Jan Heijdra, cyber security specialist bij Cisco Nederland

01-05-2021 | door: **Blog**

Deel dit artikel:

De impact van domeinnamen en veilig internet

Precies 35 jaar geleden, op 1 mei 1986, registreerde Piet Beertema het eerste Nederlandse domein CWI.NL voor het Centrum Wiskunde en Informatica. De komst van domeinnamen in 1986 en 2 jaar later op 17 mei 1988 de beschikbaarheid van internet hebben in Nederland voor drastische veranderingen gezorgd, onder andere rond security zo schrijft Jan Heijdra, cyber security specialist bij Cisco Nederland, in deze blog.

Vandaag de dag is het een pandemie die heeft gezorgd voor een ongekende versnelling van de manier van leven en werken op en via de digitale snelweg. Zonder internet en domeinnamen zag het leven anders uit en was het onmogelijk om kinderlijk eenvoudig te bankieren, alles aan huis te laten bezorgen, online college te volgen, binnen een aantal uur een oude fiets te verkopen aan een onbekende, massaal coronatesten in te plannen of op alle vragen een antwoord te vinden met behulp van een zoekmachine.

10 feiten over 35 jaar .NL

- **1986** 25/04 Registratie van het Top Level Domein(tld) .NL en het beheer wordt overhandigd aan Piet Beertema.
- **1986** 01/05 Uitgave van eerst Nederlandse domeinnaam cwi.nl.
- **1998** 24/06 Registratie Cisco.nl (cisco.com bestond al sinds 1987).
- **1991** Eerste web browser publiek beschikbaar (Web browser had als naam WorldWideWeb en is later hernoemd naar Nexus om verwarring met het World Wide web te voorkomen).
- **2006** 01/07 Oprichting OpenDNS (DNS security-oplossing).
- **2015** 30/06 Cisco kondigt overname OpenDNS aan.
- **2020** 18/06 De 6 miljoenste .NL domein registratie bij het SIDN (Stichting Internet Domeinregistratie Nederland).
- **2020** 16/12 Publicatie "EU Cybersecurity Strategy for the Digital Decade" met daarin een verwijzing naar DNS security. De Europese Commissie stimuleert de ontwikkeling van publieke Europese DNS resolvers (DNS4EU).
- **2021** 25/04 35 jaar geleden werd het Nederlandse top level domein .NL officieel geregistreerd door Piet Beertema.
- **2021** 01/05 35 jaar na eerste registratie Nederlands domeinnaam (cwi.nl).

Waarom gebruiken we domeinnamen?
Websites en alle overige internetresources zijn bereikbaar via een IP-adres, een lange en lastige numerieke code vergelijkbaar met een telefoonnummer. Omdat het lastig is om al deze codes te onthouden is het Domain Name Systeem (DNS) ontwikkelt, dit systeem vertaalt een simpel webadres zoals cisco.nl naar een IP-adres. Simpel gezegd is DNS het telefoonboek van het internet.

Cybersecurity & DNS
Iedereen kent de e-mailtjes wel die zogenaamd namens de bank zijn verstuurd, waarin wordt gevraagd om snel een check uit te voeren op de website, omdat anders de rekening of pas het risico loopt geblokkeerd te worden. De gepresenteerde website lijkt verdacht veel op de legitieme website en het domeinnaam verschilt maar 1 letter (een nul i.p.v. een o bijvoorbeeld). Dit is een herkenbaar voorbeeld waar kwaadwillende domeinnamen en links naar websites gebruiken om toegang te krijgen tot persoonlijke financiële informatie of proberen kwaadaardige software te installeren (bijv. ransomware).

Bovenstaand voorbeeld laat een spam methode zien die gebruikt wordt om kwaadaardige websites onder de aandacht te brengen bij onschuldige gebruikers. Het systeem achter e-mail leunt ook op DNS en kwaadwillende kunnen bij organisaties zonder goede beveiliging onder een andere naam mailen (CEO fraude) of spam te versturen. Het Nederlandse forum voor standaardisatie heeft DANE (DNS-based Authentication of Named Entities) in 2016 op de pas-toe leg- uit lijst geplaats voor ontvangende e-mail-servers en op 29 november 2018 is de pas-toe leg- uit lijst uitgebreid naar ontvangende- en verzendende-mail servers. DANE biedt d.m.v. een DNS-certificaatcheck zekerheid over de identiteit van de ontvangende-mailserver. Dit voorkomt dat een kwaadwillende als ontvangende-mailserver kan optreden en het mailverkeer kan onderscheppen.

Naast technische uitdagingen gerelateerd aan DNS is ook een zorgvuldige administratie van domeinnamen van cruciaal belang. Daniel Verlaan, onderzoeksjournalist bij RTL, wist in oktober 2020 miljoenen Burgerservicenummers in te zien door een oude domeinnaam van het Jeugd Riagg over te nemen. Een instelling die jeugdzorg verleent aan duizenden gezinnen en in 2015 van naam veranderde. Deze journalist wist de oude domeinnaam over te nemen, waardoor het mogelijk was om nieuw binnengekomen e-mails te lezen (die nog naar het oude domein werden gestuurd).

In 2019 publiceerde de Cisco Talos Threat Intelligence organisatie bevindingen over de “Sea Turtle DNS Hijacking campagne”. Deze campagne van kwaadwillende (waarschijnlijk statelijke actoren) had het gemunt op militaire- en overheidsinstellingen in het Midden Oosten, Noord Afrika en o.a. Griekenland (40 organisaties in 13 landen). Via phishing of het gebruik van kwetsbaarheden in de software wist men toegang te verschaffen tot de DNS-inloggegevens van de desbetreffende organisaties. Met de login gegevens werden de DNS-gegevens, die richting de legitieme servers verwezen, aangepast en naar een kwaadwillende server verwezen. Op deze manier werd een klassieke “Man in the Middle” aanval opgebouwd en werden logingegevens verzameld om gevoelige data te ontvreemden.

Veiliger internetten met DNS filtering oplossingen
De gemakkelijkste manier om het beveiligingsniveau van een organisatie naar een hoger niveau te tillenis het toepassen van een DNS-oplossing met security filter functionaliteit. In deze verbeterde situatie wordt de standaard DNS (die alle website verzoeken vertaald naar een IP-adres) voor de gehele organisatie gewijzigd naar een DNS-oplossing die naast deze vertaling ook de security reputatie van de aangevraagde website controleert en kwaadaardige websites op voorhand blokkeert. De reputatiescore van websites wordt opgebouwd uit de 620 miljard DNS-verzoeken van 24.000 klanten uit 190 landen die Cisco Umbrella voorbij ziet komen per dag. Deze grote hoeveelheid informatie wordt verrijkt door de Threat Intelligence van de Talos research organisatie. Door gebruik te maken van DNS-filtering oplossingen zoals OpenDNS(gratis voor consumenten) of Umbrella (zakelijke klanten) weten organisaties op een simpele manier phishing activiteiten dwars te zitten en ransomware tegen te gaan.

Zonder domeinnamen en het achterliggende DNS systeem komt het internet tot stilstand. Gezien het economische en maatschappelijke belang van stabiele en veilige internettoegang, is het van groot belang dat organisaties alle mogelijkheden aangrijpen om op een snelle en eenvoudige manier een basis DNS security filter toe te passen, waarmee gebruikers beschermd worden tegen de dreigingen en zonder zorgen op weg kunnen naar nog eens 35 jaar internetervaringen.

Bekijk ook onze video .nl bestaat 35 jaar.

Door: Jan Heijdra, cyber security specialist bij Cisco Nederland