ONTHULLEND: MET INVESTERING VAN €5000 KAN IEDEREEN AAN DE SLAG ALS GEVAARLIJKE CYBERCRIMINEEL

HACKERS KOMEN MOEITELOOS binnen bij KPN, honderdduizenden klanten van bierbrouwer Bavaria en elektronicareus Philips vonden deze maand hun gegevens na een kraak op internet terug. Probleemloos dringen hackers in de besturing van Zeeuwse gemalen. „Nederlandse bedrijven en consumenten zijn totaal niet voorbereid op computerkrakers en Russische cyberterroristen", zegt hoogleraar Chris Verhoef. Want wat blijkt: voor nog geen 5000 euro koop je op internet een professionele, kogelvrije 'hackwinkel'...

HACKEN KINDERSPEL

Waarom is pc niet standaard beschermd, op nieuwe auto zit toch ook een rem?

door **THEO BESTEMAN** en **ALFRED MONTERIE**

AMSTERDAM, zaterdag

Internet is nog steeds zo lek als een mandje. Cybercriminelen konden vorig jaar doordringen tot creditcardgegevens van 2,2 miljoen Sony PlayStation-spelers en daarmee shoppen. Grote bedrijven leerden daar weinig van. Als de beveiliging zo te wensen overlaat zoals deze maand bij nationale trots KPN, zegt hoogleraar informatica Chris Verhoef (Vrije Universiteit), kun je met een beetje geluk zo in de systemen van grote bedrijven binnen.

„Dat zijn heus niet allemaal professionele krakers. KPN heeft het laten versloffen", ziet Verhoef aan de coderijtjes op zijn pc. „Winst en topsalarissen zijn kennelijk belangrijker dan hun klanten."

Omdat het telecombedrijf verzuimd had een weinig gebruikte netwerkcomputer te onderhouden en als het ware een 'achterdeur' had openstaan, kreeg een hacker toegang. Die had aanvankelijk zelfs niet door dat hij bij het telecombedrijf op bezoek was. Aangezien KPN ook binnenshuis diverse 'tussendeuren' slecht had afgesloten, kon de hacker verbazend ver in het interne netwerk doordringen.

Pas toen merkte de hacker waar hij was beland. De inbraak bij KPN begon als een toevalstreffer. Wie bij duizenden computers aan de deur gaat morrelen, zal zich dus altijd wel ergens entree verschaffen.

'Hobby-inbrekers'

De hacker van KPN behoort tot het gilde van 'hobby-inbrekers', die op internet zoeken naar openstaande deuren, zeggen beveiligingsexperts. Het geeft hun een kick als ze binnen weten te dringen. Sommigen waarschuwen eerst het bedrijf dat de beveiliging mankeert. Anderen zien zich als een moderne Robin Hood en tonen hun buit uitvoerig op internet. Dat kunnen bijvoorbeeld klantengegevens zijn of lijsten met wachtwoorden.

Veel gevaarlijker dan deze hobbyhackers zijn de echte cybercriminelen, die eropuit zijn zo veel mogelijk te stelen. „Hersenen heb je er niet voor nodig", zegt ook Dmitry Bestuzhev, hoofd onderzoek van het antivirusbedrijf Kaspersky. De Rus legt uit dat een criminele carrière in de internetwereld zo is gestart. We zoeken hem in winters Moskou op om meer te weten te komen over de methoden die computermisdadigers gebruiken.

Al snel blijkt uit Bestuzhevs relaas dat zelfs de grootste sukkel kan hacken. Je hoeft helemaal geen genie te zijn of nachtenlang achter de computer te zitten om succesvol bij computers op internet te kunnen inbreken. Een beetje geld is voldoende. „Dan kan je zo aan de slag."

Russische bendes achter webwinkels

Het meeste werk valt namelijk goed uit te besteden. Bestuzhev rekent voor dat je voor welgeteld 6130 dollar het mannetje bent. Met die investering is een vliegende start in de computercriminaliteit te maken. Het begint met een goede 'bouwdoos' om kwaadaardige software, *malware*, te maken. Voor 750 dollar heb je een verfijnd pakket als *Spy Eye* of *Zeus*, waarmee de beste malware valt te maken.

Ideaal is software die zich als een Trojaans paard in een computer nestelt om daar wachtwoorden of andere belangrijke gegevens te stelen. Om herkenning door antiviruspakketten te voorkomen moet je een variant op bestaande malware zien te maken. Dat is een kwestie van knutselen. Een verstandige inbreker laat het resultaat van zijn knutselwerk niet zomaar los op de computers die hij wil aanvallen. Deze malware moet eerst een heuse kwaliteitscontrole ondergaan.

Daarbij wordt gekeken hoe snel de kwaadaardige software wordt herkend door de vele tientallen antiviruspakketten die momenteel in omloop zijn. Een aantal weinig scrupuleuze websites doet dit karwei voor ongeveer 1 dollar per scan. De Russische 'dienstverlener' Virtest-.com biedt voor 480 dollar een jaarabonnement aan waarmee je onbeperkt bestanden kunt laten checken.

Vervolgens is nog een speciaal pakket zoals BlackHole of BleedingLife nodig, dat criminelen helpt computers effectiever te besmetten. Gemiddeld ben je hiervoor 1300 dollar kwijt.

Maar daarmee ben je er nog niet als startende crimineel. Je moet ook een computer hebben die goed van de buitenwereld is afgeschermd en niet door de politie kan worden ontdekt. Uiteraard is overal computercapaciteit te krijgen, maar de meeste verhuurders houden criminelen buiten de deur. „Om een computer 'kogelvrij' te huisvesten ben je al snel 3600 dollar per jaar kwijt. Dit is veruit de grootste 'kostenpost' voor de crimineel", weet de onderzoeker.

Voor criminelen die geen zin of tijd hebben om malware te installeren op de computers die ze willen aanvallen, zijn er organisaties die dat werk uit handen nemen. Bestuzhev toont een tarieflijst van zo'n 'dienstverlener'. GoldInstall bijvoorbeeld rekent 150 dollar voor duizend computers in de VS.

Nederland behoort tot de goedkopere landen. Per duizend te besmetten pc's betaal je 20 dollar. Ook is het mogelijk netwerken van besmette computers te verhuren. Die pc's van nietsvermoedende consumenten dienen alleen om virussen en andere malware te verspreiden. Voor gemiddeld 27.000 dollar heb je zo'n netwerk, ook wel *botnet* geheten, een jaar tot je beschikking.

Criminelen kunnen met ontvreemde persoonsgegevens zelf bankrekeningen leeghalen of hun gestolen waren op de zwarte markt verkopen. De prijzen van Amerikaanse creditcards variëren van 23 dollar (klassiek of standaard) tot 40 dollar (goud) en 45 dollar (wereld). Een Nederlandse creditcard kost 15 dollar. Vooral MasterCard is populair bij het inbrekersgilde. Ook accountgegevens van Facebook en PayPal worden massaal verhandeld.

• *Dmitry Bestuzhe ...beetje geld...*

• *Chris Verhoef ...illusie...*

Hoogleraar informatica Chris Verhoef: 'Internetbankieren? Ik niet!'

Misdaad

Traditionele misdaad en cybercrime gaan hand in hand. Veel mensen scannen hun paspoort en bewaren het bestand in een pc. Zo kunnen criminelen makkelijk zo'n document namaken. Een Nederlands paspoort kost op internet €600. Voor €100 extra krijg je er een rijbewijs bij. ,,Alles heeft zijn prijs'', zo concludeert de onderzoeker van Kaspersky.

„Maar maak het consumenten makkelijk zich tegen die criminelen te beveiligen", zegt Verhoef. „Als je een pc of tablet koopt, moet daar standaard beveiliging op zitten. Waarom leveren bedrijven dat niet? Zoals in een auto standaard een rem zit als ze uit de fabriek komen. Dat vindt niemand vreemd. Maar bij een nieuwe pc is virusbescherming een optie, alsof de rem op een auto er als een accessoire bij zit. Nee dus."

Het gevaar op internet wordt alsmaar groter, consumenten doen er steeds meer op. Bedrijven maken hun gegevens vaker mobiel bruikbaar, voor smartphones en tabletcomputers, in wat de *cloud* heet; een 'wolk' met het mobiele internetnetwerk, dat datacenters wereldwijd in de lucht houden. Cloud-diensten op smartphones zijn vaak zonder wachtwoord te gebruiken. De helft van alle Nederlanders heeft zo'n telefoon.

'Kema-keurmerk'

,,Niet de oudjes die achter een pc kruipen, blijken kwetsbaar'', zegt hoogleraar Verhoef, ,,juist jongeren. Die zitten op sites als het onlangs gekraakte Baby-Dump.nl, zij laten digitaal overal hun sporen na en worden gevolgd door bedrijven én criminelen.'' Een 'Kema-keurmerk' voor veilige sites zou goed zijn, zegt hij.

Bedrijven zullen klantgegevens veel beter moeten beveiligen, vindt de Tweede Kamer. Staatssecretaris Teeven (Justitie) stelt boetes tot twee ton voor als bedrijven de data niet goed beschermen en inbraken niet melden. In de VS zijn bestuurders daarvoor al de gevangenis ingegaan. Eurocommissaris Vivian Redding wil bedrijven voor lakse beveiliging van klantgegevens tot een miljoen euro of twee procent van hun hele omzet beboeten.

„Maar het is een illusie te denken dat we het internet onder controle krijgen. Dat hebben we nog nooit gehad, omdat iedereen toegang houdt", zegt Verhoef.

,,Er is geen controlerende instantie, geen internetpolitie. Als consument moet je dus tot de tanden toe bewapend dat internet op. Banken eisen van consumenten bij internetbankieren dat zij zich superzwaar beveiligen, antivirussoftware volgens de laatste versies vernieuwen. Doe je dat niet, dan krijg je bij een inbraak niets vergoed. Terwijl banken, professionals hoor, vaak zelf niet aan die veiligheidseisen voldoen. En daarmee wel wettelijke eisen overtreden'', aldus Verhoef. ,,Een van de redenen waarom ik niet aan internetbankieren doe en elke week gewoon enveloppen met acceptgiro's dicht lik...''

Wat is goed wachtwoord?

Volgens Robert Webbe, technisch specialist van BelCompany, is het hoog tijd dat de consument aan zijn digitale veiligheid gaat denken. Hij geeft de tip drie typen wachtwoorden te hanteren, al naargelang de mate van veiligheid die is vereist. Zijn advies is voor alle websites waar persoonlijke identiteit van het allergrootste belang is, een uniek en moeilijk wachtwoord te maken. DigiD, dat onder meer bij de belastingaangifte wordt gebruikt, behoort tot deze categorie. Vaak heb je deze inloggegevens maar enkele keren per jaar nodig.

Hier zijn wachtwoorden die worden gevormd door bestaande woorden uit den boze. Typ willekeurig 20 tekens in en gebruik hoofdletters, kleine letters, cijfers en een paar leestekens. Schrijf dit wachtwoord op een apart lijstje en bewaar dit op een geheime plek. Vertel alleen je partner erover.

Dan zijn er websites waar persoonlijke informatie zoals e-mail wordt uitgewisseld. De eisen die daarbij aan de veiligheid worden gesteld zijn hoog, maar minder dan bij de eerste categorie. Webbe raadt aan hier een standaard wachtwoord te gebruiken aangevuld met een uniek gedeelte. „Gebruik wederom geen woorden, maar bedenk een zin die makkelijk is te onthouden. Gebruik telkens alleen de eerste letters. Voorbeeld: *Ik heb 1 grijze Toyota Yaris en die is erg mooi!* Dit levert wachtwoord *Ih1gTYediem!* op. Achter dit standaard wachtwoord zet je de toepassing of websitenaam, maar dan zonder www ervoor en nl erachter. Voor Hotmail zou dit tot *Ih1gTYediem!hotmail* leiden."

Moeilijk te onthouden? Webbe: „Welnee, eigenlijk staat er een makkelijk te onthouden zinnetje en de naam waar je het wachtwoord voor gebruikt."

Ten slotte zijn er nog sites waar men moet inloggen zonder dat hackers hier directe schade kunnen aanrichten. Voorbeeld is een internetforum. Webbe: „Daar kun je dan een internetalias zoals 'Henk1943' gebruiken in plaats van je echte naam. Waak over je privacy. Vul alleen de vereiste informatie in. Is bepaalde informatie zoals een telefoonnummer verplicht, vul dan gewoon onjuiste gegevens in zoals 0612345678. Voor dit soort toepassingen kan je prima een gemakkelijk wachtwoord gebruiken, wellicht dat wat je nu al gebruikt."

• *Robert Webbe, BelCompany ...veiligheid...*

• *Veel gevaarlijker dan hobbyhackers zijn de echte cybercriminelen, die eropuit zijn zo veel mogelijk te stelen. „Hersenen heb je er niet voor nodig..."*

FOTO: GETTY IMAGES

Huisje-boompje-beestje

Op de schooltelevisie is met regelmaat een 'vak' te zien dat luistert naar de naam 'Huisje-boompje-beestje'.

Het gaat over natuur en techniek en het moet (volgens de site) de kinderen vertrouwd maken met de spannende dingen in hun omgeving. Ik hoop voor hen dat het vak spannender is dan de naam doet vermoeden.

De betekenis van de uitdrukking huisje-boompje-beestje is immers 'heel gewoon' (volgens Van Dale), maar ook 'buitengewoon saai' (volgens mezelf). Een huisje-boompje-beestjegezin is dus te associëren met 'niks bijzonders, burgerlijk zelfs'.

De uitdrukking kwam in de jaren vijftig van de vorige eeuw algemeen in gebruik. Aanvankelijk werd gedacht dat vooral NS-machinisten daarvoor verantwoordelijk waren. Zij spraken van huisje-boompje-beestje als ze op steeds hetzelfde eentonige traject werden ingezet. Later werd dat het beruchte 'rondje om de kerk'.

Toch is de uitdrukking niet afkomstig uit de treinwereld. Logischer lijkt dat ze uit de luchtvaart komt. Vlieger/schrijver A. Viruly schreef een boek waarin hij wél het 'huisje-boompje-beestjetijdperk' vermeldt, maar geen verdere uitleg geeft. Mogelijk verwijst hij naar de tijd dat de piloten nog op zicht moesten vliegen, maar ik vermoed iets anders.

De uitdrukking 'huisje-boompje-beestje' werd vlak vóór en vlak ná 10 mei 1940 vaak op schrift gesteld, niet door burgervliegers, maar door oorlogsvliegers, en wel in hun dagboeken. Dáár moeten we de oorsprong zoeken, temeer omdat de vliegmethode bij de luchtmacht ook een veelgebruikte afkorting kende: Hu-Bo-Be.

Zo beschrijft luchtmachtpiloot S.J. Postma hoe hij in zijn Fokker C.X ging deelnemen aan de strijd om de Grebbeberg (vlucht van 13.05.40 te 03.25 uur): „Direct na het loskomen, houden we het toestel gedrukt. We vliegen tussen de boerderijen door: Hu-Bo-Be." Zijn boekje verscheen direct na de oorlog al (1945).

Op een Nederlandse website over de eerste dagen van de Tweede Wereldoorlog komt ook de zinsnede voor: „De tweede Fokker T-V ontkwam op boomtophoogte (de zgn. Hu-Bo-Be) en keerde veilig terug op Schiphol." Auteur is Hans Geel.

Zelfs in de Engelstalige Wikipedia komt de uitdrukking voor. Dat zegt niet alles, omdat die teksten deze eeuw werden geschreven. Toch is het opvallend dat bij een artikel over de Fokker C.X (een Nederlandse verkenner annex lichte bommenwerper) wordt verteld dat de Nederlandse Fokkers in de begindagen van de oorlog de veel snellere Messerschmidts vaak te vlug af waren, door hun Hu-Bo-Be-tactiek.

Uit alles blijkt wat er met 'huisje-boompje-beestje' werd bedoeld. Het had volstrekt niets te maken met de sfeer in een burgerlijk huisgezin, niet met treinen en ook niet met Viruly. Bij de luchtmacht werd er in 1940 mee bedoeld dat er laag werd gevlogen door wendbare kisten. Zó laag dat het vliegtuig min of meer voor elk huis, voor elke boom en voor elk beest-in-de-wei moest optrekken om eroverheen te 'springen'. De reden is duidelijk: buiten het zicht van de vijand blijven.

Intussen is die krijgszuchtige aanduiding uit de eerste oorlogsdagen van 1940 verbleekt tot een graad van burgerlijkheid...

Klare Taal

klaretaal@telegraaf.nl