Van: (10)(2e) (10)(2e)
Aan: (10)(2e) @rivm.nl
Cc: (10)(2e) (10)(2e) Forum Standaardisatie; (10)(2e) (10)(2e) Zonnenberg, Raoul
Onderwerp: FW: Responsible disclosure RIVM-(sub)domeinen
Datum: vrijdag 10 april 2020 16:03:53
Bijlagen: RIVM_domeinen_OSINT-2020-04-06.xlsx
RIVMnl_subdomeinen_OSINT-2020-04-06.xlsx
image001.png
image002.png
image003.png

Dag (10)(2e)

Onderstaande mail van Forum Standaardisatie stuur ik je, in aanvulling op ons gesprek eerder deze middag. Zoals je ziet in de bijlagen, voldoen te meeste websites/-registraties niet aan de gestelde webeisen. Daardoor is de kans op potentieel misbruik zeer groot aanwezig.

Gezien de huidige perikelen rondom Corona, is de kans dat zich een risico voordoet zelfs zeer aannemelijk (er zijn al gevallen in het nieuws geweest) en de impact daarvan erg groot. Het is dus nu echt het moment om door te pakken en acties te ondernemen! Uit ons gesprek bleek dat je de urgentie om de kwetsbaarheden van de websites en dergelijke te mitigeren met mij deelde.

We hebben drie actielijnen besproken:

1. De defensief geclaimde DNS-registraties zsm uitfaseren;
2. De registraties van de overige sites (zoveel als mogelijk) bij MinAZ onderbrengen;
3. Mail-policies (zoals DMARC) op orde brengen.

Nogmaals druk ik je op het hart om –ondanks de drukte rondom de Corona- juist prioriteit te geven en de acties uit jullie plan (die zoals je zegt overeenkomt met bovenstaande) uit te voeren.
Waar mogelijk (bijvoorbeeld bij het overzetten van de DNS-registraties) wil ik jullie graag ondersteunen.

Mocht je nog vragen hebben, dan kan je natuurlijk bij mij terecht.

Vriendelijke groet,
(10)(2e)

Van (10)(2e) - Forum Standaardisatie <(10)(2e)@forumstandaardisatie.nl>
Verzonden: maandag 6 april 2020 19:01
Aan: '(10)(2e)@rivm.nl' <(10)(2e)@rivm.nl>
CC: '(10)(2e)@rivm.nl' <(10)(2e)@rivm.nl>; (10)(2e) - Forum Standaardisatie <(10)(2e)@forumstandaardisatie.nl>
Onderwerp: Responsible disclosure RIVM-(sub)domeinen

Beste (10)(2e)

Afgelopen weekend zagen we dat het RIVM recent de website databronnencovid19.nl heeft gelanceerd.
Dit domein bevat dezelfde spoofing-kwetsbaarheid die rivm.nl afgelopen vrijdag ook had:
https://www.internet.nl/mail/databronnencovid19.nl/345320/#control-panel-8
Getriggered door de berichtgeving in de media afgelopen vrijdag over het spoofing-risico, en het aantreffen van dezelfde kwetsbaarheid in het nieuwe domein databronnencovid19.nl, heb ik op basis van OSINT domeinen waar RIVM verantwoordelijk voor is geïnventariseerd.
In totaal trof ik zo'n 365 hoofddomeinen aan en 342 *.rivm.nl subdomeinen.

Het aantal domeinen schrok ik wel een beetje van. Hoe houden jullie hier grip op? Zowel vanuit veiligheidsperspectief als vanuit communicatief perspectief? Dit artikel is in dit kader wellicht interessant.
Hoe moet een burger er met alle berichtgeving rond coronaphishing eigenlijk op vertrouwen dat databronnencovid19.nl écht van het RIVM is?

De domeinen heb ik in bulk door Internet.nl gehaald om te kijken in hoeverre deze voldoen aan de verplichte standaarden.
In de bijlage vind je de scanresultaten inclusief legenda.

Enkele zaken die opvallen:

*Subdomeinen *.rivm.nl:*

- De meeste subdomeinen hebben geen mailserver geconfigureerd, maar veel daarvan hebben wel een DMARC p=quarantaine policy. Voor die domeinen kan een DMARC p=reject policy worden gehanteerd.
- Eventueel kan op het hoofddomein rivm.nl een DMARC subdomain policy worden ingesteld: sp=reject . Voor specifieke subdomeinen waarvan wel gemaild wordt kan vervolgens een specifiek DMARC policy worden ingesteld (mailgw01-dmz.rivm.nl, mailgw02-dmz.rivm.nl, test.rivm.nl, menukaart-kansrijkestart-nl.rivm.nl)
- SPF is op de niet-verzendende subdomeinen niet goed ingesteld, plaats bij elk niet-verzendend subdomein een "SPF -all" record. Hiermee zet je het domein ook dicht voor ontvangende mailservers die geen DMARC validatie doen maar wel SPF validatie.

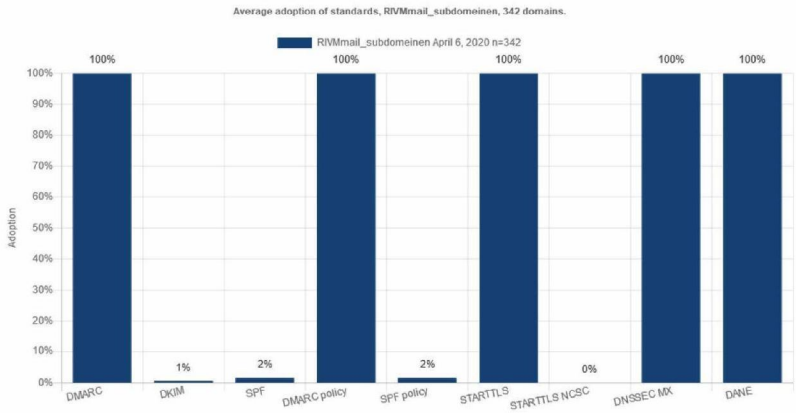
Hoofddomeinen:

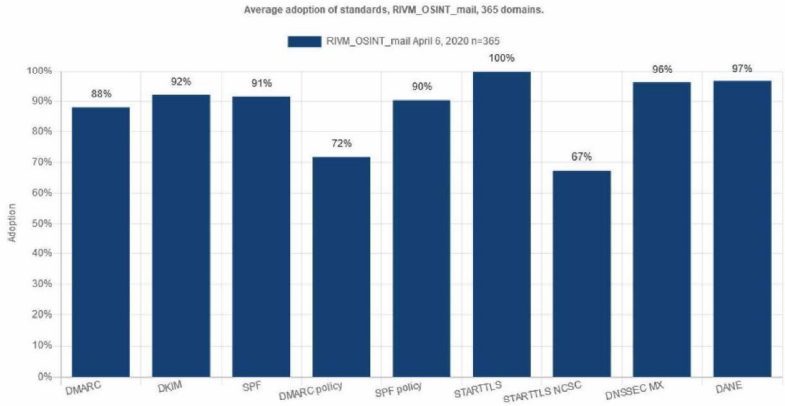
- 339 RIVM-hoofddomeinen hebben een mailserver geconfigureerd; van 107 daarvan is de STARTTLS-verbinding niet conform de TLS-richtlijnen (v1.1) van het NCSC geconfigureerd
- 99 RIVM-hoofddomeinen hebben nog geen DMARC quarantaine of reject policy.

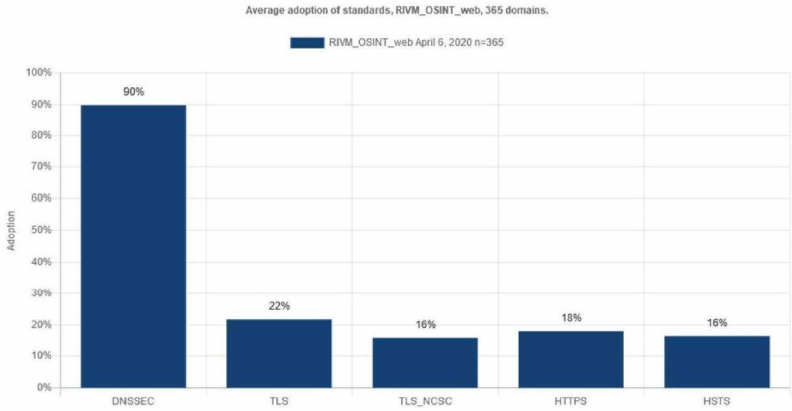
- Voor hoofddomeinen waar niet van gemaild wordt is het aan te raden om deze dicht te zetten om spoofing te voorkomen, ook eventuele subdomeinen:
  - Plaats een zogenaamd "null MX" record in de DNS zone.
  - Plaats een "SPF -all" record in de DNS zone.
  - Plaats een "DMARC p=reject" record in de DNS Zone.
  - Plaats geen DKIM record.

- 10% van de RIVM-hoofddomeinen maakt nog geen gebruik van DNSSEC.
- Veel webdomeinen lijken niet te functioneren, ze verwijzen naar IP-adressen die niet antwoorden. Zijn al deze webdomeinen wel nodig?

Hieronder nog enkele statistieken over alle domeinen heen. De TLS-statistieken voor web kunnen met een korreltje zout worden genomen, veel domeinen waren onbereikbaar waardoor deze in de HTTPS-test faalt.
Indien jullie dit soort rapportages zelf willen kunnen maken kunnen jullie (kosteloos) toegang vragen tot het bulkmeting dashboard van Internet.nl via [10(2e)]@internet.nl. Internet.nl is een initiatief van de Nederlandse internetgemeenschap en de Nederlandse overheid.







Met vriendelijke groet,

(10)(2e)
Adviseur standaardisatie
(10)(2e)

Van: (10)(2e) - Forum Standaardisatie
Verzonden: vrijdag 13 maart 2020 18:47
Aan: '(10)(2e)@rivm.nl'
CC: (10)(2e) - Forum Standaardisatie
Onderwerp: Voorkomen van spoofing middels strikte DMARC policy

Beste (10)(2e)

Via het nieuws vernamen we dat er valse mails namens het RIVM in omloop zijn over het coronavirus om betaalgegevens te ontfutselen en malware of ransomware te verspreiden. Voor het RIVM – als 'trusted advisor voor de samenleving' – is dit natuurlijk onwenselijk, helemaal in deze tijd.

We hebben de mails zelf niet onder ogen gehad, en kunnen dus ook niet zien of deze daadwerkelijk vanuit de @rivm.nl domeinnaam of een ander legitiem RIVM-domein is verzonden. Wel willen we je er op wijzen dat een voldoende strikt DMARC-beleid (p=quarantaine of p=reject) cruciaal is in het bestrijden van phishing uit naam van overheidsorganisaties.

Via een test met Internet.nl zien we dat rivm.nl de meeste standaarden goed op orde heeft, behalve een voldoende strikte DMARC-policy: https://www.internet.nl/mail/rivm.nl/333430/#control-panel-9

Uit een test blijkt dat een gespoofde mail van bijvoorbeeld corona@rivm.nl bij Gmail daarom ook gewoon aankomt:

Met een voldoende strikt DMARC beleid vertelt u wat ontvangende mailservers (bijvoorbeeld die van Gmail of Outlook.com) moeten doen als zij een verdachte email (op basis van SPF en DKIM die al goed zijn ingesteld) ontvangen uit naam van het RIVM. Hiermee wordt phishing vanuit legitieme domeinen voorkomen. Uiteraard voorkomt dit geen phishing uit domeinnamen die lijken op die van RIVM.

Voordat u het DMARC-beleid aanpast is het van belang te weten dat een voldoende strikt DMARC beleid niet zomaar van de een op de andere dag kan worden ingevoerd, omdat er mogelijk legitieme mailstromen zijn namens @rivm.nl waarvan de mail niet juist is ondertekend met de DKIM-handtekening of waarvan de mailservers niet juist zijn geautoriseerd via het SPF-record.

Een handreiking om tot een strikte DMARC-policy te komen vindt u hier:
https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS-191211.5A4%20opdracht-implementatie-strikte-dmarc-policy.pdf

Met vriendelijke groet,

(10)(2e)
(10)(2e)

Bureau Forum Standaardisatie
Wilhelmina van Pruisenweg 52 | 2595 AN | Den Haag
Postbus 96810 | 2509 JE | Den Haag

M 0(10)(2e) | @(10)(2e)@forumstandaardisatie.nl
W forumstandaardisatie.nl | @openstandaarden | LinkedIn

Standaard Samenwerken