicht
- Ein größerer Sicherheitsvorfall wurde im Januar, drei weitere im Februar gemeldet

Automatische Warnmeldungen - E-Mails



- Peak in den Events im Dezember zeigt sich nicht in den E-Mails, da Ursache vor allem eine Event mit vielen Treffern (Scan DDoS Middlebox) war
- Statistiken erhalten Monitoringevents und -E-Mails, aus den letztgenannten ist das Monitoring heraus gerechnet (daher Zahlen nicht exakt)
- Von November bis Januar gab es verschiedene Informationen zu RCE-, XSS-, SQL-Injection- und Open Redirect-Schwachstellen bei verschiedenen Einrichtungen vom CERT-Bund
- Im Januar gab es auch Meldungen zu Schwachstellen in Ivanti- und Cisco-Systemen vom CERT-Bund
- CERT-Bund arbeitet derzeit generell an den Reports, da sind Änderungen zu erwarten (gerne bei uns melden, wenn was nicht passt, doppelt ist o. ä.)

Logdatenanalyse

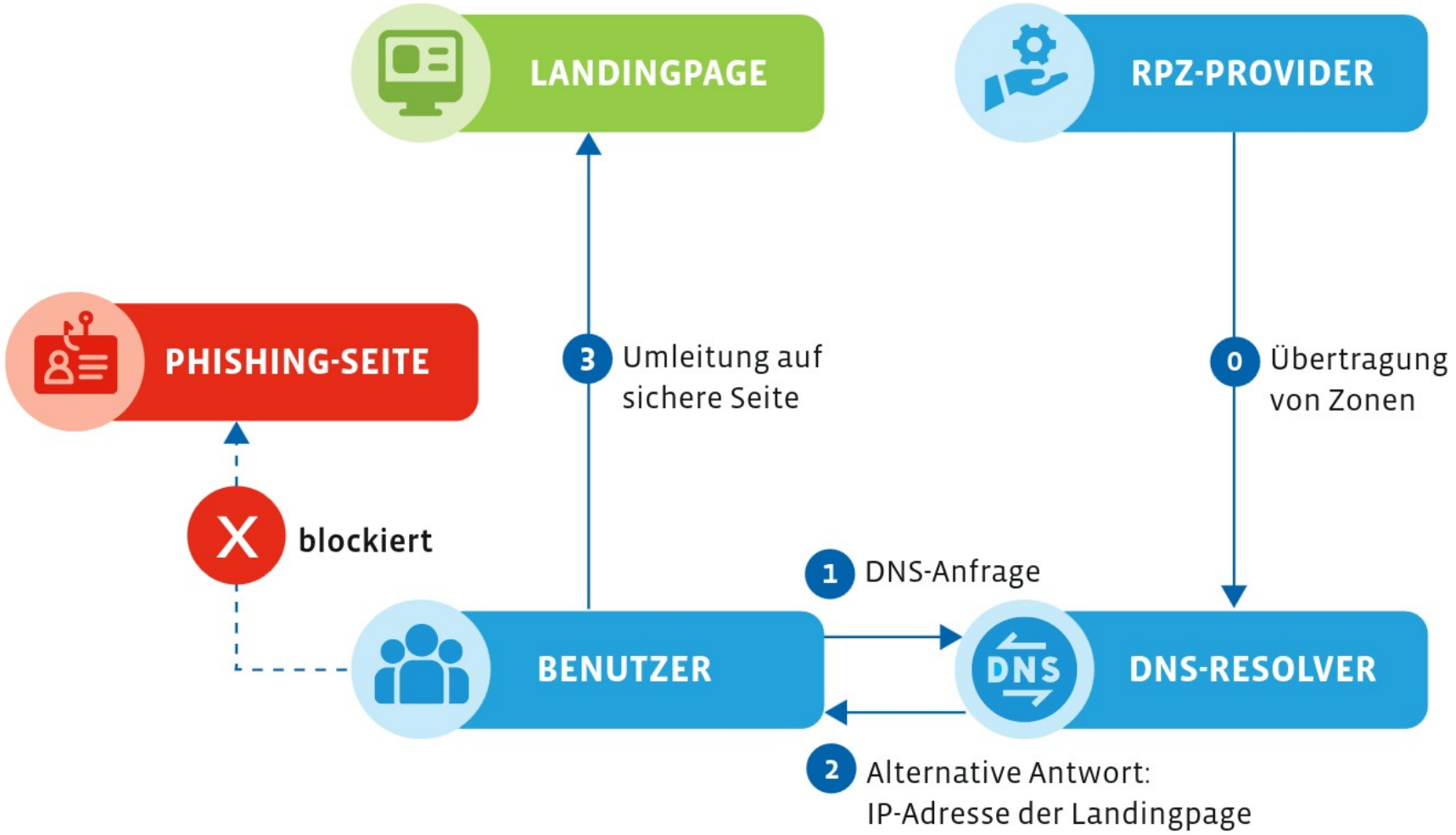
Logdatenanalyse - Status

- SOC-Connector für Linux (Webseite: https://www.dfn-cert.de/leistungen/security-operations/) und Windows (auf Anfrage) nutzbar
- Unterstützte Usecases (Webseite) und Usecases in Vorbereitung (im Zuge des Onboardings) verfügbar
- Seit Mitte Juni 2023 sind die neuen Verträge und damit die Logdatenanalyse für alle Teilnehmer im DFN erhältlich
  - ca. 60 Teilnehmer haben Verträge für Basisleistungen unterzeichnet
  - 4 Teilnehmer sind in den erweiterten Leistungen
  - Etwa gleich viele offene Anfragen existieren
- Obige Zahlen wären akzeptabel, wenn
  - Alle Teilnehmer, die die Verträge unterzeichnet haben, auch Logdaten einliefern würden
  - Und alle Teilnehmer in den Basisleistungen ihr zugesichertes Volumen ausnutzen würden

Wenn Sie weitere Dinge von uns benötigen, um diesen Dienstbestandteil zu nutzen, lassen Sie uns das wissen!

DNS-RPZ

DNS-RPZ



- Domain Name System Response Policy Zone
- Verfahren, um bei der Namensauflösung durch rekursive Resolver mittels eigener Richtlinien einzugreifen
- Aktive Gefahrenabwehr insbesondere von Phishingangriffen

DNS-RPZ - Status

- In Kooperation mit der Schweizer Stiftung SWITCH umgesetzt
- Testbetrieb beim DFN-CERT seit Juni 2023
- Pilotbetrieb mit fünf Teilnehmern seit Ende Januar 2024
- Dieser Dienstbestandteil ist **jetzt freigegeben** für alle Teilnehmer, die mindesten die Basisleistungen DFN.Security nutzen können (Unterzeichnung der Dienstvereinbarung und AVV erforderlich!)
- Voraussetzung: RPZ-fähige DNS-Software
- Konfigurationsbeispiel für BIND verfügbar
- Informationen
  - Werden über die Mailingliste dfnsecops-d verteilt
  - Stehen über die Webseite https://www.dfn-cert.de/leistungen/security-operations/ zur Verfügung

DNS-RPZ – Status

- Neue Mailingliste für RPZ-spezifische Themen: **dfnsecurity-dns-rpz**
- Was müssen Sie für das Onboarding tun?
  - Formular in DNS-RPZ_Teilnehmerdaten ausfüllen
  - Formular an uns schicken: **dns-rpz@dfn-cert.de**
  - Nach Rückmeldung von uns: Konfiguration Ihres DNS vornehmen
- Was tun bei ‚false positives‘
  - Meldung an: **dns-rpz@dfn-cert.de** und ggf. an **dfnsecurity-dns-rpz@listserv.dfn.de**
  - Produktiver ‚Test‘ führte zur Korrektur innerhalb einer guten Stunde

DNS-RPZ - Ausblick

- Aktuell basiert der Dienstbestandteil primär auf den Daten von SWITCH
- Kein Unterschied zwischen Basisleistungen und erweiterten Leistungen
- Der Einkauf weiterer Zonen ist derzeit nicht geplant, aber auch nicht ausgeschlossen
- Die Konfiguration ist vorbereitet für eine Community-Zone, DFN-eigene aktive und Evaluierungszonen
- Community Zone
  - Soll nach aktueller Idee von Teilnehmer für Teilnehmer sein
  - Braucht noch Gehirnschmalz und Entwicklung
  - Wenn Sie da Ideen haben und sich aktiv einbringen möchten, melden Sie sich gern

Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie Fragen?

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

DFN.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/