Fraudepreventie tegen phishing en pharming

Ir. ing. J.J.C. Steevens

Identiteitsdiefstal is al jaren een bekend fenomeen. Desondanks heeft phishing pas in de laatste twee à drie jaar veel aandacht gekregen in het landelijke nieuws. Dit artikel beoogt duidelijkheid over de werking van phishingaanvallen te geven en daarnaast aan te geven wat betrokken partijen kunnen doen om te voorkomen dat phishing en pharming succesvol zijn.

Inleiding

Het woord *phishing*, met de karakteristieke 'ph' erin, is afgeleid van de termen 'password harvesting' (ph) en 'fishing' en stamt uit de tijd toen inbelgegevens van AOL gestolen werden om gratis internettoegang te verkrijgen ([APWG07]). Het is een fenomeen dat zich de afgelopen jaren voornamelijk in de financiële sector als een serieus probleem heeft gemanifesteerd.

Met de term phishing wordt in essentie bedoeld: 'op digitale wijze 'stelen' van gevoelige informatie (zoals creditcardnummers, sofinummers, inloggegevens, etc.) van individuen met behulp van vervalste e-mails'. Men tracht een gebruiker met behulp van een authentiek lijkende e-mail te bewegen persoonlijke gegevens direct via e-mail of via een vervalste website in te voeren, waardoor deze in de handen van personen terechtkomen die hiermee vervolgens fraude trachten te plegen.

Misbruik op deze wijze is aanlokkelijk omdat veel authenticatiemethoden zijn gebaseerd op een authenticatiefactor die iemand *weet*. Er worden in de praktijk drie soorten factoren onderscheiden: iets wat je *hebt* (een pasje), iets wat je *bent* (vingerafdruk) en iets wat je *weet* (wachtwoord). Een wachtwoord kan, indien gestolen, door een derde worden gebruikt om toegang te verkrijgen tot alle functionaliteiten waartoe de oorspronkelijke eigenaar geautoriseerd is, inclusief het uitvoeren van bijvoorbeeld financiële transacties uit naam van die gebruiker.

Naast phishing bestaat het fenomeen *pharming*. Pharming is geen aanval op zich maar wordt gebruikt als technische component in een phishingaanval. Er bestaat daarom niet zoiets als een pharmingaanval. Het doel van pharming is ervoor te zorgen dat de vertaling van internetnamen (DNS-namen) naar internetadressen (IP-adressen) voor een gebruiker anders verloopt dan normaal. Dit is mogelijk door het wijzigen van instellingen op de computer (de hostfile of DNS-server) met behulp

Ir. ing. J.J.C. Steevens
is junior adviseur in de groep ICT Security and Control van KPMG IT Advisory in Amstelveen. Hij is verantwoordelijk voor het geven van adviezen met betrekking tot authenticatiesystemen en autorisatiemanagement en daarnaast voor het uitvoeren van IT-audits. Zijn expertise is voornamelijk gericht op Identity en Access Management, authenticatiesystemen, Public Key Infrastructures en IT-auditing.

steevens.jules@kpmg.nl

van een Trojan óf door het hacken van de DNS-server van de gebruiker. DNS-vertaling is een belangrijk proces omdat dit ervoor zorgt dat een gebruiker die 'www.fictievebank.nl' benadert op de juiste webserver terechtkomt. In het geval van pharming kan een aanvaller de DNS-vertaling in een computer zo aanpassen dat bij het intypen van 'www.fictievebank.nl' in de webbrowser de gebruiker niet uitkomt bij de originele website maar bij een aangepaste website gemaakt door de aanvaller.

Dit artikel gaat verder met de werking van phishingaanvallen en maatregelen die kunnen worden getroffen om phishing en pharming tegen te gaan.

Achtergrond

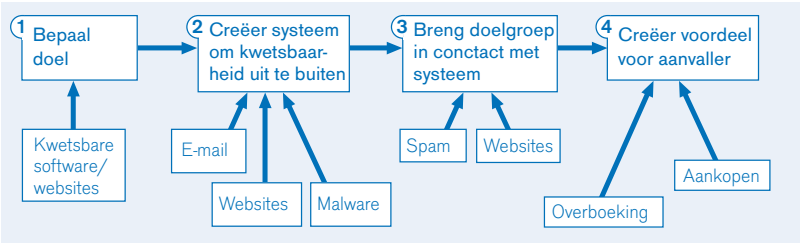
De basisopzet van een phishingaanval bestaat uit vier stappen, geïllustreerd in figuur 1:
1. bepalen van een doelgroep en kwetsbaar systeem;
2. creëren van een systeem om de kwetsbaarheid uit te buiten;
3. doelgroep in contact brengen met het systeem;
4. creëren van voordeel voor de aanvaller.

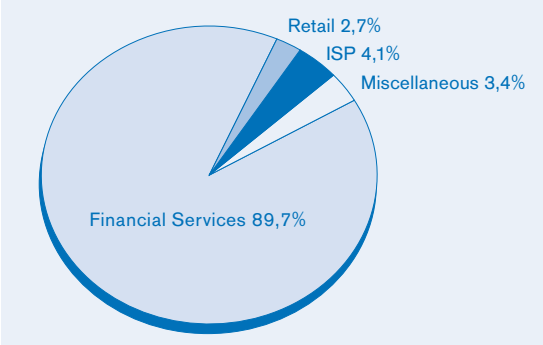
Stap 1. Bepaal doel

Om een succesvolle aanval op te zetten is in eerste instantie een tekortkoming in het systeem van een bedrijf nodig waardoor uiteindelijk fraude kan worden gepleegd. Deze zwakke plek kan zich praktisch overal in het bedrijf bevinden, hoewel in de context van phishing het meestal een zwakke plek betreft die vanaf het internet uit te buiten is. De keuze voor internet heeft als voordeel voor de aanvaller dat de communicatie lastig te traceren is naar de afzender én dat personen in het buitenland juridisch lastig te vervolgen zijn.

Voorbeelden van tekortkomingen zijn: een eenvoudig te omzeilen authenticatiesysteem, fouten in de website voor internetbankieren en het handelen van gebruikers. Het laatste voorbeeld moet genuanceerd worden. Wat bedoeld wordt is: indien een gebruiker verleid wordt zijn wachtwoord kenbaar te maken kan er eenvoudig fraude worden gepleegd. Hierbij moet vermeld worden dat gebruikers vaak beperkt in staat zijn legitieme websites van de valse website te onderscheiden ([Soni07]).

Figuur 1. Basisopzet van een phishingaanval.





Figuur 2. Sectoren waarop phishingaanvallen zijn gericht ([APWG07]).

De doelgroep van phishingaanvallen bestaat in de meeste gevallen uit klanten van een financiële instelling, bijvoorbeeld gebruikers van internetbankieren. De rapportages die maandelijks door de Anti Phishing Working Group worden uitgegeven, geven al maandenlang aan dat het overgrote deel (bijna negentig procent, zie ook figuur 2) van alle aanvallen is gericht op financiële instellingen.

Stap 2. Creëer een systeem om kwetsbaarheid uit te buiten

Om de tekortkoming uit te buiten zijn specifieke 'gevoelige' gegevens nodig. Voorbeelden hiervan zijn rekeningnummers, creditcardnummers, pincodes, inlognamen en wachtwoorden. Om deze gegevens van een persoon te stelen moet de aanvaller een manier ontwikkelen waarop de gebruiker deze gegevens kenbaar maakt. Belangrijke gevoelige gegevens worden normaliter niet zomaar afgegeven door personen. Er moet een goede aanleiding zijn om een persoon te verleiden deze informatie toch te geven.

De manier waarop aanvallers hun doelgroep aanvallen is continu aan verandering onderhevig. De basis van praktisch elke phishingstrategie berust op gebruik van een e-mail die de gebruiker overtuigt om een (vervalste) website te bezoeken waarop een pagina wordt gepresenteerd die de bezoeker vraagt om een aantal specifieke gegevens in te vullen. De vervalste website wordt getoond in plaats van de legitieme website die de gebruiker verwacht.

Een voorbeeld van een technologische vernieuwing in een phishingaanval is pharming, een techniek die gebruikmaakt van wijzigingen in het DNS-vertaalsysteem om internetgebruikers naar de vervalste website te dirigeren. In de volgende paragrafen wordt op phishing en pharming dieper ingegaan.

Stap 3. Breng doelgroep in contact met het systeem

De doelgroep wordt in een phishingaanval benaderd door middel van een e-mail. Omdat het voor aanvallers

moeilijk is om een goede set e-mailadressen met klanten van de betreffende instelling te verzamelen, wordt met een grootschalige set (dergelijke sets worden vaak ook gebruikt om spam te versturen) gehoopt dat men ook een behoorlijk aantal klanten zal raken. Phishing-aanvallen gaan daarom vaak gepaard met grootschalige e-mailgolven.

In enkele gevallen zijn aanvallers in staat het klantenbestand van een instelling te bemachtigen, waardoor het effect van de aanval vele malen groter wordt.

Stap 4. Creëer voordeel voor de aanvaller

Het 'voordeel' dat een aanvaller kan creëren hangt af van het type gegevens dat hij buit heeft gemaakt. Zoals eerder is aangegeven, trachten de meeste aanvallers te frauderen bij financiële instellingen. Het doel is om financiële middelen van de slachtoffers af te boeken richting de aanvallers.

De aanvaller wil het geld naar zich toe laten komen zonder dat zijn identiteit bekend wordt. Omdat financiële instellingen transactieverkeer monitoren en rekeningen op naam staan is het onmogelijk om geld niet-traceerbaar over te boeken. Een veelgebruikte strategie is het gebruik van zogenaamde intermediairs, ook wel oneerbiedig 'mules' genoemd. Deze intermediairs sturen het geld op contante wijze, door middel van een 'international money transfer', in een keten van andere intermediairs door naar de eindbestemming. Een 'international money transfer' betaalt een aangeboden hoeveelheid geld, contant of giraal, in het buitenland aan een andere persoon contant uit. De eindbestemming van het geld is uiteindelijk een persoon dicht bij de aanvaller die het geld fysiek overbrengt.

De werkwijze rondom het gebruik van intermediairs is als volgt. De intermediairs worden geronseld via valse banenwebsites waar ze veel geld wordt beloofd om een 'internationaal georiënteerde' baan aan te nemen ([Ollm05]). De intermediair wordt geïnstrueerd om een nieuwe bankrekening te openen bij de aan te vallen financiële instelling. De aanvallers boeken vervolgens het geld van de rekening van het phishingslachtoffer naar de zojuist geopende rekening van de intermediair. De intermediair krijgt de instructie om het geld op te nemen, minus zijn 'commissie', en door te sturen via een 'international money transfer' naar een andere intermediair. Met gebruik van elke volgende intermediair komt het geld dichter bij de aanvaller. Uiteindelijk wordt het geld fysiek aan de aanvaller overgedragen.

Tracering van het spoor door de banken en/of politie levert, als de hiervoor beschreven methode is gevolgd, alleen tussenpersonen op die weinig tot niets van de algehele fraude weten.

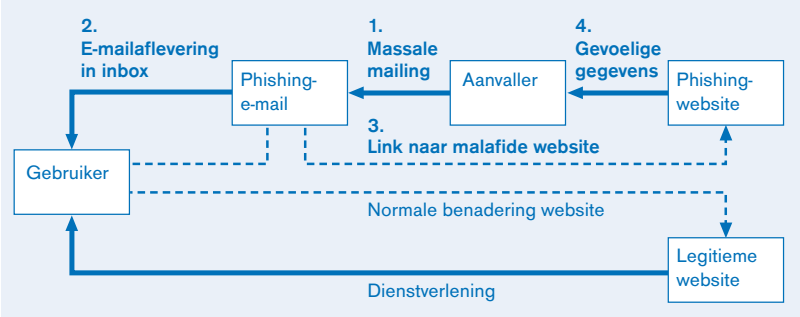
Techniek achter phishing en pharming

Er zijn twee aanvalsvarianten te identificeren. De eerste, oudste en meest gebruikte variant maakt alleen gebruik van een e-mail die de gebruiker overtuigt om 'de website van de bank' te bezoeken. De tweede variant maakt gebruik van een aanpassing in het DNS-vertaalsysteem om internetgebruikers naar valse webpagina's te dirigeren. Beide varianten worden hier verder uitgewerkt.

Variant 1. E-mail + website

De eerste variant start met het massaal verzenden van een e-mail naar internetgebruikers, vergelijkbaar met spam (zie ook figuur 3). De e-mail heeft als doel de internetgebruikers te verleiden om de phishingwebsite te bezoeken. Een nadeel van het massaal verzenden van e-mail is dat het zeer waarschijnlijk is dat een groot deel van de ontvangers geen klant is van de betreffende instelling.

Het potentiële slachtoffer wordt een link aangeboden in de e-mail die uitkomt op een website gecreëerd door de aanvaller. Deze website is er volledig op gericht om een gebruiker het idee te geven dat hij op de website van de betreffende instelling komt. Daar aangekomen wordt de bezoeker gevraagd om een set persoonlijke gegevens in te vullen en te versturen. Het proces eindigt nadat de ingevulde gegevens vanaf de website automatisch naar de aanvaller zijn gestuurd.

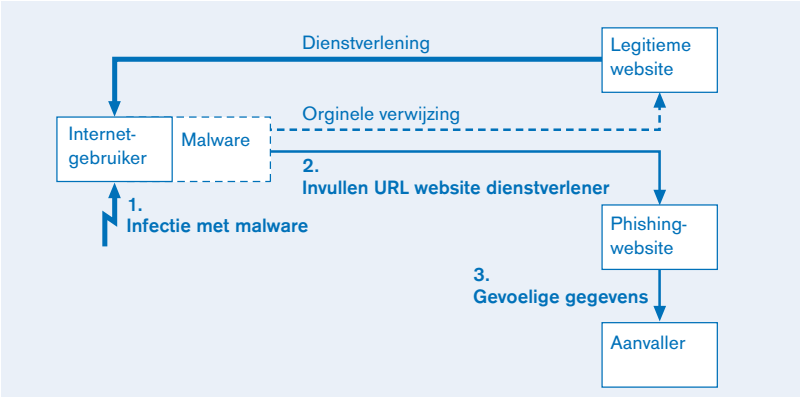


Figuur 3. Werking misleidende e-mail met vervalste website.

Variant 2. Vervalste DNS-informatie + website

In de tweede variant wordt geknoeid met de DNS-vertaling van de internetgebruiker (pharming). Door deze onjuiste vertaling kan een internetgebruiker op een andere website uitkomen dan normaal, ook als hij netjes zelf het adres van zijn bank foutloos intypt. In deze uitwerking wordt ervan uitgegaan dat instellingen op de computer van de gebruiker gewijzigd zijn. In werkelijkheid kan de wijziging ook plaatsvinden op de DNS-server van de internet service provider.

In figuur 4 is geïllustreerd dat een internetgebruiker tracht een legitieme website te openen. Door de gewijzigde DNS-vertaling zal de oproep voor www.fictievebank.nl niet uitkomen op de legitieme website maar op de vervalste website van de aanvaller.



Figuur 4. Werking vervalste DNS-informatie en vervalste website.

Het vervolg is analoog aan de website van variant 1. De vervalste website zal de gebruiker uitnodigen om informatie in te vullen die na verzending doorgestuurd zal worden naar de aanvaller.

Relevante actoren

Bij een phishingaanval zijn meer partijen betrokken dan de aanvaller (de fraudeur) en zijn slachtoffer (de internetgebruiker en het bedrijf). De volgende actoren kunnen als relevant worden betiteld in een phishingaanval en de afwikkeling ervan:

- *Internetgebruikers*. Internetgebruikers vormen de kwetsbare groep voor phishingaanvallers.
- *Phishingaanvallers*. Deze mensen trachten op digitale wijze gegevens van internetgebruikers afhandig te maken met het doel fraude te plegen.
- *Bedrijven*. Bedrijven die financieel-gerelateerde diensten aanbieden of gevoelige gegevens registreren op internet zijn een potentieel slachtoffer van phishingaanvallen richting hun klanten.
- *Internet Service Providers*. ISP's zijn de transporteurs voor het internetverkeer en daarmee de spil in het internet. Vanuit deze rol hebben zij raakvlakken met vrijwel alle partijen in deze problematiek, wat hen in zekere mate een morele verantwoordelijkheid geeft om iets met deze problematiek te doen.
- *Overheid*. De overheid heeft als wetgevende instantie de verplichting om de regels op een dusdanige manier in te richten dat crimineel gedrag vervolgd kan worden. De taak van de wetsuitvoerende tak van de overheid is om preventief en repressief op te treden tegen fraudeurs. In de praktijk wordt het repressieve optreden op internet, zoals het uit de lucht halen van een phishingwebsite, door de ISP's gedaan. Vanuit bestuurlijk oogpunt heeft de overheid de verantwoordelijkheid om burgers voor te lichten over eventuele bedreigingen en hen daartegen te beschermen.

Mogelijke tegenmaatregelen

In deze paragraaf wordt ingegaan op mogelijkheden die actoren uit de voorgaande paragraaf hebben om te voorkomen dat zij slachtoffer worden van phishing én om phishing in z'n totaliteit tegen te gaan. De phishingaanvallers zijn niet meegenomen omdat we ervan uitgaan dat deze groep geen maatregelen tegen zichzelf zal nemen.

Gebruikers

Alle courante webbrowsers zijn op dit moment geschikt voor het gebruik van anti-phishing toolbars. Deze plugins geven de gebruiker een risico-indicatie van een benaderde website. Anti-phishing toolbars gebruiken onder andere achtergrondinformatie over het IP-adres van de website, ervaringsinformatie van andere gebruikers, tekstanalyse en een zwarte lijst met IP-adressen en domeinnamen van bekende phishingwebsites om de betrouwbaarheid van de website te beoordelen. De praktijk leert dat deze plugins een vrij goede inschatting maken.

Door het installeren van beveiligingssoftware (virusscanner en firewall) kan een behoorlijke bescherming worden bereikt tegen virussen, Trojans en aanverwante software die de correcte werking van de computer verstoren. Dit is van belang om te voorkomen dat er met de DNS-vertaling in het systeem kan worden geknoeid. Een voorwaarde om een acceptabel veiligheidsniveau te creëren is dat virusscanner én firewall up-to-date worden gehouden. Naast beveiligingssoftware is het een goede gewoonte om ook het besturingssysteem regelmatig van de laatste updates te voorzien. Hierdoor worden beveiligingslekken gedicht wat de infecteerbaarheid van de computer beperkt.

Qua gedrag is het belangrijk dat gebruikers kritisch zijn over de afgifte van persoonlijke gegevens. Daarnaast is het een goede gewoonte om bij de keuze voor een nieuwe bank of dienst ook het veiligheidsbeleid mee te nemen in de evaluatie.

Bedrijven

Bedrijven hebben als dienstverlenende partij een scala aan mogelijkheden om te detecteren en te voorkomen dat klanten slachtoffer worden van phishing.

Op technologisch vlak:

- Bedrijven dienen de eigen website en het internet te monitoren voor potentieel frauduleuze activiteiten jegens het eigen bedrijf. In het geval dat het bedrijf met dergelijke activiteiten wordt geconfronteerd, kan gepaste actie worden ondernomen om de activiteit tegen te gaan. Er kan bijvoorbeeld worden getracht de betrokken computers met hulp van ISP's offline te brengen. Zowel het monitoren als het offline brengen van computers

wordt door gespecialiseerde bedrijven als dienst aangeboden.
- Door een hoogwaardig authenticatieproces op de gebruiker toe te passen wordt een grote mate van zekerheid verkregen over de identiteit van de persoon die inlogt. De kwaliteit van een authenticatieproces wordt bepaald door enerzijds de sterkte van het authenticatiemiddel en anderzijds de waarborging in het uitgifteproces. Elk authenticatiemiddel, bijvoorbeeld een wachtwoord, token, smartcard of combinatie van middelen, geeft een andere mate van zekerheid over de vraag of de gebruiker die zich aanmeldt ook de gebruiker is die het middel uitgereikt heeft gekregen. Het uitgifteproces geeft een mate van zekerheid dat het authenticatiemiddel is uitgereikt aan de persoon die eigenaar van het account is.
- In lijn met het vorige punt wordt de veiligheid verhoogd door het toepassen van transactieverificatie of -authenticatie. Door deze maatregel valideert de gebruiker expliciet elke (set van) transactie(s) die plaatsvindt op zijn account. Bekende werkwijzen zijn SMS of een token. Hierdoor heeft de gebruiker de mogelijkheid om, door phishingaanvallers, geïnjecteerde transacties op te merken. Transactieverificatie complementeert sterke authenticatie.
- Standaard SSL-certificaten worden door websites gebruikt om sessies met de gebruiker te versleutelen en om zichzelf te identificeren aan de gebruiker. De nieuwe variant (Extended Validation SSL) certificaten kent een strikter gecontroleerd uitgifteproces waardoor deze een grotere mate van zekerheid biedt dan normale SSL-certificaten. In dit verbeterde uitgifteproces worden de identiteit en autoriteit van de aanvrager beter geverifieerd en wordt er onderzocht of er verwarring met bestaande namen kan ontstaan. Extended Validation SSL-certificaten worden inmiddels door de meeste partijen aangeboden hoewel deze significant duurder zijn dan SSL-certificaten.
- Door het intensief monitoren van transacties kunnen frauduleuze en verdachte transacties worden opgemerkt en kunnen gepaste maatregelen worden genomen. Fraudedetectie kan worden gebaseerd op kenmerken van een transactie. Voorbeelden hiervan zijn: geografische locatie van de gebruiker, tijdstip van transactie, gebruikt IP-adres, bestemming van de transactie, hoogte van het bedrag, etc.

Op procesmatig vlak:
- Gepersonaliseerde communicatie naar klanten bevordert het gevoel van veiligheid in e-mailcommunicatie. Ongepersonaliseerde e-mailcommunicatie wordt hierdoor impliciet minder betrouwbaar dan gepersonaliseerde.
- Actieve voorlichting richting gebruikers over de basisprincipes van veilig online bankieren is een algemeen toepasbare tegenmaatregel. Dit is eerder met de pincode gedaan waardoor iedereen deze als een belangrijke sleutel tot dienstverlening is gaan beschouwen.
- Het stimuleren van klanten om beveiligingssoftware te gebruiken bevordert de veiligheid van systemen van gebruikers. Een bedrijf kan, als voorbeeld, ter stimulering van het gebruik van beveiligingssoftware korting geven op software in samenwerking met een softwareleverancier.

Overheid

De overheid is in haar hoedanigheid beperkt tot juridische maatregelen en voorlichting, mede doordat zij geen direct raakvlak met de phishingaanval heeft.

Nederland kent sinds enkele jaren wetgeving die ruimte biedt om digitale fraudeurs te vervolgen. Waar het op dit moment nog aan schort is voldoende capaciteit en prioriteit ter vervolging van digitale criminaliteit en internationale samenwerking. Voor digitale criminaliteit is het kenmerkend dat opsporing tijdintensief is en criminelen zich vrijwel altijd in andere landen bevinden waar wetgeving op het gebied van digitale criminaliteit vaak minder volwassen is dan in de Europese landen.

Ter preventie van digitale criminaliteit zijn er legio kanalen om burgers voor te lichten hoe zij het beste kunnen omgaan met onlinediensten en internetbankieren. Voorbeelden van deze kanalen zijn: Postbus 51, Digibewust.nl en Waarschuwingsdienst.nl.

Momenteel schort het nog aan voldoende capaciteit en prioriteit ter vervolging van digitale criminaliteit

Internet Service Providers

De volgende *technologische maatregelen* kunnen door ISP's worden genomen:
- ISP's zijn in staat malafide e-mailverkeer te filteren. E-mail is onder andere te filteren op basis van zogenaamde 'zwarte lijsten' en tekstanalyse. De meeste ISP's bieden al een bepaalde vorm van e-mailfiltering aan.
- ISP's dienen garant te staan voor de juiste werking van hun infrastructuur. Daarbij ligt de nadruk op de DNS-functionaliteit die op juiste wijze internetnamen naar internetadressen vertaalt. Deze DNS-functie kan kwetsbaar zijn voor manipulatie (een vorm van pharming) waardoor alle gebruikers van de ISP onjuiste informatie kunnen krijgen over bepaalde domeinnamen.
- Om verspreiding van virussen, Trojans en aanverwanten tegen te gaan kunnen ISP's besmette computers in een quarantaine netwerk plaatsen. Hierdoor wordt de creatie van botnets en het versturen van spam sterk beperkt. Botnets zijn netwerken van geïnfecteerde computers die worden bestuurd door aanvallers.

Als *procesmatige maatregel* kunnen ISP's een rol spelen als meldpunt voor frauduleuze e-mail en kunnen zij beveiligingssoftware tegen gereduceerd tarief aanbieden.

Conclusie

De problematiek rondom phishing en pharming kenmerkt zich door een speelveld met meerdere gedeeltelijke probleemeigenaren. Het gedrag waarmee phishing en pharming tot uiting komt is moeilijk tegen te gaan door één enkele actor waardoor een collectieve aanpak logisch lijkt.

In het artikel is ook naar voren gekomen dat elke partij een beperkte set van maatregelen kent om een deel van het probleem op te lossen. Hoewel fraude een gedrag is dat niet geheel voorkomen kan worden, zowel in de fysieke als in de digitale wereld, is uit dit artikel gebleken dat er wel degelijk maatregelen genomen kunnen worden om fraude tegen te gaan. Door als collectief in het speelveld maatregelen en standaardwerkwijzen af te spreken is het mogelijk om phishing en pharming minder effectief te maken. Een voorwaarde hiervoor is dat bedoelde afspraken tussen alle relevante actoren worden gemaakt.

Literatuur

[Alla06] Ant Allan en Avivah Litan, *Transaction verification complements fraud detection and stronger authentication*, Gartner, september 2006.

[APWG07] Anti Phishing Working Group, www.antiphishing.org, geraadpleegd op 20-2-2007.

[APWG06] *Anti Phishing Working Group report*, december 2006.

[Lita06a] Avivah Litan, *How to evaluate combined fraud detection and authentication services*, Gartner, april 2006.

[Lita06b] Avivah Litan, *Phishing attacks leapfrog despite attempts to stop them*, Gartner, november 2006.

[Ollm05] Gunter Ollmann, *Next Generation Security Software Ltd.*, 27-9-2004, pagina 27, www.nextgenss.com/papers/NISR-WP-Phishing.pdf, geraadpleegd op 2-5-2005.

[Pesc07] John Pescatore, Avivah Litan, Vic Wheatman en Greg Young, *Extended Validation SSL certificates: A big step forward, but more progress is needed*, Gartner, februari 2007.

[Soni07] Sonicwall.com, *Phishing IQ Test - Find out how well you can recognize a Phishing email*, geraadpleegd op 17-3-2007.

[Stee05] J. Steevens, *Desktop Security - De bescherming van internetgebruikers tegen phishing*, Technische Universiteit Eindhoven, oktober 2005, www.justbiz.nl/personal/Eindscriptie_Jules_Steevens_Phishing.pdf.

[Wiki07] Wikipedia, *Phishing*, http://en.wikipedia.org/w/index.php?title=Phishing, geraadpleegd op 20-2-2007.