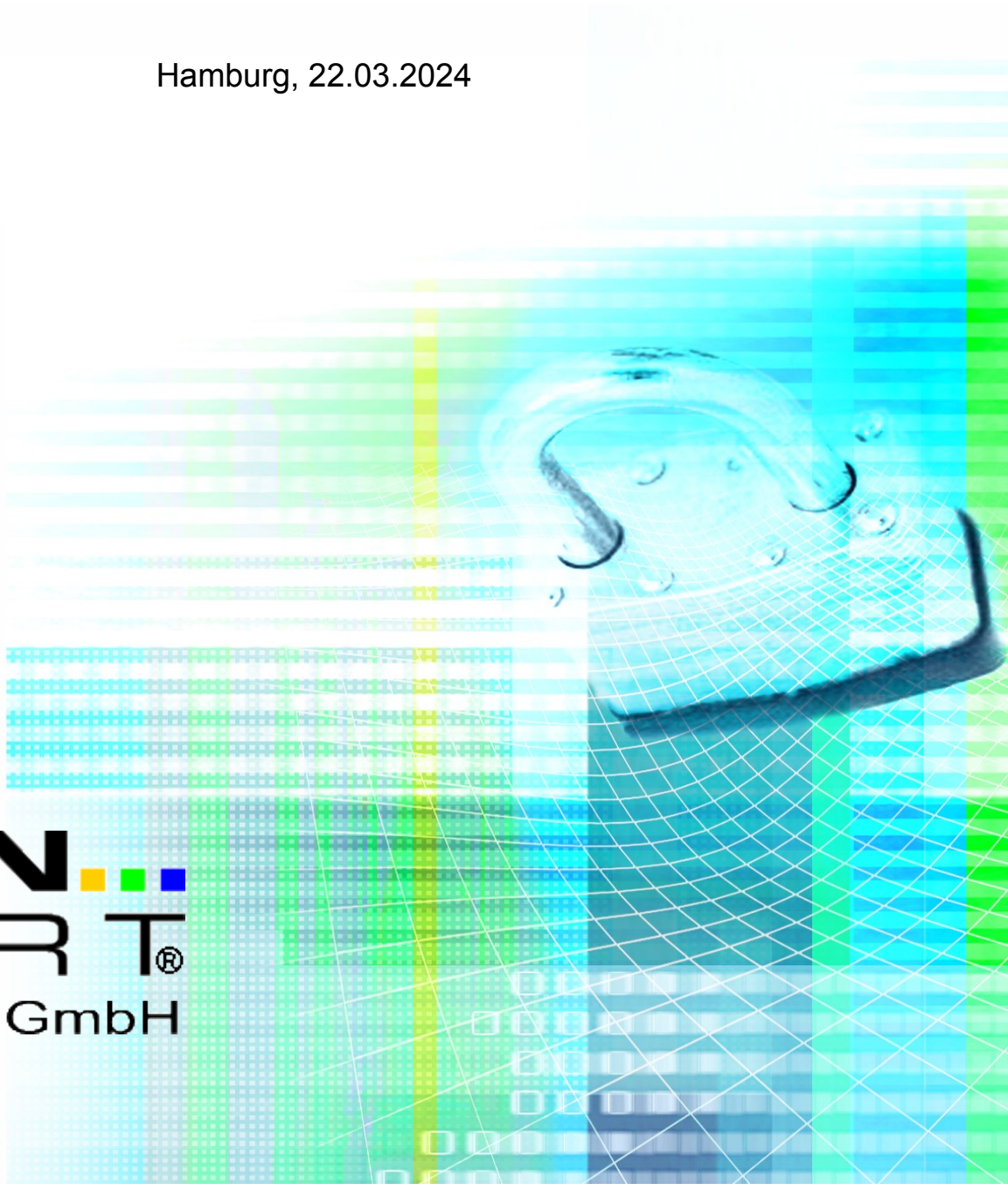
DNS-RPZ

- Teil 3: Administration -

Hamburg, 22.03.2024



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_Administration-V1.10.odt
letzte Bearbeitung	Freitag, 22. März 2024
Seitenanzahl	10
URL aktuelle Version	https://www.dfn-cert.de/leistungen/security-operations/

Inhaltsverzeichnis

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.

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.ph.rpz.dfn.de` `zone3.ph.rpz.switch.ch`	Diese Zonen beinhalten bekannte Phishing-Webseiten und bekommen daher auch eine entsprechende Landingpage zugewiesen.
`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.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).

`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.community.rpz.dfn.de`	Diese Zone ist für zukünftige Inhalte vorgesehen und wird erst zu einem späteren Zeitpunkt definiert. In der aktuell vorliegenden Konfiguration wird sie daher rein passiv eingesetzt (`passthru`).

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 {
                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 on;`), 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 on;
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, hier also für die Landingpage interessant

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. 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
        zone "zone.eval-f.rpz.dfn.de" policy passthru log yes;
        zone "zone.al.rpz.dfn.de" policy passthru log no;
        zone "zone.community.rpz.dfn.de" policy passthru log yes;
        zone "zone.ph.rpz.dfn.de" policy cname landingpage-
ph.security.dfn.de;
        zone "zone.mw.rpz.dfn.de" policy cname landingpage-
mw.security.dfn.de;
        zone "zone.eval-l.rpz.dfn.de" policy passthru log yes;

        // SWITCH RPZ
        zone "zone.wl.rpz.switch.ch" policy passthru log no;
        zone "zone.test.rpz.switch.ch" policy passthru;
        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-
mw.security.dfn.de;
    }
    // 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 geupdated oder herunter geladen werden könnten.

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

Hier können bei Bedarf auch andere Einstellungen getätigt werden.

2.4 Authentifizierung und Übertragung zwischen Teilnehmern und DFN-CERT

Unterhalb der Optionen wird der vom DFN-CERT generierte Schlüssel eingetragen. Dieser kann erst ausgestellt werden, sobald 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 Die Zonen im Detail

Unter `masters` werden die RPZ Upstream-Server aufgeführt, welche die Daten an die entsprechenden Zonen weiterleiten. Hier reichen die vorkonfigurierten Einträge aus.

```
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.;
};
```

Die oberen sechs Zonen werden vom DFN-CERT und die anderen werden durch SWITCH gepflegt:

```
// DFN RPZ Zones
// Zone zum testen von neuen Eintragen
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-Einschraenkungen (allow-list)
zone "zone.al.rpz.dfn.de" {
        type slave;
        file "slave/zone.al.rpz.dfn.de.db";
        masters { dfn-rpz-masters; };
};
// Zone mit noch zu definierendem Inhalt
zone "zone.community.rpz.dfn.de" {
        type slave;
        file "/slave/zone.community.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; };
};
// Bekannte Malware-Sites
zone "zone.mw.rpz.dfn.de" {
        type slave;
        file "slave/zone.mw.rpz.dfn.de.db";
        masters { dfn-rpz-masters; };
};
// Zone zum Testen von neuen Eintragen
zone "zone.eval-l.rpz.dfn.de" {
        type slave;
        file "slave/zone.eval-l.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, fuer die keine Kategorisierung passt
zone "zone3.misc.rpz.switch.ch" {
        type slave;
        file "slave/zone3.misc.rpz.switch.ch.db";
        masters { dfn-rpz-masters; };
};
```

2.6 Lokale Ausnahmen

Die obige Konfiguration stellt noch keine lokale Ausnahmeliste (Allow-List/White-List) zur Verfügung, die von der teilnehmenden Einrichtung selber verwaltet werden kann, um kurzfristig Domains zu entblocken. Dafür ist eine eigene Zone anzulegen, die dann in `response-policy` (siehe Abschnitt 2.3) der erste Eintrag in der Struktur sein sollte mit `policy passthru`, damit diese Zone Vorrang vor allen anderen Zonen bekommt und die Anfragen an die dort konfigurierten Domains durchgelassen werden. Alternativ können auch zwei Sichten, sogenannte Views, in BIND definiert werden, eine mit und eine ohne RPZ, wobei die Sicht ohne RPZ dann die Ausnahmen bereitstellt.

