

Volwassenen weer kleuter op het internet



PERSPUBLICATIE 17 februari 2007

www.digitaleopspring.nl

Volwassenen weer kleuter op het internet

Door Rob Cox



Hallo, ken je me nog? Elly.

Deze e-mail, met het onderwerp School, valt tegelijk bij negen mannelijke medewerkers in de elektronische brievenbus. Negen mannen met een goede functie bij een multinational waar wereldwijd tienduizenden mensen werken. Eén manager reageert niet, een tweede laat weten geen prijs te stellen op contact, maar zeven mannen sturen een mailtje terug. Bij elk mail zit een digitaal visitekaartje met de contactgegevens en functie van de manager. Op die eerste dag versturen de nieuwsgierige managers 46 emails naar Elly. Het mailverkeer krijgt nog een opleving als Elly een foto meestuurt. Elly ziet er namelijk lekker uit.

Maar Elly krijgt wroeging want ze mailt via haar bedrijfsaccount, dat zal haar baas nooit goed vinden. Bovendien moet ze maandag naar Amsterdam; dinsdag neemt ze weer contact op.

Een van de mannen is niet van het afwachtende soort: hij stelt een ontmoeting voor in Amsterdam. En hoewel Elly nooit meer iets van zich laat horen, komen tot op de dag van vandaag nog mailtjes binnen voor haar. 'Elly' is in werkelijkheid het Horster bedrijf Com-Connect van Paul de Vlieger, Wilfred van Roij en Jim Bosman, via cursussen het bedrijfsleven bewust wil maken van de gevaren van internet. Want die gevaren zijn véél groter dan wij, naïvelingen, in de gaten hebben. Een van de motto's van ComConnect is: als volwassenen op internet gaan, worden het weer kleuters. „Elk bedrijf steekt veel geld in virusscanners en firewalls, maar het grootste risico van internet is de mens zelf”, zegt De Vlieger. En deze test was daarvan een voorbeeld. „Het bedrijf wilde dat we onderzochten hoe kwetsbaar de onderneming is. Die zeven mannen hadden allemaal goede functies. Door te reageren op de mail van Elly waren ze kwetsbaar voor chantage. En dit gebeurt regelmatig hoor. In Oost-Europa zijn hele bendes met deze vorm van afpersing bezig. Die bendes willen geld of bedrijfsgeheimen. Dat je er weinig van hoort, komt doordat de bedrijven die door deze chantage worden getroffen, dat echt niet aan de grote klok hangen.”

De namen van de zeven medewerkers van het bewuste bedrijf zijn niet doorgegeven aan de directie. „Maar ze worden via een stuk in het personeelsblad op de hoogte gesteld van de ware identiteit van Elly”, zegt De Vlieger. „Ik zou er wat voor over hebben om de gezichten van die mannen te zien.”

INTERNETFRAUDE dupeert het bedrijfsleven jaarlijks voor tientallen miljarden schat het Amerikaanse anti-virusbedrijf McAfee. Het gebeurt op verschillende manieren. Grofweg delen de mannen van Com-Connect de fraudes in vier categorieën in: social engineering, identiteitsdiefstal, gegevensdiefstal en al redelijk bekende phishing.

Com-Connect kreeg de opdracht van een bedrijf na te gaan hoe kwetsbaar de directeur was voor internetcriminaliteit. De directeur kon echter nauwelijks met internet overweg en had dus ook geen sporen achtergelaten. Maar de voetbalclub waarvan de directeur voorzitter was, had een eigen website. Daarop stond het privé-adres van de directeur. Door via dat adres te zoeken op het internet, bleek dat de twee dochters van de directeur vrijwel dagelijks op internet te vinden waren. Uit de internetssporen was veel af te leiden over hun privéleven dat bij eventuele gijzelingsplannen van pas kon komen.

SOCIAL engineering is het ingrijpendst. Het is een gevalletje 'Elly' in het kwadraat. Via internet wordt zo diep mogelijk in uw privacy gegraven, met als doel u kwetsbaar te maken en te chanteren. „Het is ongelofelijk wat mensen allemaal blootgeven op internet“, zegt Wilfred van Roij, parttime werkzaam bij de recherche van de politie en zakenpartner van De Vlieger. Van Roij is bij binnenkomst van de verslaggever al op de hoogte van zijn opleidingsgegevens, de namen van zijn kinderen en hun leeftijd. Resultaat van een korte zoektocht op het internet waar ik die gegevens ooit eens heb achtergelaten. De belangrijkste bronnen voor social engineering zijn de internetgemeenschappen. Dat zijn digitale vriendenkringen waarbij elke deelnemer een profiel van zich zelf opstelt. „Mensen vullen daar hun naam in, hun huwelijks staat, hobby's, vrienden, baan. Dit is ongelofelijk populair bij jonge managers die op deze manier hun netwerk willen uitbreiden. Maar het is een gouden site voor internetcriminelen. Die weten na het lezen van die website genoeg om je te benaderen. Het praat altijd gemakkelijker als je doet of je iemand anders kent of zijn hobby's weet. Het gaat om websites als Hyves, MySpace, CU2 en Sugababes. Maar ook datingsites, Schoolbank.nl en Dienstmakkers.nl geven vaak voldoende informatie om kwaadwillenden de kans te geven u persoonlijk aan te spreken. Als je zoiets wilt doen via het internet, gebruik dan nooit je echte naam“, verzucht Van Roij.

Een andere schat aan informatie zijn de zoekmachines op internet. Google is daarvan veruit de belangrijkste. Bijna iedereen heeft op het internet wel een keer zijn eigen naam ingetikt om te zien wat er over hemzelf bekend is op het web. Wie echter goed om kan gaan met de zoekmachines kan schatten aan informatie boven water halen. Uw ranking bij de tennisclub of uw adresgegevens zijn vaak een makkie. „Sommige mensen zetten alle gegevens op een eigen website, inclusief foto's van zichzelf en de familie“, zegt Van Roij. „Zo was er een van de deelnemers aan onze bijeenkomsten die we vooraf hadden gegoogled. We vonden een foto van hem met Frans Bauer op het net. Die hebben we hem die dag laten zien met de vraag: „Hang je die foto ook op het prikbord bij de Albert Heijn? Nee dus.“

De enige oplossing om je minder kwetsbaar te maken, is je zelf 'ontgooglen'. Daarvoor moet je alle beheerders van een website benaderen die je privégegevens publiceert en vragen of ze je kunnen schrappen. Maar zelfs dán is er voor de criminelen nog een mogelijkheid: de Wayback Machine. In Amerika zit een bedrijf dat om de paar dagen een kopie maakt van alle nieuwe pagina's die op internet zijn verschenen. Bijna alle internetpagina's van de voorbije tien jaar zijn daar te vinden. „Mensen moeten één ding beseffen“, zegt Paul de Vlieger: „Een gummetje bestaat niet op internet.“

De Vlieger: „We hebben gezien op internet dat jij geschreven hebt over de Hells Angels. Iemand kan ervoor zorgen dat je binnen twee weken mannen met leren jasjes op je stoep staan. Uit mijn onderzoek is gebleken dat het domein www.limburgs-dagblad.nl niet geclaimd is. Die claimt hij dan. Vervolgens stuur hij naar alle Hells Angels emails met als afzender jouw naam. In die mails zegt hij dat alle motorclubleden homo's en criminelen zijn. Reken maar dat je bezoek krijgt als hij genoeg van die mails verstuurt.“

Bij identiteitsdiefstal zoekt de crimineel voldoende gegevens bij elkaar om te doen alsof hij u is. Met uw gegevens vraagt hij vervolgens creditcards of doet online-bestellingen. Een sofinummer, een adres en uw geboortedatum zijn al voldoende. Maar het kan ook anders. Je kunt je concurrent gemakkelijk via internet kapotmaken. Door in naam van dat bedrijf allerlei mails te verspreiden, krijgt de concurrent een slechte naam. „En geloof me, het gebeurt”, zegt Van Roij.

Identiteitsdiefstal komt steeds vaker voor. Het slachtoffer is er vaak niet van op de hoogte of hoort het pas als het te laat is. Soms worden foto's van internet gehaald en door digitale montage wordt een erotische foto gemaakt van u. Leg dat maar eens uit aan je partner.

Overigens kun je je eigen identiteit ook beïnvloeden. Heel veel jonge werknemers pimpen hun cv. Van Roij: „Het hoofd personeelszaken zei eens heel trots dat hij alle jobkandidaten googlet. Daarop vroeg ik hem hoe hij zeker wist dat die gegevens op het net ook echt kloppen. Niemand gaat na of die kandidaat wel al die scholen heeft doorlopen of op al die plekken heeft gewerkt. Wij geven trainingen hoe je dit soort zaken kunt uitzoeken.”

Com-Connect legde op een parkeerplaats van een bedrijf zeven usb-sticks neer. Dat zijn apparaatjes ter grootte van een aansteker waarop digitale gegevens opgeslagen kunnen worden. De usb-sticks kunnen op vrijwel elke computer aangesloten worden. De zeven 'verloren' usb-sticks werden binnen het uur gevonden. Alle zeven werden ze nog diezelfde dag aangesloten op een computer van het bedrijf. Criminelen kunnen een programma op die stick zetten dat automatisch actief wordt als de stick wordt aangesloten op een computer. Dat programmaatje start dan automatisch met het versturen van vitale bedrijfsgegevens naar de internetbende.

PHISHING lijkt op het engelse woord Fishing (vissen). En dat is niet voor niets. Als u zich op internet begeeft, bent u een van de vissen waarnaar criminelen zitten te hengelen. Soms doen ze dat via een email zoals de criminelen die mails verstuurd die uiterlijk perfect leken op de Postbank. Ze vroegen daarin of de mensen hun pinpas en rekeninggegevens wilden invoeren ter controle. Vele tientallen mensen trapt erin en hun bankrekening werd geplunderd. De schade voor de Postbank is overigens veel groter. De betrouwbaarheid van deze bank heeft grote schade opgelopen. De Rabobank heeft sinds kort ook last van phishing.

Een andere manier is veel subtieler. Veel mensen kijken films of spelen spelletjes via internet waarvoor een programmaatje geladen moet worden. Maar heel soms zit daar geheime software in waarmee een aanval wordt gedaan op uw gegevens. Er zijn speciale programma's die precies bijhouden welke toetsen u intikt op het toetsenbord en dat doorsturen naar de criminelen. Handig om achter al uw wachtwoorden te komen. Dit soort programmaatjes kan ook op telefoons, usb-sticks, diskettes of andere gegevensdragers zitten.

Overigens zijn mannen het zwakke geslacht op internet. Vrouwen zijn veel zakelijker en dus beter, hebben ze geleerd bij Com-Connect. Mannen gebruiken internet om te gamen en te surfen. Vrouwen gebruiken internet omdat het nuttig is.

En dan gegevensdiefstal. Niet altijd is het de criminelen om geld te doen. De informatie op uw werkplek kan ook van groot belang zijn. Elke vorm van gegevensdragers kan daarbij worden gebruikt: diskettes, cd-rom, usb-sticks, complete computers. Daar kwam de medewerker van het ministerie van Defensie achter toen hij een usb-stick kwijtraakte met geheime informatie over Afghanistan. En officier van justitie Joost Tonino die zijn computer vol informatie over criminelen bij het oud vuil zette omdat hij dacht dat ie kapot was.

Maar steeds vaker worden medewerkers omgekocht om bedrijfsgeheimen naar buiten te smokkelen. Op één usb-stick kan de inhoud van honderd boeken staan. En dan is er nog de ontevreden werknemer die een digitaal kopietje maakt om te gebruiken bij zijn ontslag.

Hans gaat op vakantie en zet zijn email-adres op afwezig. Het programmaatje dat je afwezigheid meldt, zit op elke windowscomputer en heet de Out of office-assistant. Service voor je vaste klanten. Maar ook heel attent voor criminelen. „Je kunt net zo goed op vakantie gaan en de deuren van de zaak wagenwijd openzetten met een bordje erbij 'kom maar halen'', zegt Wilfred van Roij. En met een beetje googlen (Detelefoongids.nl) komen ze ook nog even op Hans' privé-adres langs.

BEWUSTWORDING is het enige dat helpt, zeggen de mannen van Com-Connect. „En dat is wat we de mensen willen leren in onze cursussen“, zegt Paul: „Wees alert wat je doet op internet en met je computer.“ Van Roij: „Geef me je pc en ik laat je je andere ik zien.“ Is het allemaal wel zo erg als de mannen van Com-Connect zeggen? Is dit niet bangmakerij, een groot promotiepraatje om hun product aan de man te brengen? „Je moet maar eens kijken op www.internetoplichting.nl“, zegt Wilfred van Roij. „Daar kom je de drama's tegen van mensen die zijn opgelicht via het web.“

Meer weten:

www.digitaleopsporing.nl

www.internetawareness.nl

Projectleider:

Wilfred van Roij

Tel: 077-8500295

Mob: 06-21570813

info@digitaleopsporing.nl

