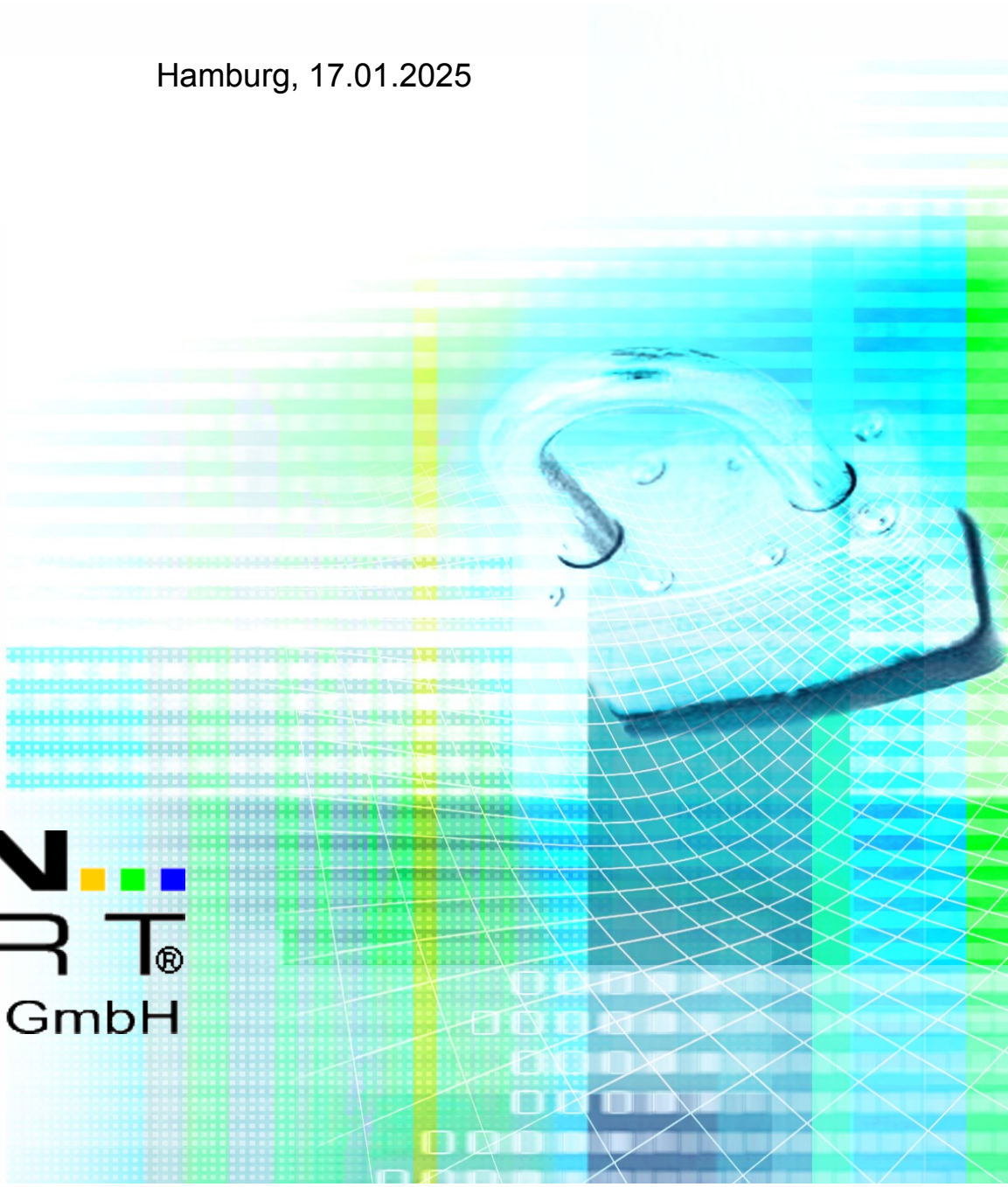
DNS-RPZ

- Teil 3: Administration -

Hamburg, 17.01.2025



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_Administration-V2.04.odt
letzte Bearbeitung	Freitag, 17. Januar 2025
Seitenanzahl	14
URL aktuelle Version	https://www.dfn-cert.de/leistungen/security-operations/

Inhaltsverzeichnis

1. Einführung....5
1.1 Ziel dieses Dokuments....5
1.2 Zielgruppe dieses Dokuments....5
1.3 Grenzen dieses Dokuments....5
2. Konfigurationshinweise für BIND9....6
2.1 Beschreibung der Zonen....6
2.2 Einstellung des Loggings....7
2.3 Einstellung der Optionen....7
2.4 Schlüsselmaterial für die Authentifizierung....9
2.5 Server des DFN-CERTs als Bezugsquelle....9
2.6 Die Zonen im Detail....9
2.7 Lokale Ausnahmen....11
2.8 Aktivierung der Community-Zone....13
2.9 Überprüfung der korrekten Funktionsweise....13
2.10 Testadressen für die SWITCH- und DFN-CERT-Zonen....14
2.11 Limitierungen der Landingpages....14

1. Einführung

1.1 Ziel dieses Dokuments

Dieses Dokument dient als Hilfestellung, um DNS-RPZ mit der DNS-Software BIND im Rahmen des Dienstes DFN-Security zu konfigurieren.

1.2 Zielgruppe dieses Dokuments

Dieses Dokument wendet sich an die verantwortlichen Administratoren der am Dienst DFN-Security teilnehmenden Organisationen, die DNS-RPZ in ihre DNS-Server einbinden wollen.

1.3 Grenzen dieses Dokuments

Dieses Dokument beschränkt sich auf Konfigurationshinweise für die DNS-Software BIND. Für eine ausführliche Dokumentation zur Inbetriebnahme eines solchen Servers hilft die offizielle Website weiter (https://bind9.readthedocs.io/en/v9.18.13/reference.html#response-policy-zone-rpz-rewriting). Zusätzliche Informationen können außerdem im IETF-Entwurf zu dem Thema gefunden werden (https://datatracker.ietf.org/doc/html/draft-vixie-dnsop-dns-rpz).

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.

Die Konfiguration ist auch als eigenständige Datei DNS-RPZ_BIND_Konfiguration.txt erhältlich und muss nicht aus diesem Dokument extrahiert werden.

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

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

2. Konfigurationshinweise für BIND9

Die korrekte Konfiguration liegt in der Verantwortung der teilnehmenden Organisation. In diesem Dokument wird ein Konfigurationsbeispiel für die DNS-Software BIND gezeigt, die einen eingerichteten BIND DNS-Server der Version 9.10 oder höher voraussetzt, da ältere Versionen DNS-RPZ nicht unterstützen. Andere DNS-Software wie PowerDNS Recursor oder Knot Resolver sowie DNS-Appliances z.B. von Infoblox, BlueCat, EfficientIP oder Nokia VitalQIB (Quelle: SWITCH) können ebenfalls verwendet werden, wobei die Konfiguration eigenständig analog eingerichtet werden muss.

2.1 Beschreibung der Zonen

In diesem Abschnitt findet sich eine Übersicht der Zonen, welche durch SWITCH und das DFN-CERT betreut werden.

Bezeichnung der Zone	**Aufgabe im Kontext von DNS-RPZ**
`zone.mw.rpz.dfn.de` `zone3.mw.rpz.switch.ch`	Webseiten, welche bekanntermaßen Schadsoftware (Malware) beinhalten, werden durch diese Zonen blockiert. Auch hier muss eine Landingpage definiert werden.
`zone.ph.rpz.dfn.de` `zone3.ph.rpz.switch.ch`	Diese Zonen beinhalten bekannte Phishing-Webseiten und bekommen daher auch eine entsprechende Landingpage zugewiesen.
`zone.misc.rpz.dfn.de` `zone3.misc.rpz.switch.ch`	Die misc-Zone (miscellaneous, sonstiges) dient dem Filtern von Domains, welche nicht eindeutig den Phishing- oder Malware-Einträgen zuzuordnen sind. Auch hier sollte dementsprechend eine Landingpage definiert werden.
`zone.al.rpz.dfn.de` `zone.wl.rpz.switch.ch`	In die Allow-List (auch White-List genannt) werden Domains eingetragen, die auf keinen Fall blockiert werden sollen, d.h. diese werden von keiner anderen Zone geblockt.

`zone.eval-f.rpz.dfn.de`
`zone.eval-l.rpz.dfn.de`
`zone.test.rpz.switch.ch`
	Diese Zonen dienen in erster Linie Tests und werden von SWITCH und DFN-CERT genutzt, um neue Zulieferer zu testen. Hier ist es grundsätzlich sinnvoll, die Zonen nicht aktiv zum Filtern zu nutzen (`passthru`).
	Das DFN-CERT hat zwei solcher Zonen, um Einstellungen als erste und als letzte Zone testen zu können (first, last).

`zone.community.rpz.dfn.de`	Diese Zone enthält zu blockierende Domains, die aus eingelieferten Daten der am Dienstmerkmal DNS-RPZ teilnehmenden Einrichtungen erstellt wird.

2.2 Einstellung des Loggings

Das Logging dient der Analyse von DNS-RPZ-spezifischen Informationen, die auch als Eingabe für die Logdatenanalyse durch das SoC genutzt werden. Dazu muss in der Konfiguration folgendes eingetragen werden, wobei unbedingt die Dateipfade an die lokale Umgebung angepasst werden müssen.

```
logging {
        // ...
        channel rpz_local {
                // Auf Debian-Systemen kann es notwendig sein, den
                // folgenden Pfad in "/var/log/named/named_rpz" zu ändern.
                // Wenn der relative Pfad benutzt wird, könnte eine
                // Anpassung von AppArmor erforderlich sein.
                file "var/log/named_rpz" versions 10 size 10m;
                severity info;
                print-time yes; print-category yes; print-severity yes;
        };
        category rpz { rpz_local; };
        // ...
};
```

2.3 Einstellung der Optionen

Dieser Abschnitt beschreibt notwendige sowie sinnvolle Optionen.

Das `recursion`-Flag muss aktiviert sein (`recursion yes;`), da DNS-RPZ ansonsten nicht funktioniert. Wichtig ist auch, dass das darauf folgende `allow-recursion` gesetzt ist mit dem entsprechenden Adressraum, damit der DNS-Server kein Open-Resolver ist.

```
recursion yes;
allow-recursion { 192.168.2/24; };
```

Der nachfolgende Teil definiert die eigentliche DNS-RPZ, wobei die Reihenfolge wichtig ist. Die Zonen werden nacheinander geprüft und der erste Treffer, falls vorhanden, liefert das Ergebnis. Die einzelnen Regeln der Zonen können dabei durch die `policy` überschrieben werden, insbesondere die Landingpage wird über diesen Eintrag gesteuert, aber auch beispielsweise das Logging kann hier eingestellt werden. An dieser Stelle wird entsprechend die Landingpage des DFN-CERTs eingebunden oder auf eine eigene geleitet, falls diese eingerichtet ist. Die wichtigsten Parameter sind im folgenden aufgeführt:

`policy passthru`	Dieser Parameter wird für Allow-Lists (White-Lists) genutzt. Bei Treffern werden keine Aktionen ausgeführt, ggf. nur protokolliert
`policy cname`	Bei Treffern werden die Nutzer an den gegebenen cname weitergeleitet, ist hier also für die Landingpage interessant
`policy nxdomain`	Falls keine Landingpage eingesetzt werden soll, ist diese Policy empfohlen. Der DNS-Client erhält auf seine Anfrage die Fehlermeldung, dass die Domain bzw. der Hostname unbekannt ist

`policy drop`	Die Anfrage des DNS-Clients wird verworfen. Da der DNS-Client keine Rückmeldung auf seine Anfrage erhält, hängt er bis zum Timeout in Wartestellung fest
`policy given`	Es wird die Policy benutzt, die in der Zone selbst angegeben ist
Ergänzt werden kann die gewählte Policy um den Parameter `log`:	
`log no`	Deaktiviert das (standardmäßig aktivierte) Logging

Eine DNS-Anfrage wird also der Reihenfolge entsprechend von oben nach unten abgeglichen und bei einem Treffer die vordefinierte Aktion (oder hier auch Policy) durchführt.

An dieser Stelle ist die Information wichtig, dass es zwischen den Zonen keine Duplikatserkennung gibt. Jede Zone, die mit `policy passthru` konfiguriert ist und in der Reihenfolge vorn steht, kann doppelte Einträge einer weiter hinten stehende Zone deaktivieren, d.h. sie wirkt wie eine White-List.

DNS-RPZs sind im übrigen vergleichbar mit anderen Zonen des DNS und können daher wie solche administriert werden, nur dass es spezielle DNS-RPZ-Parameter dafür gibt. Die genaue Reihenfolge und standardmäßigen Aktionen für die verschiedenen Zonen des DFN-CERTs und von SWITCH sind im folgenden aufgeführt:

```
    // BEGIN RPZ Policy
    response-policy {
        // DFN RPZ zones
        zone "zone.eval-f.rpz.dfn.de" policy passthru log yes;
        zone "zone.al.rpz.dfn.de" policy passthru log no;
        zone "zone.mw.rpz.dfn.de" policy cname landingpage-
mw.security.dfn.de;
        zone "zone.ph.rpz.dfn.de" policy cname landingpage-
ph.security.dfn.de;
        zone "zone.misc.rpz.dfn.de" policy cname landingpage-
misc.security.dfn.de;
        // SWITCH RPZ zones
        zone "zone.wl.rpz.switch.ch" policy passthru log no;
        zone "zone3.mw.rpz.switch.ch" policy cname landingpage-
mw.security.dfn.de;
        zone "zone3.ph.rpz.switch.ch" policy cname landingpage-
ph.security.dfn.de;
        zone "zone3.misc.rpz.switch.ch" policy cname landingpage-
misc.security.dfn.de;
        // DFN RPZ Community zone
        // zone "zone.community.rpz.dfn.de" policy cname landingpage-
misc.security.dfn.de;
        zone "zone.eval-l.rpz.dfn.de" policy passthru log yes;
    }
    // Apply RPZ policy to DNSSEC signed zones
    break-dnssec yes;
```



```
    // END RPZ Policy
```

Die Option `break-dnssec yes;` wird genutzt, weil DNSSEC-Pakete laut Voreinstellungen nicht gefiltert werden. Eine Prüfung solcher Anfragen muss also explizit aktiviert werden, da unsichere Websites auch DNSSEC nutzen können.

Die Berechtigungen müssen eingeschränkt werden per `allow-transfer { none; };` und `allow-update { none; };`, da die Zonen ansonsten aktualisiert oder herunter geladen werden könnten.

```
    allow-transfer { none; };
    allow-update { none; };
```

Hier können bei Bedarf auch andere Einstellungen getätigt werden.

2.4 Schlüsselmaterial für die Authentifizierung

Unterhalb der Optionen wird der vom DFN-CERT generierte Schlüssel eingetragen. Dieser Schlüssel soll die Authentizität der DNS-Partner sicherstellen und die Datenintegrität bei Transaktionen gewährleisten. Er wird deshalb erst ausgestellt, nachdem die Teilnehmerdaten übertragen wurden.

```
// TSIG key for RPZ zone-transfer
// DO NOT CHANGE THE NAME OF THE KEY OR COMMUNICATION WILL FAIL!!!
key rpz1-basis.security.dfn.de. {
      algorithm "HMAC-SHA512";
      secret "vom DFN uebermittelt";
};
```

2.5 Server des DFN-CERTs als Bezugsquelle

Unter `masters` werden die Server des DFN-CERTs aufgeführt, welche die Zonendaten unter Angabe des Schlüssels an die DNS-Server der Einrichtungen verteilen. Die vorkonfigurierten Einträge müssen ohne weitere Änderungen übernommen werden:

```
masters dfn-rpz-masters {
        // ns1.security.dfn.de
        195.37.33.18 key rpz1-basis.security.dfn.de.;
        2001:638:dfce:1:23::1 key rpz1-basis.security.dfn.de.;
        // ns2.security.dfn.de
        195.37.33.146 key rpz1-basis.security.dfn.de.;
        2001:638:dfce:1001:23::1 key rpz1-basis.security.dfn.de.;
};
```

2.6 Die Zonen im Detail

Die Zonen unterhalb von „rpz.dfn.de“werden – mit Ausnahme der Community-Zone -- vom DFN-CERT gepflegt, die anderen Zonen durch SWITCH:

```
// DFN RPZ zones
```



```
// Zone zum Testen von neuen Eintragen (first)
zone "zone.eval-f.rpz.dfn.de" {
        type slave;
        file "slave/zone.eval-f.rpz.dfn.de.db";
        masters { dfn-rpz-masters; };
};
// Zone ohne RPZ-Einschränkungen (allow-list). Diese Liste enthält
insbesondere die aktuell verifizierten Domains aller Einrichtungen im DFN-
Security-Portal.
zone "zone.al.rpz.dfn.de" {
        type slave;
        file "slave/zone.al.rpz.dfn.de.db";
        masters { dfn-rpz-masters; };
};
// Bekannte Malware-Sites
zone "zone.mw.rpz.dfn.de" {
        type slave;
        file "slave/zone.mw.rpz.dfn.de.db";
        masters { dfn-rpz-masters; };
};
// Bekannte Phishing-Sites
zone "zone.ph.rpz.dfn.de" {
        type slave;
        file "slave/zone.ph.rpz.dfn.de.db";
        masters { dfn-rpz-masters; };
};
// Sites, für die keine Kategorisierung passt
zone "zone.misc.rpz.dfn.de" {
        type slave;
        file "slave/zone.misc.rpz.dfn.de.db";
        masters { dfn-rpz-masters; };
};
// SWITCH RPZ zones
// Zone ohne RPZ-Einschraenkungen (white-list)
zone "zone.wl.rpz.switch.ch" {
        type slave;
        file "slave/zone.wl.rpz.switch.ch.db";
        masters { dfn-rpz-masters; };
};
// Zone zum Testen von neuen Eintragen
zone "zone.test.rpz.switch.ch" {
        type slave;
        file "slave/zone.test.rpz.switch.ch.db";
        masters { dfn-rpz-masters; };
};
// Bekannte Malware-Sites
zone "zone3.mw.rpz.switch.ch" {
        type slave;
        file "slave/zone3.mw.rpz.switch.ch.db";
        masters { dfn-rpz-masters; };
};
// Bekannte Phishing-Sites
zone "zone3.ph.rpz.switch.ch" {
        type slave;
        file "slave/zone3.ph.rpz.switch.ch.db";
        masters { dfn-rpz-masters; };
```



```
};
// Sites, für die keine Kategorisierung passt
zone "zone3.misc.rpz.switch.ch" {
        type slave;
        file "slave/zone3.misc.rpz.switch.ch.db";
        masters { dfn-rpz-masters; };
};
// DFN RPZ Community zone
// Zone aus eingelieferten Daten der teilnehmenden Einrichtungen
zone "zone.community.rpz.dfn.de" {
        type slave;
        file "slave/zone.community.rpz.dfn.de.db";
        masters { dfn-rpz-masters; };
};
// Zone zum Testen von neuen Eintragen (last)
zone "zone.eval-l.rpz.dfn.de" {
        type slave;
        file "slave/zone.eval-l.rpz.dfn.de.db";
        masters { dfn-rpz-masters; };
};
```

2.7 Lokale Ausnahmen

Die obige Konfiguration stellt noch keine lokale Ausnahmeliste (Allow-List/White-List) zur Verfügung, die von der teilnehmenden Einrichtung selbst verwaltet werden kann, um kurzfristig Domains zu entblocken.

An dieser Stelle wird daraufhin gewiesen, dass für Domains, die als verifiziert im DFN-Security-Portal hinterlegt sind, keine eigenen Ausnahmeeinträge vorgenommen werden müssen, da diese in der DFN-CERT-weiten Ausnahmeliste (zone.al.rpz.dfn.de) aufgeführt sind. Es ist also einfacher und besser, die eigenen Domains im Portal zu konfigurieren.

Die erste Variante für lokale Ausnahmen besteht in der Verwendung sogenannter Views (Sichten). In BIND können zwei Views definiert werden: eine mit und eine ohne RPZ, wobei die Sicht ohne RPZ dann die Ausnahmen bereitstellt. Diese Variante wird eventuell in Zukunft aufgegriffen.

Die andere Möglichkeit ist, eine eigene Zone anzulegen, die dann in der Struktur `response-policy` (siehe Abschnitt 2.3) der erste Eintrag sein muss, damit diese Zone Vorrang vor allen anderen Zonen bekommt und die Anfragen an die dort konfigurierten Domains entsprechend der angegebenen Policy behandelt werden.

Dieser Konfigurationsteil sieht dann etwa so aus, wobei „example.de“ entsprechend der lokalen Umgebung ersetzt werden muss:

```
// BEGIN RPZ Policy
  response-policy {
          zone "zone "zone.no-rpz.example.de" policy given;
          // DFN RPZ Zone
          ...
```


Die Zone muss dann wie jede andere Zone, für die der DNS-Server autoritativ ist, als "type master" eingetragen werden. Dies kann z.B. in der Liste der obigen Zonen stattfinden:

```
// Zone ohne RPZ-Einschränkungen (white-list)
zone "zone.no-rpz.example.de" {
        type master;
        file "master/zone.no-rpz.example.de.db";
};
```

Der Kopf dieser Zonendatei unterscheidet sich nicht von anderen Zonen:

```
zone.no-rpz.example.de. IN SOA     dns.example.de. hostmaster.example.de. (
                  2024042303 10800 1800 604800 86400 )
;
zone.no-rpz.example.de. IN NS      dns.example.de.

$ORIGIN zone.no-rpz.example.de.
```

Anschließend folgen die Einträge, die von der RPZ-Verarbeitung ausgenommen werden sollen.

Der typische Anwendungsfall ist, Hostnamen auszunehmen wie z.B.:

```
www.example.de    CNAME rpz-passthru.
```

Eine weitere Möglichkeit besteht darin, bestimmte Systeme anhand ihrer IP-Adresse als Ausnahmen zu listen. Wenn von diesen IP-Adressen Anfragen an den DNS-Server gestellt werden, dann werden sie nicht der RPZ-Filterung unterworfen. Wenn, wie im folgenden Beispiel zu sehen, Mail-Relays gelistet sind, werden keine False-Positives bei einem Verbindungsaufbau von externen bösartigen Domains zu den Relays protokolliert und dementsprechend auch keine unnötigen automatischen Warnmeldungen generiert. Diese Zugriffe werden durch Mail-Relays, die RBL und andere restriktive Maßnahmen konfiguriert haben, in der Regel abgelehnt. Allerdings werden dann auch keine E-Mails von Intern an bösartige Domains geblockt, so dass sich hier ein möglicher Exfiltrationsvektor ergibt. Aussehen würde ein solcher Abschnitt in etwa so:

```
; Mail-Relay Eins
32.1.11.11.10.rpz-client-ip              CNAME rpz-passthru.
128.1.zz.1.111.111.638.2001.rpz-client-ip CNAME rpz-passthru.

; Mail-Relay Zwei
32.2.11.11.10.rpz-client-ip              CNAME rpz-passthru.
128.2.zz.1.111.638.2001.rpz-client-ip    CNAME rpz-passthru.
```

Eine IPv4- oder IPv6-Adresse setzt sich dabei aus der Netzmaske (hier /32 bei IPv4 und /128 bei IPv6), der IP-Adresse in umgekehrter Notation (die IPv4 von Mail-Relay Eins ist also

10.11.11.1) und der Angabe „rpz-client-ip“ zusammen. Die Zeichenkombination `zz` entspricht der Notation `::` bei IPv6-Adressen.

2.8 Aktivierung der Community-Zone

Die Community-Zone ist in der Beispielkonfiguration bereits vorgesehen. Die Aktivierung besteht für neue Teilnehmer hauptsächlich darin, die Kommentarzeichen vor der Community-Zone im Konfigurationsabschnitt `response-policy` zu entfernen und den DNS-Server mit der neuen Konfigurationsdatei laufen zu lassen.

Als Standard-Policy werden die Domains der Zone blockiert und die DNS-Clients auf eine Landingpage verwiesen. Eine Alternative wäre, die Policy `passthru log yes` zu benutzen, z.B. für Testzwecke.

Teilnehmende Einrichtungen, die bereits vor Einführung dieser Zone dabei waren, sollten den Konfigurationsabschnitt überprüfen, da es dort einige Veränderungen gibt. Insbesondere ist die Community-Zone bis fast ans Ende der Zonenliste gewandert und der Policy-Default hat sich zum Blockieren geändert. Die Reihenfolge wurde geändert, um ein versehentliches White-Listing zu vermeiden, falls die Policy auf `passthru` geändert wird.

2.9 Überprüfung der korrekten Funktionsweise

Der Hostname `rpz-test.dfn-cert-testbed.de` ist in der Zone `zone.ph.rpz.dfn.de` eingetragen, wodurch er von RPZ als bösartig eingestuft wird. Darauf aufbauend steht die URL

https://rpz-test.dfn-cert-testbed.de/rpz-test

bereit.

Administratoren können mit einem Aufruf der URL in einem Browser die generelle Funktionstüchtigkeit ihres RPZ-Setups testen.

Vorbedingungen für den Test sind eine abgeschlossene Konfiguration, in der auch die Zone `zone.ph.rpz.dfn.de` abonniert sein muss, mindestens einmal wurde ein Zonentransfer der Zone durchgeführt und der Browser benutzt den RPZ-fähigen DNS-Server für die Namensauflösung.

Selbstverständlich wird unter dieser URL keine Malware oder Phishing-Seite bereitgestellt, d.h. der Besuch der Testseite hat in dieser Hinsicht keine schädlichen Folgen.

Wenn bei Aufruf der URL die Landingpage nach dem Akzeptieren der Zertifikatswarnung angezeigt wird, war die Konfiguration erfolgreich.

Sollte stattdessen die auf dem Webserver des DFN-CERTs eingerichtete „Testseite für die DNS-RPZ-Konfiguration“ angezeigt werden, dann ist die Konfiguration fehlerhaft und muss überprüft werden!

2.10 Testadressen für die SWITCH- und DFN-CERT-Zonen

Für die blockierenden Zonen von SWITCH und DFN-CERT existieren weitere Testadressen, die auf eine entsprechende Landingpage führen, falls die Zonen korrekt konfiguriert sind.

Die Testadressen für die Zonen von SWITCH sind:

https://test.mw.rpz.switch.ch/

https://test.ph.rpz.switch.ch/

https://test.misc.rpz.switch.ch/

Die Testadressen für die Zonen des DFN-CERTs sind:

https://test.zone.mw.rpz.dfn.de/

https://test.zone.ph.rpz.dfn.de/

https://test.zone.misc.rpz.dfn.de/

https://test.zone.community.rpz.dfn.de/

Wenn bei Aufruf der URL die Landingpage nach dem Akzeptieren der Zertifikatswarnung angezeigt wird, ist die Zone korrekt konfiguriert.

2.11 Limitierungen der Landingpages

An dieser Stelle ist noch ein Hinweis für den weiteren Betrieb wichtig, da Webbrowser wie Chrome, Firefox und andere ein Feature implementieren, das für Administratoren im Zusammenhang mit verhinderten Zugriffen auf Landingpages überraschend sein könnte.

Der Aufruf einer Landingpage für eine zu blockierende Domain, für die HTTP Strict Transport Security (HSTS) in der Chrome-Preload-Liste definiert ist (https://hstspreload.org/), ist in aktuellen Browsern mit Standardeinstellungen nicht möglich. Der Grund dafür ist, dass viele Browser diese Liste einsetzen, um den HSTS-Header noch vor dem Laden der Webseite einer Domain setzen, falls die Domain in der Liste existiert. Wenn das Zertifikat, wie im Fall der Landingpages, nicht zu der Domain passt, kann die entsprechende Landingpage nicht angezeigt werden, da das Angebot für eine Ausnahmeregelung für das Akzeptieren des ungültigen Zertifikats in diesem Fall durch den Browser nicht zur Verfügung gestellt wird.

