Auteur: Ronald Eygendaal schrijft sinds 1990 over informatiebeveiliging, beveiliging van industriële automatisering en elektronische & technische beveiliging, voor de toonaangevende vakbladen in Nederland en België. Ronald is te bereiken via: info@cqure.nl.

Vernieuwde aanpak voor securitymeldingen

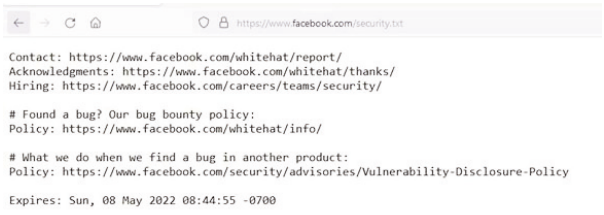
In de beginjaren van het internet was er het Internet Mail Consortium (IMC) dat zich richtte op het gezamenlijk beheren en promoten van standaardisatie voor elektronische post op internet. Zo hebben we in 1997 met het IMC afspraken gemaakt over het gebruik van e-mailadressen. Afgesproken werd voor welke doelen bepaalde e-mailadressen gebruikt mogen (moeten) worden. Deze afspraken zijn uiteindelijk voorgesteld als standaard en zijn vastgelegd in de RFC 2142 (1). Deze RFC heeft de naam `Mailbox Names for Common Services, Roles and Functions' gekregen.

Vele jarenlang vervulde een aantal van deze 'verplichte' adressen een belangrijk rol bij het veilig houden van internet. Zo is het adres abuse@domeinnaam bedoeld om ongewenste e-mails en chatberichten en ander ongepast internetgedrag te melden. Het 'verplichte' e-mailadres security@domeinnaam biedt de mogelijkheid bepaalde dreigingen en kwetsbaarheden te melden. Het melden van kwetsbaarheden wordt ook wel Coordinated Vulnerability Disclosure (CVD) of Responsible Disclosure proces genoemd. Dit proces regelt hoe we op een verantwoorde wijze en in gezamenlijkheid ICT-kwetsbaarheden melden en openbaar maken. Iedereen kan een Responsible Disclosure-melding doen bij een bedrijf, overheidsinstantie of andere organisatie. De organisatie heeft dan de kans om de kwetsbaarheid op te lossen. Voor het melden van een CVD dient, conform RFC 2142, dient het e-mailadres security@domeinnaam te worden gebruikt. Ook wordt geadviseerd om de e-mail adressen zoals abuse@domeinnaam en security@domeinnaam op de hoofdpagina van de website te zetten zodat melders en klagers de adressen makkelijk kunnen vinden. Door de opkomst van contentmanagers, websiteredacteuren en andere editors die de hoofdpagina's vullen, zijn de vermeldingen van de abuse en secure e-mailadressen op hoofdpagina's verdwenen. In veel gevallen zijn de 'verplichte' adressen helemaal verdwenen.

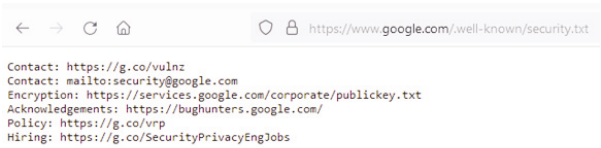
Voorspelbare locatie

In augustus 2021 hebben Edwin Foudil en Yakov Shafranovich bij het Internet Engineering Task Force (IETF) een voorstel ingediend om te komen tot RFC 9116 (2). Deze RFC heeft de naam 'A File Format to Aid in Security Vulnerability Disclosure'. De RFC beschrijft een andere methode om het e-mailadres bekend te maken waarop kwetsbaarheden kunnen worden gemeld. Het idee achter de RFC is eenvoudig: men plaatst een bestand met de naam security.txt op een voorspelbare locatie op de site. Dit is een locatie waar de 'content jongens en meisjes' geen last van hebben en dus de hoofdpagina kunnen volplempen met content. Zoals RFC 9116 aangeeft kan het security.txt bestand in de hoofddirectory van het domein worden geplaatst. Bijvoorbeeld https://www.domeinnaam/security.txt

Hieronder een voorbeeld hoe Facebook dit gedaan heeft:



Maar er zijn ook partijen die de security.txt in de .well-known directory zetten, zoals bijvoorbeeld google:



De inhoud van het security.txt-bestand varieert enigszins, maar de meeste bevatten links naar informatie over het beveiligingsbeleid van de organisatie en een e-mailadres voor het melden van kwetsbaarheden alsook een verloopdatum.
Komende maanden zal het Internet Engineering Task Force (IETF) besluiten of RFC 9116 geformaliseerd wordt. Het lijkt erop dat de internetgemeenschap security.txt gaat omarmen. In Nederland hebben het Digital Trust Center en het NCSC positief gereageerd op security.txt. Nu nog de implementatie. Aan de slag dus en creëer meer ruimte voor content op de hoofdpagina van uw website.
Nagekomen, zie ook het recente bericht van Tweakersnet d.d. 28.04.2022 (3), waarbij de Internet Engineering Task Force (IETF) een nieuwe standaard (RFC 9116 (4)) voorstelt.

Referenties

(1) https://www.rfc-archive.org/getrfc?rfc=2142#gsc.tab=0
(2) https://www.rfc-editor.org/rfc/authors/rfc9116.html
(3) https://tweakers.net/nieuws/196102/ontwikkelaars-stellen-security-punt-txt-standaard-voor-melden-beveiligingsfouten-voor.html?utm_source=nieuwsbrief&utm_medium=email&utm_campaign=twk_nieuwsbrief
(4) https://www.rfc-editor.org/rfc/rfc9116