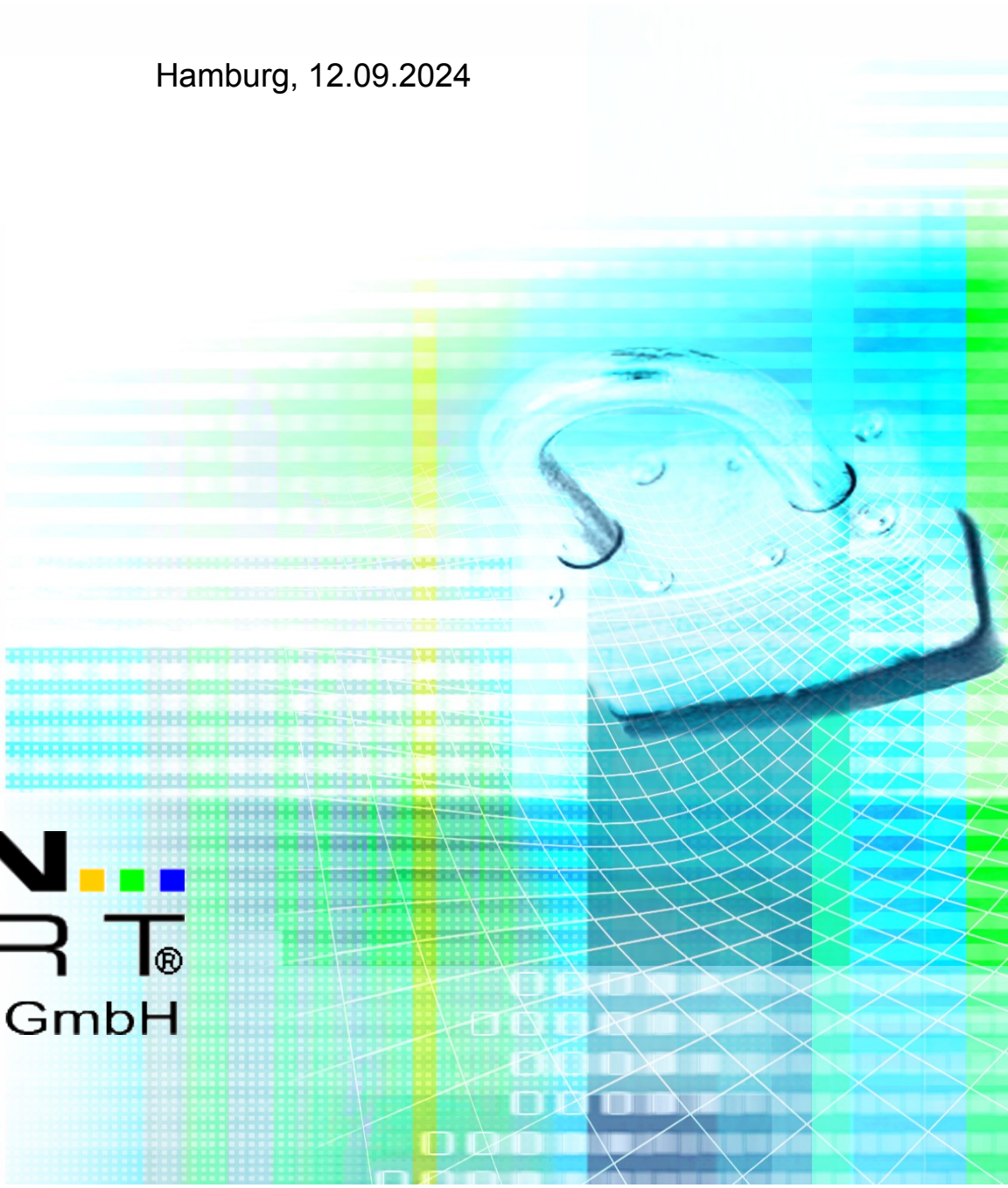
DNS-RPZ

- Teil 4: Community-Zone -

Hamburg, 12.09.2024



DFN-CERT® Services GmbH

Dokument-Informationen	
Sperrvermerk	Nur für: DFN-CERT Services GmbH, DFN-Verein, Teilnehmer und Interessierte am Dienst DFN-Security
Dateiname	DNS-RPZ_Community-Zone-V1.00.odt
letzte Bearbeitung	Donnerstag, 12. September 2024
Seitenanzahl	8
URL aktuelle Version	https://www.dfn-cert.de/leistungen/security-operations/

Inhaltsverzeichnis

1. Einführung

1.1 Ziel dieses Dokuments

Dieses Dokument beschreibt das Feature der Community-Zone als Teil von DNS-RPZ im Rahmen des Dienstes DFN-Security.

1.2 Zielgruppe dieses Dokuments

Dieses Dokument wendet sich an alle Personen, die an der Teilnahme an dem Leistungsmerkmal DNS-RPZ im Dienst DFN-Security interessiert sind.

1.3 Grenzen dieses Dokuments

Für die Beschreibung der Funktionsweise von und der Teilnahme an DNS-RPZ im Rahmen des Dienstes DFN-Security ist das Dokument DNS-RPZ_Grundlegende_Informationen.pdf vorgesehen.

Zur Inbetriebnahme von DNS-RPZ ist außerdem das Dokument DNS-RPZ_Teilnehmerdaten.pdf notwendig, da dessen Formulardaten die Anpassung von DNS-RPZ von Seiten des DFN-CERTs an die teilnehmende Organisation erst ermöglicht.

Das Dokument DNS-RPZ_Administration.pdf dient als Hilfestellung, um DNS-RPZ mit der DNS-Software BIND zu konfigurieren.

Alle Teile der Dokumentation sind unter https://www.dfn-cert.de/leistungen/security-operations/ im Abschnitt DNS-RPZ zu finden.

2. Überblick

2.1 Einführung

Im Dienstmerkmal DNS-RPZ wird ein weiteres Feature bereitgestellt, das sich Community-Zone nennt. Wie der Name es schon erahnen lässt, werden die zu blockierenden Domain-Einträge dieser Zone nicht von einem Zulieferer bereitgestellt, sondern sie werden von den teilnehmenden Einrichtungen gemeinsam erstellt und miteinander geteilt. Damit dieses Gemeinschaftsprojekt funktioniert, ist eine rege Beteiligung im Interesse aller erwünscht.

2.2 Teilnahme an der Community-Zone

Eine passive Teilnahme an dem Projekt erfordert lediglich, dass die Community-Zone in der DNS-Konfiguration der teilnehmenden Einrichtung aktiviert ist (siehe Dokument DNS-RPZ_Administration.pdf, Kapitel 2.7).

Die aktive Teilnahme umfasst darüber hinaus die Einlieferung von Daten, die über E-Mail erfolgt. Dieser Kommunikationsweg ist universell verfügbar, erfordert keine neue Software, Schulungen oder ähnliches, was eine Hürde darstellen würde.

Die Bereitstellung von Daten ist grundsätzlich allen Einrichtungen möglich, die auch am Dienstmerkmal DNS-RPZ teilnehmen. Diese Teilnahme wird auch in regelmäßigen Abständen überprüft.

2.3 Autorisierung der Dateneinlieferung

DNS-RPZ kann zu schweren Störungen der Internet-Kommunikation bei allen Teilnehmern führen. Die Domain-Daten sollen daher nur von Personen (bzw. Rollen oder Systemen) mit spezieller Autorisierung hinzugefügt werden dürfen, die sich ihrer Verantwortung bewusst sind. Die Autorisierung der Identitäten findet durch die Einrichtungen selber statt. Die Domain-Daten werden während der gesamten Verarbeitungszeit von dieser Identität begleitet und zusammen gespeichert.

Damit das DFN-CERT die Autorisierung beim Empfang prüfen kann, müssen die Einrichtungen mitteilen, welche E-Mail-Adressen für eine Dateneinlieferung berechtigt sein sollen. Das Formular für die Teilnehmerdaten (siehe Dokument DNS-RPZ_Teilnehmerdaten.pdf) wurde um ein entsprechendes Textfeld erweitert, in das diese berechtigten Absender-E-Mail-Adressen eingetragen werden sollen. Einrichtungen, die das Formular mit ihren Teilnehmerdaten bereits abgegeben haben und DNS-RPZ schon benutzen, brauchen dieses Formular nicht noch einmal vollständig ausfüllen. Es reicht dieses eine Feld. Neue Einrichtungen, die das Formular noch einreichen müssen, bearbeiten das Formular wie bisher auch komplett.

2.4 Verarbeitung der Daten

Die Community-Zone ist noch in einem frühen Entwicklungsstadium. Dennoch können bereits Daten eingeliefert werden, aus denen die Community-Zone im DNS erstellt wird.

Die Verarbeitung der Daten beim DFN-CERT basiert momentan noch auf einem halbautomatischen Verfahren, das manuelle Aktionen zwischen der Einlieferung per E-Mail und der Auslieferung der Zone via DNS erfordert, wodurch sich eine zeitliche Verzögerung nicht vermeiden lässt.

Diese Aktionen bestehen aus dem Abholen und Überprüfen der E-Mails und der internen Weitergabe der geprüften Daten an weitere Systeme, wo sie von der DNS-Infrastruktur in gewissen Intervallen abgeholt, zu Zonendateien umgewandelt und von dort ausgespielt werden.

Es ist geplant, diese Schritte in zukünftigen Versionen vollständig zu automatisieren.

2.5 Qualität der Daten

Die Daten werden gegen eine gewisse Menge von Domains geprüft, um sicherzustellen, dass diese nicht blockiert werden. Zur Zeit werden die Top 10000 Domains, die Cloudflare (siehe https://radar.cloudflare.com/domains) zur Verfügung stellt, als White-List benutzt.

Zusätzlich wird ein syntaktischer Check durchgeführt, dass es sich wirklich um gültige Domaineinträge handelt.

Eine weitere Prüfung, ob es sich tatsächlich um eine bösartige Domain handelt und ob dort Malware bereitgestellt oder Informationen mittels Phishing abgegriffen werden, findet nicht statt.

Es muss daher klar sein, dass ein erhöhtes Risiko für False Positive-Einträge besteht, das aber durch den Geschwindigkeitsvorteil gegenüber einer kuratierten Zone mehr als ausgeglichen wird.

2.6 Gültigkeitszeitraum der Zonendaten

Die Daten bleiben 30 Tage ab Datum der Einlieferung gültig. Wenn die Daten länger gültig bleiben sollen, müssen sie erneut eingeliefert werden, wodurch sie wieder für 30 Tage gültig sind.

2.7 Technische Aspekte der Dateneinlieferung

Die Einlieferung der Domaindaten erfolgt über E-Mails, die an die Adresse

dns-rpz-community-zone@dfn-cert.de

gesendet werden müssen.

Es ist erwünscht, dass die E-Mails mit SMIME signiert werden.

Die E-Mail kann einen beliebigen Betreff und Text besitzen, da beide ignoriert werden, muss aber zwingend eine Textdatei mit Namen „domains.txt“ im Anhang enthalten.

Diese Datei muss aus einem zu blockierenden Domaineintrag pro Zeile bestehen, wobei die Menge der Einträge nur durch das Größenlimit für eingehende E-Mails der Mail-Server beschränkt ist (z.Z. 25MB inklusive Encoding).

2.8 Meldung fehlerhafter Zoneneinträge

Es kann vorkommen, dass Domaineinträge in der Community-Zone nicht oder nicht mehr als bösartig einzustufen sind. Solche False Positives können und sollten gemeldet werden (siehe DNS-RPZ_Grundlegende_Informationen.pdf, Kapitel 3.1.5 und 3.5).

