DFN-CERT

deutsches forschungsnetz

Neues aus dem DFN-CERT

81. Betriebstagung | 08.10.2024

Christine Kahl

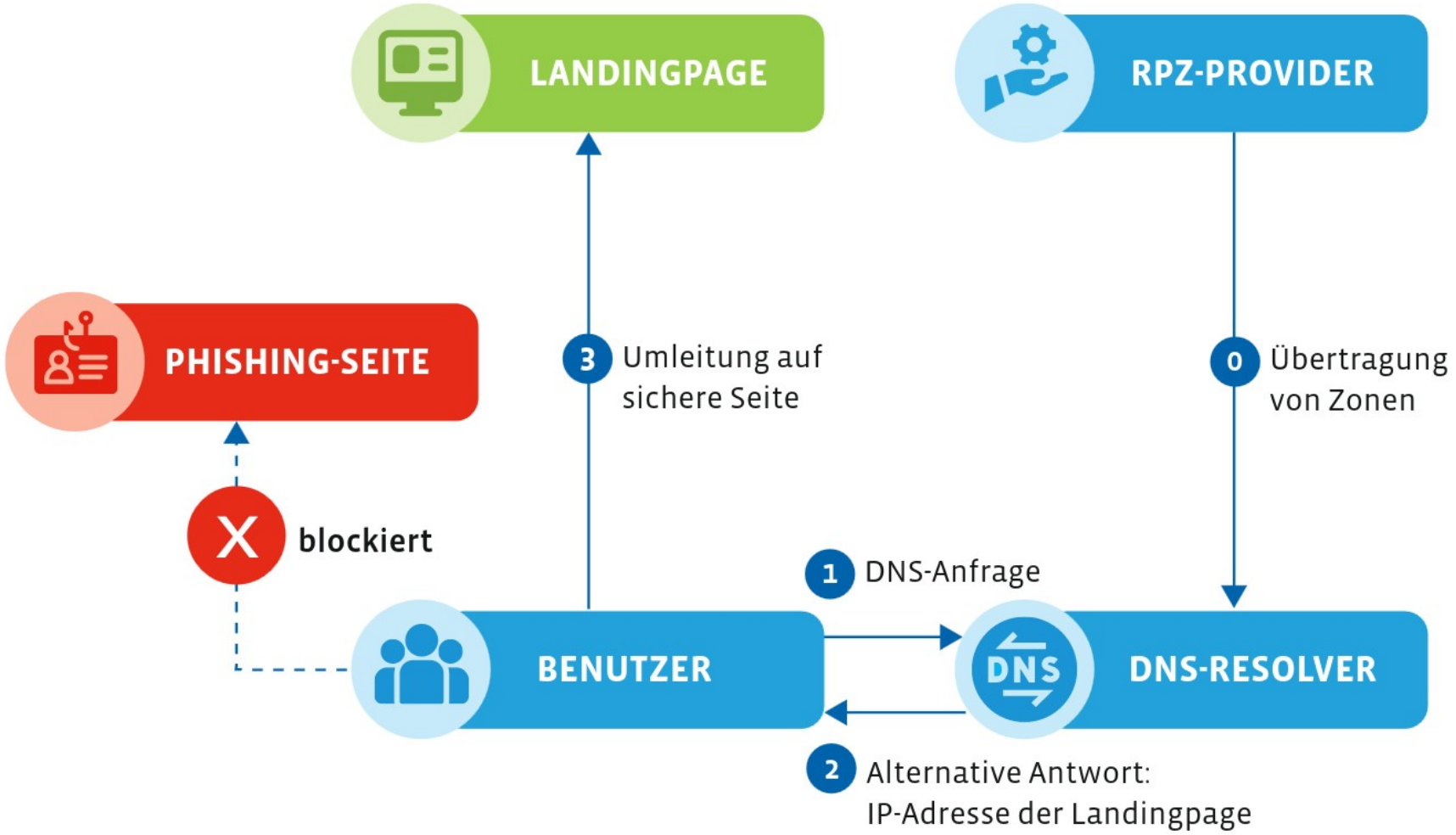
Agenda

1. DNS-RPZ
2. DNS-RPZ Community Zone
3. DFN-Security Challenge
4. Security-Portal Hands-On Training

DFN

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

- Seit März für Teilnehmer am Dienst DFN-Security verfügbar
- Technische Nutzungsvoraussetzung: RPZ-fähige DNS-Software
- Organisatorische Nutzungsvoraussetzung: Dienstvereinbarung DFN-Security und AVV-Anhang DFN-Security unterzeichnet
- Detaillierte Informationen zur Inbetriebnahme in Abstimmung mit uns finden Sie hier: https://www.dfn-cert.de/leistungen/security-operations/

  im Abschnitt DNS-RPZ
  - Beschreibung der Funktionsweise und Nutzung: DNS-RPZ_Grundlegende_Informationen
  - Erfassung der Teilnehmerdaten an uns schicken: DNS-RPZ_Teilnehmerdaten
  - Hilfestellung für die Konfiguration: DNS-RPZ_Administration, DNS-RPZ_BIND_Konfiguration

DNS-RPZ – Status

- Reihenfolge der Zonen ist wichtig, da ‚first match wins'
- Verfügbare Zonen
  - Für etwaige Evaluierungen, derzeit nicht genutzt: zone.eval-f.rpz.dfn.de, zone.eval-l.rpz.dfn.de → passthru
  - Allow-List in der alle im Security Portal eingetragenen und validierten Domains landen: zone.al.rpz.dfn.de → passthru
  - Zonen mit maliziösen Einträgen: zone.mw.rpz.dfn.de, zone.ph.rpz.dfn.de, zone.misc.rpz.dfn.de, zone.community.rpz.dfn.de → blocking!
- Blocking-Zonen
  - mw = Malware, ph = Phishing, misc = Verschiedenes: werden von uns mit Daten befüllt
  - Community: Wir nehmen von Ihnen Daten an und verteilen diese

DNS-RPZ Community-Zone

DNS-RPZ – Community-Zone

- Die Community-Zone ist eine von sieben DFN-Zonen
- Die Zone sollte blockiert werden, da sie maliziöse Domaineinträge enthält
- Die Daten für die Community-Zone stammen von DFN-Teilnehmern
- Seit September können Sie Daten für die Community-Zone einliefern

DNS-RPZ – Community-Zone - warum

- U. a. Phishingangriffe sind seit langer Zeit ein Problem für viele Teilnehmer am DFN
- Lokal gibt es daher oftmals Teams/Personen, die sich um dieses Problem kümmern und Abwehrmaßnahmen umsetzen
- Phishingangriffe sind nicht unbedingt auf eine Einrichtung beschränkt, sondern machen ‚die Runde‘
- Erkenntnisse zu Domains, die für Angriffe genutzt werden und noch nicht durch die verfügbaren Zonen blockiert werden, können anderen Einrichtungen bei der Gefahrenabwehr helfen
  - Spezifischere Daten für das DFN können wir nicht bekommen als von den Teilnehmern am DFN selbst
  - **Helfen Sie sich gegenseitig und teilen Sie Ihre Erkenntnisse**

DNS-RPZ – Community-Zone - wie

- Teilnehmer, die den Dienstbestandteil DNS-RPZ nutzen, können Kontaktpersonen für die Einlieferung von DNS-RPZ Daten benennen
  - DNS-RPZ ist ein mächtiges Werkzeug zur Gefahrenabwehr
  - Fehlerhafte DNS-RPZ Daten können daher auch zu schweren Störungen der Internet-Kommunikation führen
- Die Einlieferung von Daten für eine Blockliste sollte daher ausgewählten Personen vorbehalten sein, die über die notwendige Expertise verfügen und sich ihrer Verantwortung bewusst sind

DNS-RPZ – Community-Zone - wie

- Dateneinlieferung per signierter E-Mail
  - Aktuell halbautomatisch, daher zeitlich verzögerte Verarbeitung
  - Vollautomatische Verarbeitung in Planung
- Keine inhaltliche Prüfung der Daten
  - Nur Syntaxcheck und
  - Abgleich gegen die Top 10000 Domains (derzeit von Cloudflare)
- Daten bleiben 30 Tage in der Zone

Community-Zone

- Diese Zone lebt nur durch Sie!

- Sicherheit als gemeinsame Aufgabe aller Teilnehmer am DFN

DFN

DFN-Security **Challenge**

DFN-Security **Challenge**
Dein Beitrag zählt!

- Mit dem Dienst DFN-Security bieten wir Ihnen ein breites Leistungsspektrum, um die Sicherheit in Ihrer Einrichtung zu steigern
- Wir müssen aber feststellen, dass die wenigsten Einrichtungen wirklich alle Aspekte des Dienstes nutzen
- Warum ist das so?
  - Wir wissen das natürlich nicht, haben aber selbstverständlich mehrere Theorien
  - Eine Theorie sagt, Sie haben alle immer viel zu viel auf dem Zettel und wenn priorisiert wird, steht die Sicherheit meist hinten an
- Was können wir da machen?

- Eigentlich nicht viel, aber
- Wir können versuchen der Sicherheit ein paar Dinge zur Seite zu stellen, damit sie in der Prio-Runde ein größeres Gesamtgewicht zusammen bekommt
  - 1. Spaß: Also erfinden wir einen spielerischen Anteil in Form eines Wettbewerbs
  - 2. Belohnung: Was ist ein Wettbewerb ohne eine Belohnung? Nüscht. Also gibt es besser eine.
  - 3. Etwas Rares: Um auch den letzten Zweifler zu überzeugen, ergänzen wir das Ganze um einen sonst nicht verfügbaren Aspekt und *tada*, fertig ist die

DFN-Security **Challenge**

DFN-Security **Challenge**
Dein Beitrag zählt!

- Wir möchten zusammen mit Ihnen das DFN spielerisch sicherer machen
- Von Anfang November 2024 bis Ende Februar 2025 können Sie durch die Nutzung und Optimierung der Komponenten des Dienstes DFN-Security Punkte für Ihre Einrichtung sammeln
- Was sind die Teilnahmekriterien bzw. was müssen Sie tun?
  - Ihre Einrichtung darf den Dienst DFN-Security prinzipiell nutzen (d.h. es gibt einen unterzeichneten DFN-Rahmenvertrag & die Dienstvereinbarung DFN-Internet oder ein Dienstpaket)
  - Sie melden sich für die Teilnahme an der Challenge an: https://eveeno.com/321538697 (und bekommen damit schon die ersten Punkte)
  - Im Zuge der Anmeldung vergeben Sie bitte einen Alias, der keine Rückschlüsse auf Ihre Einrichtung ermöglicht, mit diesem Alias werden Sie im Wettbewerb dargestellt

DFN-Security **Challenge**
Dein Beitrag zählt!

- Was ist denn das Rare das es gibt?
  - Sie bekommen die Möglichkeit im Vergleich mit anderen zu sehen, wo Sie stehen (anonymisierte Punkteliste)
  - Alle Teilnehmenden bekommen (dauerhaft) Zugriff auf das Dashboard, mit dem Sie die Einspeisung Ihrer Daten in die Logdatenanalyse überwachen können (sonst nur Teil der erweiterten Leistungen), sofern Sie Logdaten einliefern
- Und sonst so?
  - Personalisierte Info-Plakate als Awareness-Maßnahme
  - Kameraabdeckungen
  - Wenn gewünscht: Siegervorstellung auf der nächsten BT
  - Weitere Kleinigkeiten

DFN-Security **Challenge**

Dein Beitrag zählt!

DFN-Security **Challenge**
Dein Beitrag zählt!

- Und Punkte gibt es für?
  - Fast alles, das im Rahmen des Onboardings und der Nutzung des Dienstes relevant ist
  - Formale Dinge, wie die Anmeldung an den Mailinglisten
  - Community-Aspekte, wie Diskussionsbeiträge auf einer Mailingliste
  - DNS-RPZ bezogene Aktionen, wie das Übermitteln von Daten für die Community-Zone
  - Logdateneinlieferung generell und spezifisch für Usecases
  - Domainverifikationen und Definition von Überwachungszielen
  - …
  - Nutzung des Security-Portals
- Besonders viele Punkte gibt es für Dinge, die der Community helfen

DFN-Security **Challenge**
Dein Beitrag zählt!

- Sie können aber auch Punkte verlieren, wenn
  - Zertifikate von Kontakten, die Zugriff auf das Security-Portal haben, ablaufen/abgelaufen sind
  - Ins Security-Portal eingeladene Kontakte über einen längeren Zeitraum unbestätigt bleiben
  - Nachrichten von uns nicht zugestellt werden können, weil z. B. der Kontakt gar nicht mehr existiert
  - ...
- Diese Liste ist ggf. noch nicht vollständig und gerade bei interpretierbaren Punkten, wie z. B. ‚Diskussionsbeiträge auf einer Mailingliste' behalten wir uns vor, diese individuell zu bewerten :)

DFN-Security **Challenge**
Dein Beitrag zählt!

- Details, wie auch die ‚Aufgabenliste' mit den darüber zu erreichenden Punkten, finden Sie unter:
  https://www.dfn.de/dienste/security-trust-and-identity-services/dfn-security-challenge/

- Anmelden direkt hier und ab sofort: https://eveeno.com/321538697

Security-Portal Hands-on Training

Security-Portal Hands-on Training

- Im Vorfeld der 32. DFN-Konferenz ‚Sicherheit in vernetzten Systemen‘ findet ein Hands-on Training für die Nutzung des Security-Portals statt
  - Idealer Weise haben Sie bereits Zugang zum Portal und
  - Bringen konkrete Fragen/Probleme mit
- 11. Februar 2025 9:30 Uhr – 11:30 im Grand Elysée Hotel Hamburg
- Separate Anmeldung erforderlich! Die Anmeldung ist **nicht** an die SiKo gekoppelt, öffnet nur zeitgleich
- Kostenfrei, wenn Sie erscheinen
- Insgesamt 30 Plätze

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/