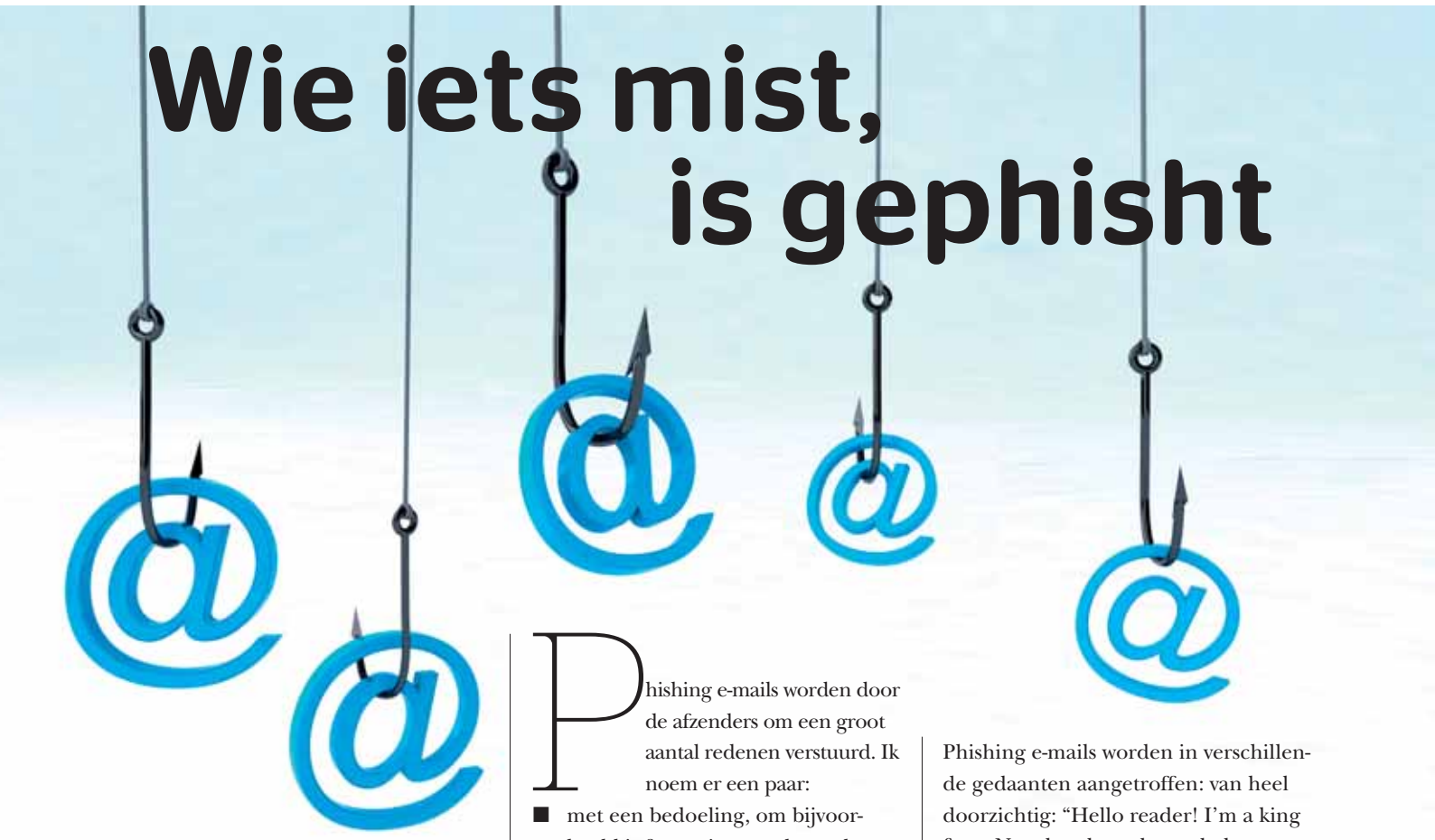
Wie iets mist, is gephisht



Security managers houden zich professioneel bezig met het beoordelen van risico's, het voorkomen van problemen en het weren van ongewenste situaties.Er is echter één piepklein risico'tje dat kan uitgroeien tot een serieus probleem. We hebben er allemaal last van – en juist daarom wordt er op dit moment nog niet veel aan gedaan: phishing e-mails.

tekst Hans Labruyère

Phishing e-mails worden door de afzenders om een groot aantal redenen verstuurd. Ik noem er een paar:

- met een bedoeling, om bijvoorbeeld informatie op te hengelen voor direct gebruik, of voor later);
- om systemen op termijn te kunnen platleggen;
- om een bot-net op te kunnen zetten;
- zonder bedoeling: gewoon omdat het kan (script-kiddies).

WAT IS PHISHING?

Phishing kan op veel manieren gebeuren: fysiek, telefonisch, online. Phishing e-mails zijn in de regel 'heel gewone' e-mails, die echter voorzien zijn van een extra feature. In veel gevallen wordt iets beloofd, als je maar snel actie onderneemt. Die actie kan van alles zijn: reactie op een webformulier, klikken op een link – wat dan ook.

De informatie die je achterlaat (je laat bijvoorbeeld door te klikken alleen al zien dat je bestaat en de mail leest) is vervolgens voor de aanvaller bruikbaar voor eventuele vervolgacties.

Phishing e-mails worden in verschillende gedaanten aangetroffen: van heel doorzichtig: "Hello reader! I'm a king from Nepal and need your help to get my gold! Read on!", tot heel geniepig en effectief: wie kent niet de verhalen over echt-lijkende bankmails waar toch nog steeds op geklikt wordt, terwijl iedereen wel zo'n beetje weet dat banken dat helemaal niet op die manier doen.

AprilAwareness 2014

Elk jaar voert LBVD een actie in het kader van AprilAwareness. Dit jaar was het onderwerp phishing e-mail. Een groot aantal opdrachtgevers deed mee, met verbazingwekkende resultaten: Gemiddeld 23% van de medewerkers klikte op de link, en ruim 80% van de digitale poorten werkte niet naar behoren.

Zijn we dan dom? Nee!

Cybercriminelen weten precies hoe ze je kunnen manipuleren. De e-mail en pagina waar je op terechtkomt nadat je op de link in de e-mail hebt geklikt, lijken vaak precies op die van de echte, betrouwbare organisatie. De boodschap is zo opgesteld dat je snel en zonder wantrouwen doet wat er staat.

Phishing-aanvallen worden op grote groepen gericht, maar ook op individuen in het geval van Spear Phishing. In dat geval is de aanvaller iets gerichts van plan. Dit soort aanvallen is vaak heel sluw opgezet, en voorzien van allerlei detailinformatie waardoor het slachtoffer niet doorheeft dat er met hem wordt gesold. En waar zou die informatie vandaan komen, denk je?

Eén van de redenen van het voortwoekeren van dit fenomeen is de relatieve succesfactor voor de crimineel. Voor de meeste digitale, gerichte aanvallen is één medewerker die klikt op de link die verstopt zit in de phishing-mail, genoeg. En met één druk op de knop kan de afzender tienduizenden mailtjes de deur uit doen. Zelfs met een ongehoord laag percentage klikkers is de reactie al gauw enkele tientallen.

IK BEN GEPHISHT - NOU EN?

Het risico van phishing is dat informatie onbedoeld in handen komt van derden. Dat hoeft niet eens 'geheime' informatie te zijn: je vult je NAW-gegevens meerdere malen per dag ergens in, soms compleet met banknummers en weet-ik-wat. Toch is die informatie waardevol – anders zoeken ze er niet naar. Die informatie kan een volgende keer worden gebruikt om geloofwaardiger over te komen en meer schade aan te kunnen richten.
Een ander risico is het installeren van software op je systeem die op zijn beurt weer allerlei narigheid kan veroorzaken. Bijvoorbeeld informatie ophengelen en doorspelen – maar dat is wel het minste. Denk nog eens aan Snowdon en de NSA.
Het risico achter bovenstaande risico's is zelfs nog groter: identiteitsfraude, onzekerheid omtrent bedrijfscontinuïteit, imagoschade, datacorruptie en ga zo maar door: big business, en risico's met grote geldstromen.

ZIJN WE DOM OF ONWETEND?

De oorzaak van dit 'succes' van de criminelen ligt vooral bij onwetendheid. Onwetendheid van de medewerker welk kwaad erin schuilt, onwetendheid waar vragen ophoudt en phishen begint, onwetendheid van de afdeling ICT rondom de effectiviteit van de aanvaller en de in-effectiviteit van tegenmaatregelen, onwetendheid van management om dit te onderkennen. Een medewerker mag er natuurlijk vanuit gaan dat de afdeling ICT de narigheid tegenhoudt, maar de keerzijde van die medaille is dat medewerkers dus overal op klikken wat in hun inbox verschijnt. Wie is nou onbewust-onbekwaam?

TOM POES, VERZIN EEN LIST!

Tegen phishing valt niet veel te doen: iemand die jou écht wil aanvallen, hou je niet tegen. Alle anderen kunnen we proberen te vinden – op tijd.
Het tegenhouden van phishing e-mails geschiedt voor een deel door de organisatie waar je werkt. Afdelingen als P&O en ICT hebben maatregelen bedacht en uitgewerkt om te voorkomen dat bedrijfsinformatie onopgemerkt de winkel verlaat. Thuis ben je echter je eigen systeembeheerder – en heb je nog steeds informatie van je werkgever in je hoofd. Je hebt dus als individu ook een taak, en een verantwoordelijkheid.

Wat je tegen phishing kunt doen is dit: oefenen. Tegen de lamp lopen en ervaring op doen helpt echt. Op enig moment word je het zat. En leer je kijken, in plaats van zien. Je leert horen in plaats van luisteren. Je leert phishingmailtjes ontdekken, je leert wanneer er iets 'niet in de haak' is. Dat is de harde manier.

KLIK JE BEWUST

Maar oefenen kan ook met PhishLink, een recent ontwikkelde methode om iets aan het fenomeen phishing te doen. Medewerkers en afdelingen ICT worden getest met een vooropgezette phishing-aanval. Door de oefening wordt de herkenbaarheid beter, en zal de 'click-rate' omlaag gaan. Medewerkers krijgen een phishing e-mail toegestuurd. Zij klikken wel of niet op de link, en komen op een pagina waar kennis omtrent phishing staat, hoe het werkt, waarom het werkt, wat je eraan kunt doen. Zo wordt de medewerker van Onbewust Onbekwaam gevormd tot Bewust Onbekwaam. ■

Hans Labruyère is directeur bij LBVD.

Wie trapt daar nou in?

We horen het je denken, lezer: wie trapt daar nou in? Ikke niet! Wie is er nou zó dom om online een wachtwoord of pincode weg te geven? Genoeg mensen trappen er blijkbaar wel in: jaarlijks groeit het aantal aanvallen wereldwijd.

- Aantal phishingaanvallen wereldwijd in 2012-2013: ruim 37 miljoen
- Aantal aangevallen personen, wereldwijd, per dag: ruim 100.000
- Gemiddelde schade per phishingslachtoffer: EUR 416,00