Hoffmann Cyber Security Onderzoek

Nederlandse organisaties kwetsbaar voor phishing aanvallen

Hoffmann

Managementsamenvatting

Misbruik van e-mail komt steeds vaker voor, met name door middel van phishing aanvallen. Bij dit soort aanvallen proberen kwaadwillenden gevoelige gegevens te verkrijgen via een vervalst e-mailbericht. Een techniek die aanvallers hiervoor regelmatig gebruiken heet spoo□ng (vervalsing). Door gebruik van deze techniek lijkt het alsof e-mails daadwerkelijk vanuit een betrouwbare organisatie zijn verstuurd.

Hoffmann heeft in mei en juni 2016 onderzoek uitgevoerd naar de kwetsbaarheid van Nederlandse organisaties als het gaat om spoo□ng en (spear)phishing aanvallen. Hierbij is met behulp van een beperkte scan bekeken of een aantal basis anti-spoo□ng instellingen, Sender Policy Framework (SPF) en Domain-based Message Authentication, Reporting, and Conformance (DMARC) bij deze organisaties zijn ingesteld.

In totaal zijn 26.734 domeinnamen in dit onderzoek benaderd. De resultaten van het onderzoek zijn ontluisterend. Van de onderzochte domeinnamen heeft **59,4% het SPF-record niet of onjuist ingesteld.** In totaal **98,4% van de onderzochte domeinnamen heeft geen DMARC-record ingesteld.** De scan is uitgevoerd op 24 mei 2016

De drie meest opvallende sectoren zijn:

1. **Gezondheids- en welzorg.** Het betreft ziekenhuizen, verzorgingstehuizen, praktijken van zorgverleners en andere organisaties die actief zijn in het zorgdomein. Van de 15.341 onderzochte domeinnamen hebben er 66,8% geen of geen juist SPF-record ingesteld.
2. **Openbaar bestuur.** Hieronder vallen de nationale overheid, gemeenten en provincies. Alle gemeenten met een geregistreerde domeinnaam, alle provincies en alle ministeries zijn in het onderzoek meegenomen. Van de in totaal 1.591 onderzochte domeinnamen hebben er eveneens 66,8% geen of geen juist SPF-record ingesteld.
3. **Overige zakelijke dienstverlening.** Het gaat hier om zakelijke dienstverleners zoals bijvoorbeeld advocatenkantoren en accountants. Van de 1.822 onderzochte domeinnamen hebben er 52,4% geen of geen juist SPF-record ingesteld.

Om het gebruik van instellingen zoals SPF, DKIM en DMARC effectief te maken is het belangrijk dat de verantwoordelijke voor een domein de juiste SPF, DKIM en DMARC instellingen con□gureert en dat de ontvangende mailserver hierop controleert en vervolgens actie neemt als er twijfel bestaat over de herkomst van de betreffende mail. Hiermee is bescherming tegen spoo□ng dus een gezamenlijke inspanning van zowel de verzendende als de ontvangende partij. Als organisaties breed maatregelen treffen om e-mail spoo□ng tegen te gaan, wordt Nederland als geheel weerbaarder op gebied van e-mail phishing.

Niet alleen technische maatregelen helpen een organisatie zich beter te beschermen tegen phishing. Het is voor organisaties belangrijk om te kiezen voor een integrale aanpak, niet alleen gericht op techniek, maar vooral ook op het inrichten van de juiste processen en medewerkers te leren hoe zij zich zo veilig mogelijk kunnen gedragen in hun communicatie.

Introductie

Misbruik van e-mail komt steeds vaker voor, met name door middel van *phishing* (vissen, hengelen) aanvallen. Bij dit soort aanvallen proberen kwaadwillenden gevoelige gegevens te verkrijgen via een vervalst e-mailbericht. In zo'n bericht wordt de ontvanger verleid om handelingen te verrichten die kunnen leiden tot het onderscheppen van zulke gevoelige informatie, of zelfs uiteindelijke "overname" van het ICT systeem van de ontvanger (slachtoffer).

Phishing e-mails zien er tegenwoordig vaak geloofwaardig uit. Er zijn voorbeelden waarbij phishing mails van een collega uit de eigen organisatie afkomstig lijken te zijn. Een techniek die aanvallers hiervoor regelmatig gebruiken heet *spoofing* (vervalsing). Door gebruik van deze techniek lijkt het alsof e-mails daadwerkelijk vanuit een betrouwbare bron zijn verstuurd. Voor de gedupeerde persoon of organisatie kan dit vervelende consequenties hebben. Het resultaat kan namelijk zijn dat een cybercrimineel zich op deze wijze toegang tot de interne ICT-infrastructuur verschaft, met alle gevolgen van dien. Het kan ook imagoschade opleveren, of ervoor zorgen dat mailproviders legitieme e-mails van een gedupeerde organisatie weren, als zij phishing vanaf een dergelijk domein vaststellen.

Recent is er veel berichtgeving rondom spoo□ng en phishing in de media. Zo berichtte Binnenlands Bestuur in haar editie van week 22 2016 over de '*gênant slechte beveiliging van e-mail bij Nederlandse gemeenten*'. Uit een steekproef bij 50 Nederlandse gemeenten bleek dat zij niet voldoen aan diverse verplichte beveiligings-standaarden voor e-mail.

Op 7 juni 2016 berichtte de NOS dat er sprake zou zijn van de '*grootste phishingcampagne van dit jaar in Nederland*'. Meer dan 100.000 personen, met name werknemers van Nederlandse organisaties, zouden een e-mail hebben ontvangen met het verzoek om betaling van een bedrag dat werd gespeci□ceerd in een met een virus besmette bijlage. Het virus zou zijn gericht op het verzamelen van bankgegevens. De e-mail adressen en persoonlijke gegevens in het bericht lijken afkomstig te zijn van een uitgelekt bestand met vertrouwelijke gegevens van LinkedIn.

Ook in de recente cyber-onderzoeken van Hoffmann zijn veel voorbeelden te vinden van succesvolle phishingaanvallen. Zo zijn er opdrachtgevers die, na besmetting via phishing, slachtoffer zijn geworden van hacking, waarbij de betaalbestanden vlak voor activatie werden gewijzigd en grote sommen geld naar bankrekeningen van criminelen werden overgeschreven. Ook zien we een grote toename van *ransomware* (chantage) voorvallen, die vaak zijn veroorzaakt door een phishing e-mail met een besmette bijlage. Uit al deze voorbeelden blijkt dat medewerkers van Nederlandse organisaties een gericht doelwit vormen van phishing aanvallen.

Hoffmann heeft in mei en juni 2016 onderzoek uitgevoerd naar de kwetsbaarheid van Nederlandse organisaties als het gaat om spoo□ng en (spear)phishing aanvallen. In totaal zijn 26.734 domeinnamen in dit onderzoek benaderd. De uitkomsten zijn ontluisterend en worden in dit onderzoeksrapport weergegeven. Ook wordt toegelicht dat een totaalaanpak nodig is om Nederland weerbaarder te maken op dit gebied en worden adviezen gegeven aan organisaties om zichzelf minder kwetsbaar te maken voor phishing.

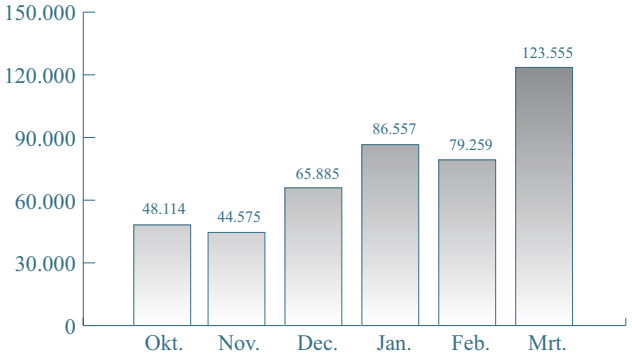
E-mail phishing

Tegenwoordig maken cybercriminelen veelvuldig gebruik van phishing-methoden als opstapje naar criminele activiteiten. Phishing, afgeleid van □shing, betekent zoveel als het vissen of hengelen naar informatie. Mensen worden verleid tot het nemen van een actie die een cybercrimineel op weg helpt.

Bijvoorbeeld het klikken op een website waarop gevraagd wordt een gebruikersnaam, wachtwoord of andere vertrouwelijke gegevens in te voeren of het klikken op een bijlage met daarin mala□de software die gebruikt kan worden om heimelijk toegang te krijgen tot iemands computer(netwerk). Bij veel van dit soort phishing acties wordt gebruik gemaakt van e-mail. Naast phishing wordt tegenwoordig ook gesproken over *spear phishing*. Er is sprake van spear phishing als de e-mails heel precies zijn afgestemd op de ontvanger, zodat deze ze maar moeilijk herkent als onbetrouwbaar. Van deze methode wordt bijvoorbeeld gebruik gemaakt bij CEO fraude, waarbij oplichters zich voordoen als directeur van een organisatie en bijvoorbeeld een mail naar een medewerker van de □nanciële afdeling sturen om een geldbedrag over te maken naar een bepaalde bankrekening.

Op 23 mei 2016 publiceerde de Anti-Phishing Working Group (APWG) in haar trendrapportage dat het aantal phishing-aanvallen in het eerste kwartaal van 2016 explosief is gestegen ten opzichte van het laatste kwartaal van 2015. Het APWG rapporteert een toename van 250%; een groei van ruim 48.000 phishing sites in oktober 2015 naar bijna 124.000 phishing sites in maart 2016.

Unique Phishing Sites Detected October 2015 - March 2016



Figuur 1 – APWG trend analyse phishing aanvallen

In dezelfde rapportage werd duidelijk dat de retail/service sector het grootste doelwit vormt van phishing aanvallen (42,7% van het totaal). De meeste phishing aanvallen worden gehost vanuit de Verenigde Staten (meer dan 75% van het totaal). Ook Nederland komt voor in de top 10 (ongeveer 2,7% van het totaal). Dagelijks komen er gemiddeld 227.000 nieuwe malware samples bij, aldus APWG.

Een onderzoeksrapport van PhishMe rapporteert eveneens een enorme toename van phishing e-mails. Zij zien een toename van 789% sinds het laatste kwartaal van 2015. Daarbij valt met name de opkomst van *ransomware* op, waarbij de meegestuurde malware ervoor zorgt dat bestanden op het computer(netwerk) versleuteld worden en pas na betaling van losgeld worden vrijgegeven. PhishMe rapporteert dat ongeveer de helft van alle aangetroffen malware in phishing e-mails in maart 2016 bestaat uit dit soort encryptie malware.

Deze cijfers laten zien dat *phishing* en *spear phishing* een groeiend probleem vormen. Het is daarom belangrijk om in een organisatie maatregelen te nemen om het risico op phishing zo klein mogelijk te maken.

Deze maatregelen zijn mogelijk op het gebied van:
1. Techniek
2. Organisatie
3. Mens

Zo helpt het bijvoorbeeld om medewerkers goed te informeren over hoe zij een phishing mail kunnen herkennen en wat zij moeten doen als ze denken dat ze een dergelijk bericht hebben ontvangen of (erger nog) op de bijbehorende links of bijlagen hebben geklikt. Ook zijn er technische maatregelen te nemen die organisaties helpen zich beter te beschermen tegen misbruik van e-mail middels phishing. Het is belangrijk dat de verschillende maatregelen op gebied van techniek, organisatie en mens goed op elkaar worden afgestemd. Het één kan niet zonder het ander.

Beveiligingstechnieken voor tegengaan e-mail phishing

Als een organisatie zich op technisch vlak wil beveiligen tegen phishing dan is het belangrijk om aandacht te besteden aan twee zaken:
1. Mala□de e-mails die afkomstig lijken te zijn uit de eigen organisatie.
2. Mala□de e-mails die afkomstig lijken te zijn uit andere organisaties.

In het geval van mala□de e-mails die afkomstig lijken te zijn uit de eigen organisatie is er vaak sprake van spear phishing. Bij dit soort e-mails lijkt de afzender een collega te zijn van de eigen organisatie. Een belangrijke techniek die aanvallers hiervoor regelmatig gebruiken heet *spoofing*. Door gebruik van deze techniek lijkt het alsof e-mails daadwerkelijk vanuit de eigen organisatie zijn verstuurd. Verderop in dit hoofdstuk wordt toegelicht welke technieken een rol spelen bij het beschermen van een organisatie tegen spoo□ng. Naast het toepassen van anti-spoo□ng instellingen op mailservers, kan een organisatie zelf ook controles inbouwen om tegen deze vorm van phishing bescherming te bieden. Als binnenkomende e-mails van de eigen domeinnamen bijvoorbeeld verstuurd zijn vanaf servers die niet in het eigen netwerk voorkomen, dan is de kans groot dat het een phishing e-mail betreft. Dit soort controles zorgt ervoor dat de kans groter wordt dat spear phishing berichten in een vroeg stadium onderschept worden.

In het geval van mala□de e-mails die afkomstig lijken te zijn uit andere organisaties is het belangrijk als organisatie om te detecteren welke ontvangen e-mails phishing e-mails betreffen. Ook hier speelt *spoofing* een rol. Een e-mail kan namelijk afkomstig lijken te zijn van een betrouwbare organisatie die slachtoffer is geworden van spoo□ng. In dit geval is het belangrijk dat die andere organisatie zich hier zo goed mogelijk tegen beschermt met een aantal technische maatregelen. *Hierbij ben je als organisatie dus afhankelijk van de getroffen maatregelen van andere organisaties tegen spoofing*. Dat is geen prettige gedachte. Wat je op technisch vlak als organisatie zelf kunt doen is het uitvoeren van technische controles op binnenkomende e-mails. Belangrijk is om in elk geval een spam□lter te gebruiken die controleert op de aanwezigheid van diverse indicatoren, waaronder die van spoo□ng. Bij voldoende negatieve indicatoren wordt een mail als spam gemarkeerd en kan een gebruiker beoordelen of dit werkelijk het geval is.

Tot slot is het goed om op te merken dat kwaadwillenden soms domeinnamen registreren die lijken op een domeinnaam van een betrouwbare organisatie, waarbij slechts één karakter is veranderd. Dit valt haast niet op als de verwisselde karakters erg op elkaar lijken, bijvoorbeeld Goog1e.com in plaats van Google.com *(typosquatting)*. Het is voor een organisatie haast ondoenlijk om alle varianten van de eigen domeinnaam, die zo te maken zijn, zelf te registreren. Wel zijn er dienstverleners die de aanwezigheid van dit soort domeinnamen regelmatig controleren, waarna e-mails vanaf deze domeinnamen geblokkeerd kunnen worden binnen de eigen organisatie of waarschuwingen worden gegeven aan belangrijke relaties.

Bescherming tegen e-mail spoo□ng (vervalsing)

E-mail spoofing: techniek waarbij een afzender van een mail of de makers van een site zich voordoen als iemand anders of een ander bedrijf of instelling.

Er zijn diverse technieken ontwikkeld die een organisatie helpen zich te beschermen tegen misbruik van hun domeinnamen door spoo□ng. Het betreft:

1. ***Sender Policy Framework (SPF)***. SPF geeft via een zogenaamd Domain Name Service (DNS) record van het domein aan welke servers gemachtigd zijn om mail te versturen namens dit domein. In dit record wordt tevens aangegeven wat de ontvangende partij met de e-mail kan doen (niets, softfail: markeren, hardfail: afwijzen).
2. ***Domain Keys Identified E-mail (DKIM).*** DKIM stuurt in elke mail een digitale sleutel en een adres mee. Hierdoor kan de ontvanger vaststellen of de mail daadwerkelijk van de verzender afkomstig is.
3. ***Domain-based Message Authentication, Reporting, and Conformance (DMARC).*** DMARC geeft aan wat volgens de eigenaar van de betreffende domeinnaam moet gebeuren met e-mails die niet voldoen aan de gepubliceerde SPF record en de meegestuurde DKIM-sleutel. Een dergelijke mail kan bijvoorbeeld in quarantaine worden gezet of worden geweigerd door de ontvangende mailserver.

Voor optimale beveiliging tegen spoo□ng is het van belang dat de drie technieken in onderlinge samenhang worden gebruikt. Daarbij is het belangrijk dat de verantwoordelijke voor een domein de juiste SPF, DKIM en DMARC instellingen con□gureert en dat de ontvangende mailserver hierop controleert en vervolgens actie neemt als er twijfel bestaat over de herkomst van de betreffende mail. Hiermee is bescherming tegen spoo□ng dus een gezamenlijke inspanning van zowel de verzendende als de ontvangende partij. Als de ontvangende mailserver geen controle heeft ingebouwd, worden vervalste e-mails van organisaties die deze technieken wel gebruiken dus gewoon afgeleverd en wordt de herkenning geheel overgelaten aan de eindgebruiker.

Hieruit volgt de logische conclusie dat **alleen** het instellen van SPF, DKIM en DMARC geen goede bescherming biedt tegen spoo□ng en phishing. Het is echter een goede eerste stap in een pakket van maatregelen om een organisatie weerbaarder te maken op dit gebied. Welke andere zaken belangrijk zijn wordt verder toegelicht in de aanbevelingen.

Tot slot wordt opgemerkt dat ook domeinnamen die geen mailserver hebben gecon□gureerd toch misbruikt kunnen worden voor spoo□ng. Voor buitenstaanders kunnen e-mails van dat soort domeinen er geloofwaardig uitzien. Het is daarom verstandig om SPF en DMARC ook in te stellen voor domeinen zonder mailserver.

Op 28 oktober 2015 publiceerde het Nationaal Cyber Security Center (NCSC) al een factsheet over het gebruik van SPF, DKIM en DMARC technieken en hoe bepaalde praktische uitdagingen daarbij het hoofd te bieden. Het Forum Standaardisatie, die de lijst met verplichte open standaarden die gelden voor de gehele publieke sector beheert, heeft het gebruik van SPF en DKIM binnen de overheid verplicht gesteld en de verwachting is dat ook DMARC binnenkort aan deze zogenaamde pas-toe-of-leg-uit lijst zal worden toegevoegd.

Kwetsbaarheid Nederlandse organisaties voor e-mail phishing

Effectieve technische bescherming tegen phishing begint met bescherming tegen spoo□ng. Zoals eerder in dit rapport toegelicht, helpt deze bescherming alleen als zoveel mogelijk organisaties gebruik gaan maken van SPF, DKIM en DMARC, zowel voor het verzenden van e-mails, als bij het controleren van binnenkomende e-mails. Met name SPF en DMARC zijn over het algemeen eenvoudig te con□gureren. DKIM kan lastiger te con□gureren zijn omdat niet alle mailservers (waaronder Exchange) DKIM standaard ondersteunen en additionele tooling nodig is om de digitale sleutels aan de uitgaande e-mails toe te voegen.

Om een beeld te krijgen van de actuele kwetsbaarheid van Nederlandse organisaties voor e-mail spoo□ng heeft Hoffmann onderzocht in hoeverre deze organisaties nu al gebruik maken van anti-spoo□ng instellingen. Hoffmann heeft een scan uitgevoerd op in totaal 26.734 domeinnamen van Nederlandse organisaties. Bij al deze organisaties is gecontroleerd in hoeverre zij gebruik maken van Sender Policy Framework (SPF) records en Domain-based Message Authentication, Reporting, and Conformance (DMARC). Het derde protocol, DKIM, is niet getest. Een passieve manier van testen is voor DKIM niet mogelijk.

Bij DKIM wordt een digitale sleutel toegevoegd aan een uitgaande e-mail en zou dus een daadwerkelijke recente e-mail van alle onderzochte 26.734 domeinnamen nodig zijn om deze test uit te kunnen voeren. Het verkrijgen van deze e-mails gaat voorbij aan het non-intrusive karakter van dit onderzoek en is daarom achterwege gelaten. De scan is uitgevoerd op 24 mei 2016.

De resultaten van het onderzoek zijn ontluisterend. Van de onderzochte domeinnamen heeft **59,4% het SPF record niet of onjuist ingesteld**. In totaal **98,4% van de onderzochte domeinnamen heeft geen DMARC record ingesteld**. Een klein deel betrof domeinnamen waarop geen mailserver is ingesteld (getest via het MX_RECORD). Echter, ook deze domeinnamen zijn bij een ontbrekend SPF en DMARC record kwetsbaar voor spoo□ng, zoals in het vorige hoofdstuk is toegelicht. Deze zijn dus meegenomen in de totale resultaten zoals hiervoor genoemd.

Top 3 opvallende sectoren

Van de 26.734 geteste domeinnamen zijn er 24.413 ingedeeld in 60 verschillende sectoren. Omdat vrijwel geen van de onderzochte domeinnamen gebruik maakt van DMARC gaan de onderstaande statistieken alleen over de SPF records.

De drie meest opvallende sectoren zijn:

1. **Gezondheids- en welzorg.** Het betreft ziekenhuizen, verzorgingstehuizen, praktijken van zorgverleners en andere organisaties die actief zijn in het zorgdomein. Van de 15.341 onderzochte domeinnamen hebben er 66,8% geen of geen juist SPF-record ingesteld.
2. **Openbaar bestuur.** Hieronder vallen de nationale overheid, gemeenten en provincies. Alle gemeenten met een geregistreerde domeinnaam, alle provincies en alle ministeries zijn in het onderzoek meegenomen. Van de in totaal 1.591 onderzochte domeinnamen hebben er eveneens 66,8% geen of geen juist SPF-record ingesteld.
3. **Overige zakelijke dienstverlening.** Het gaat hier om zakelijke dienstverleners zoals bijvoorbeeld advocatenkantoren en accountants. Van de 1.822 onderzochte domeinnamen hebben er 52,4% geen of geen juist SPF-record ingesteld.

Andere opvallende sectoren

- Zoals verwacht maken veel ICT organisaties inmiddels gebruik van SPF. Echter, nog steeds heeft 34,8% van de 904 geteste domeinnamen in deze sector geen of geen juist SPF-record ingesteld.
- In de sector dienstverlening ten behoeve van vervoer heeft 40,5% van de 934 onderzochte domeinnamen geen of geen juist SPF-record ingesteld.
- De meeste banken en andere financiële instellingen maken gebruik van SPF-records. Toch zijn er nog enkele organisaties in deze sector die (sub)domeinen niet goed hebben ingesteld op het gebied van SPF.
- In de vitale sector zijn gelukkig veel goede voorbeelden. Ook daar zijn er echter organisaties, zoals enkele telecomproviders, olieproductiebedrijven, elektriciteitsbedrijven, nucleaire voorzieningen en drinkwatervoorzieningen die geen SPF-record hebben ingesteld.
- In de onderzochte overheidsdomeinen valt op dat er organisaties zijn in het domein openbare orde en veiligheid, zonder SPF-record. In sommige gevallen komt dit doordat de betreffende domeinen alleen een website hosten. Ook dan zijn zij, zoals eerder in dit rapport toegelicht, kwetsbaar voor e-mail spoofing.

Tot slot moet opgemerkt worden dat in alle sectoren belangrijke organisaties zijn die kwetsbaar zijn voor e-mail spoofing. In het worst case scenario kan een kwaadwillende, met de informatie die Hoffmann in dit onderzoek beschikbaar heeft, deze organisaties gebruiken als stepping stones bij een complexe operatie met als doel de samenleving te ontwrichten. Hoewel het niet aannemelijk is dat zo'n scenario snel optreedt, is het belangrijk vast te stellen dat Nederland hier als gevolg van onvoldoende maatregelen op dit gebied, wel kwetsbaar voor is.

Impact van recente mediaberichten op gebruik van SPF en DMARC

Na de berichtgeving van Binnenlands Bestuur op 2 juni 2016 over het ontbreken van SPF, DKIM en DMARC bij veel Nederlandse gemeenten, is een tweede scan uitgevoerd op 9 juni 2016 om vast te stellen in hoeverre de media-aandacht heeft geleid tot verbeterd gebruik van de genoemde technieken.

Na de berichtgeving in de media is er slechts een kleine verbetering te zien, met name bij Nederlandse gemeenten. In totaal zijn er 133 organisaties die sinds de berichtgeving een SPF-record hebben ingesteld binnen dezelfde testset, een toename van 0,5%. Daarnaast zijn 37 nieuwe DMARC records ingesteld. De grootste toename is te zien bij gemeenten; 25 gemeenten hebben sinds de berichtgeving SPF ingesteld en 22 gemeenten DMARC. Verder valt op dat sinds de berichtgeving 47 zorg- en welzijnsinstellingen een SPF-record hebben aangemaakt. Dus ook in die sector heeft de berichtgeving kennelijk een positief effect gehad.

Aanbevelingen

Gezamenlijk spoo□ng tegengaan

Zoals met veel beschikbare standaarden voor beveiliging, geldt ook voor SPF, DKIM en DMARC dat deze nog onvoldoende geadopteerd zijn in de markt. Hoffmann adviseert organisaties om hun beleid hieromtrent te herzien. Als organisaties breed maatregelen treffen om e-mail spoo□ng tegen te gaan, wordt Nederland als geheel weerbaarder op gebied van e-mail phishing. Met name SPF en DMARC zijn redelijk eenvoudig te con□gureren. DKIM is in sommige gevallen lastiger te con□gureren, als de gebruikte mailserver dit niet ondersteunt, of als andere organisaties uit jouw naam mogen mailen. Aan dit laatste aspect wordt nog gewerkt door de IETF DMARC Working Group. Overigens vindt Hoffmann het opvallend dat het gebruik van SPF en DMARC sinds 2012 verplicht is voor overheidsinstellingen onder “pas toe of leg uit” en dat met name zij dus beter hadden kunnen en (kennelijk) moeten weten.

Effectieve bescherming tegen phishing: mens/techniek/organisatie

Niet alleen technische maatregelen helpen een organisatie zich beter te beschermen tegen phishing. Zoals toegelicht bieden technieken zoals SPF, DKIM en DMARC maar beperkte bescherming tegen phishing middels spoo□ng, zeker zolang deze technieken nog maar door een kleine groep van organisaties zijn geadopteerd.

Het is daarom belangrijk om te kiezen voor een integrale aanpak, niet alleen gericht op techniek, maar vooral ook op het inrichten van de juiste processen en om medewerkers te leren hoe zij zich zo veilig mogelijk kunnen gedragen in hun communicatie.

Ten aanzien van de medewerkers helpen bewust-wordings-campagnes als eerste stap, bijvoorbeeld door uit te leggen hoe een medewerker een phishing-bericht kan herkennen. Het is verstandig deze bewustwording onderdeel te maken van een cultuurverandering binnen de organisatie, gericht op veilig gedrag. Hier kan het helpen de medewerkers er op te wijzen dat het iedereen kan gebeuren en dat het dus belangrijk is dat zij een melding maken dat het is gebeurd en niet uit angst voor de gevolgen een onhandige actie op dit gebied verzwijgen.

Tegelijkertijd is het goed om ook de benodigde processen adequaat in te richten. Bijvoorbeeld een proces dat vastlegt wat er in een organisatie moet gebeuren zodra een phishing mail is gedetecteerd. Zo’n proces gaat niet alleen over het afhandelen van de speci□eke risico’s als iemand op een bijlage heeft geklikt, maar ook over het informeren van de rest van de organisatie over zo’n bericht, het instrueren van de helpdesk, etc. Verder is het belangrijk een goede back-up procedure te hebben. Organisaties die verder gaan in hun aanpak, zouden bestanden alleen nog maar via een uitwisselingsdienst kunnen versturen, waardoor klikken op attachments helemaal niet meer nodig is.

Ook met een goede mix van maatregelen blijft phishing een reëel risico. Het is daarom verstandig om van tijd tot tijd de genomen maatregelen te evalueren en te vernieuwen waar nodig.

Bescherming e-mail communicatie

Er valt nog veel meer te zeggen over beveiliging van e-mail communicatie, breder dan alleen phishing. Technische oplossingen zoals SMTPS, DNSSEC, PGP en STARTTLS komen dan in beeld. Dit onderzoek gaat daar verder niet op in, maar het verdient de aanbeveling om vanuit een risico inventarisatie te bezien welke maatregelen noodzakelijk zijn voor een goede bescherming van de gevoelige gegevens binnen een organisatie.

Zelf controleren?

Om te controleren welke beveiligingsmaatregelen uw organisatie heeft genomen kunt u bijvoorbeeld gebruik maken van:

- www.internet.nl
- www.phishingscorecard.com

Dit soort sites geven een eerste inzicht in technische maatregelen die binnen uw organisatie zijn toegepast.

Bijlage A - gebruikte bronnen

- Diverse beschikbare (open) bronnen waaruit een lijst met domeinnamen van 26.734 Nederlandse organisaties is samengesteld.
- Pas toe of leg uit lijst van Forum Standaardisatie: https://www.forumstandaardisatie.nl/ptolu
- PhishMe kwartaal rapport Q1 2016: http://phishme.com/phishme-q1-2016-malware-review/
- Phishing rapporten APWG: https://www.apwg.org/resources/apwg-reports/
- Factsheet ‘Bescherm domeinnamen tegen phishing’ van Nationaal Cyber Security Centrum: https://www.ncsc.nl/actueel/factsheets/factsheet-bescherm-domeinnamen-tegen-phishing.html

Hoffmann

Luidsprekerstraat 10 - 1322 AX Almere
Postbus 60090 - 1320 AB Almere

www.hoffmannbv.nl