Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Handreiking security.txt

Centraal security.txt-bestand voor organisaties van de Rijksoverheid

Dit document biedt een handreiking voor Rijksoverheidsorganisaties om verwijzingen naar het centrale Rijksoverheid security.txt-bestand te implementeren op hun webservers.

Wat is een security.txt-bestand?

Een security.txt-bestand[1] is een tekstbestand waarmee organisaties hun contactgegevens voor het melden van security-gerelateerde zaken kunnen publiceren. Beveiligingsonderzoekers (ook wel goedwillende of ethische hackers) kunnen deze informatie gebruiken om contact met de organisatie op te nemen over beveiligingsproblemen die zij in de website of systemen van de organisatie hebben gevonden. Het formaat van het bestand is bedoeld om machinaal en menselijk leesbaar te zijn. Security.txt is sinds april 2022 een Internet Engineering Task Force (IETF)-standaard onder de noemer RFC 9116.[2] Organisaties kunnen de standaard implementeren door een security.txt-bestand onder een speciale URL te serveren op hun webservers. Het is optioneel om ook andere relevante informatie voor beveiligingsonderzoekers op te nemen, zoals een link naar uw beleid voor het omgaan met meldingen van beveiligingskwetsbaarheden.

Doelgroep

Deze handreiking is bedoeld voor organisaties van de Rijksoverheid.

Samenwerkingspartners

Deze handreiking is tot stand gekomen met de medewerking van:

- Forum Standaardisatie
- Digital Trust Center
- Dienst Publiek en Communicatie

[1] Zie: https://securitytxt.org/

[2] Zie: https://www.rfc-editor.org/rfc/rfc9116. De RFC heeft bij IETF de status "Informational".

Hoe werkt een security.txt-bestand?

Een voorbeeld security.txt-bestand kunt u hieronder zien. Regels die starten met een '#' karakter dienen als commentaar. IANA houdt een register bij van alle velden die een security.txt-bestand kan bevatten.[3]

Voorbeeld security.txt

```
# Een link, e-mailadres of telefoonnummer waarmee contact opgenomen kan worden
# indien een beveiligingsonderzoeker een kwetsbaarheid wilt melden voor dit
# domein.
Contact: mailto:mail@example.nl
Contact: https://example.nl/contact-formulier/

# Dit veld specificeert de houdbaarheidsdatum van het bestand. Indien de datum
# verstreken is dient een beveiligingsonderzoeker dit bestand niet meer te gebruiken.
Expires: 2023-09-13T11:38:00.000Z

# Indien u de beveiligingsonderzoeker de mogelijkheid wilt bieden om u een versleuteld
# bericht te sturen met PGP kunt u met het 'Encryption' veld uw publieke PGP-sleutel
# kenbaar maken.
Encryption: https://example.nl/pgp.txt

# Hiermee geeft u aan in welke talen er gecommuniceerd kan worden. De volgorde,
# bij het specificeren van meer talen, geeft de mate van voorkeur uit waarbij de
# eerste optie meer voorkeur heeft.
Preferred-Languages: nl,en

# De URL waarop dit bestand geserveerd wordt.
Canonical: https://example.nl/.well-known/security.txt

# Een link naar uw security policy.
Policy: https://example.nl/security-policy/
```

Een security.txt-bestand is opvraagbaar via het pad */.well-known/security.txt* op het bijbehorende domein. Voor het domein *example.nl* zou een organisatie haar security.txt-bestand kunnen serveren op *https://example.nl/.well-known/security.txt*. Momenteel wordt er binnen de Internet Engineering Task Force (IETF) ook gewerkt aan een specificatie die de URL waarop een PGP key geserveerd wordt standaardiseert.[4]

[3] Zie: https://www.iana.org/assignments/security-txt-fields/security-txt-fields.xhtml

[4] https://datatracker.ietf.org/doc/draft-koch-openpgp-webkey-service/

Waarom een centraal security.txt-bestand voor de Rijksoverheid?

Het Nationaal Cyber Security Centrum (NCSC) is het eerste centrale contactpunt voor Coordinated Vulnerability Disclosure (CVD) meldingen voor systemen van de Rijksoverheid.[5] Dit betekent dat CVD-meldingen in eerste instantie gemeld moeten worden aan het NCSC, waarna het NCSC contact zal opnemen met de relevante organisatie binnen de Rijksoverheid.[6]

In plaats van alle webservers van de Rijksoverheid te voorzien van een apart security.txt-bestand, biedt het verwijzen naar een centraal security.txt-bestand met een *HTTP 302 Redirect* meerdere voordelen:

- Gemak: Organisaties van de Rijksoverheid hoeven zelf geen security.txt-bestand te genereren en te publiceren, maar hoeven alleen maar te verwijzen.
- Proces: Het centrale security.txt-bestand sluit aan bij het bestaande proces waarin NCSC een centrale rol speelt bij het afhandelen van CVD-meldingen voor de Rijksoverheid.
- Wijzgigingenbeheer: Wijzigingen hoeven alleen in het centrale security.txt-bestand doorgevoerd te worden. Webservers die verwijzen naar het centrale security.txt-bestand zullen hierdoor automatisch verwijzen naar de nieuwe content. Zonder een centraal security.txt-bestand zouden alle security.txt-bestanden op iedere webserver geüpdatet moeten worden.
- Up-to-date: De verplichte houdbaarheidsdatum (in het Expires-veld) van het centrale security.txt-bestand hoeft maar op een plek aangepast te worden zodra deze verstreken is. Zonder een centraal security.txt-bestand zouden alle webservers die gebruik maken van security.txt-bestanden periodiek geüpdatet moeten worden om de houdbaarheidsdatum te verversen.

Als u als Rijksoverheidsorganisatie wilt dat onderzoekers kwetsbaarheden in uw systemen melden bij NCSC, dan is het handig om op uw domeinnamen te verwijzen naar de het centrale security.txt-bestand. Het kan ook zo zijn dat u als Rijksoverheidsorganisatie zelf de capaciteit en kennis in huis hebt om meldingen direct te ontvangen. In dat geval dient u als Rijksoverheidsorganisatie een eigen security.txt met daarin eigen contactgegevens te publiceren. Tot slot, in het geval van een systeem dat wordt geleverd door een externe leverancier kan een Rijksoverheidsorganisatie ervoor kiezen om van de leverancier te eisen dat deze een security.txt met eigen contactinformatie publiceert en dat de leverancier capaciteit en kennis heeft om meldingen direct (zonder tussenkomst van de Rijksoverheidsorganisatie) snel en goed af te handelen.

Wat zijn de risico's?

De specificatie van security.txt vermeldt dat er door het opnemen van contactgegevens in een security.txt-bestand een risico op spam, nepmeldingen en phishing bestaat. Dit risico speelt bijvoorbeeld ook wanneer een organisatie contactgegevens op haar website publiceert.

Omdat het NCSC via het centrale security.txt-bestand het aanspreekpunt is voor CVD-meldingen zullen eventuele frauduleuze meldingen er door het NCSC uitgefilterd worden zodat u alleen, via het NCSC, de legitieme meldingen zult ontvangen.

[5] Zie: https://www.ncsc.nl/contact/kwetsbaarheid-melden

[6] De voorheen gangbare naam voor Coordinated Vulnerability Disclosure (CVS) is Responsible Disclosure (RD).

Hoe implementeer ik security.txt voor mijn systemen?

Rijksoverheidsorganisaties kunnen gebruik maken van het centrale security.txt-bestand door verzoeken op het pad *https://<uw_domeinnaam>/.well-known/security.txt* door te verwijzen d.m.v. een HTTP 302 Redirect naar *https://www.ncsc.nl/.well-known/security.txt*. Op deze manier kunnen beveiligingsonderzoekers contact leggen met het NCSC indien er een kwetsbaarheid gevonden is op een van uw systemen. Het NCSC zal vervolgens contact opnemen met uw organisatie om deze kwetsbaarheid op te lossen. Meer informatie voor het implementeren van verwijzingen kunt u vinden op de website van het Digital Trust Center (DTC).[7]

Soms is het lastig om een security.txt-bestand te serveren op een IP-adres. Omdat beveiligingsonderzoekers vaak systemen scannen op basis van een IP-adres, is het aan te raden om vanuit dit IP-adres via reverse DNS (rDNS) naar het bijbehorende webdomein te verwijzen. Op dit webdomein kan dan een security.txt-bestand geserveerd worden op het reguliere pad. Via rDNS kunnen beveiligingsonderzoekers dan toch een bijpassend security.txt-bestand vinden.[8]

Indien u als Rijksoverheidsorganisatie van plan bent naar dit centrale security.txt-bestand te verwijzen, dan is het van belang dat uw domeinnaam conform het Domeinnaambeleid van de Rijksoverheid geregistreerd is via Dienst Publiek en Communicatie (DPC), een agentschap van het Ministerie van Algemene Zaken.[9, 10] De registratie door DPC maakt het voor NCSC eenvoudiger te controleren of een ontvangen CVD-melding gaat over een domeinnaam van de Rijksoverheid en ook om de juiste contactgegevens van de domeinnaam te achterhalen. Daardoor kan NCSC CVD-meldingen snel en gericht doorsturen naar uw organisatie zodat geen kostbare tijd verloren gaat met het oplossen van de kwetsbaarheid.

Met de tool Internet.nl kunt u testen of de domeinnaam van uw organisatie op correcte wijze naar het centrale security.txt-bestand verwijst.[11]

[7] https://www.digitaltrustcenter.nl/securitytxt/it-dienstverleners

[8] Om de integriteit van de rDNS-antwoorden te waarborgen is het aan te raden om reverse zones (onder .ip6.arpa voor IPv6 en onder .in-addr.arpa voor IPv4) te ondertekenen met DNSSEC.

[9] Zie: https://www.communicatierijk.nl/vakkennis/rijkswebsites/verplichte-richtlijnen/domeinnaamregistratie-en--beheer

[10] Zie: https://www.communicatierijk.nl/vakkennis/rijkswebsites/verplichte-richtlijnen/domeinnaambeleid

[11] Zie: https://internet.nl/article/securitytxt-test-toegevoegd/

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

Februari 2023