

Je geld online

VEILIG EN OOK WEER NIET

Klantgegevens gejat uit het PlayStation Network en Rabobank-internetbankieren plat wegens aanval van hackers... De afgelopen weken is onlineveiligheid een nog hotter item geworden dan het al was. Maar hoe groot is het probleem nou écht?

In één klap de gegevens van 100 miljoen online gamers binnen harken. Dan sla je effe een slag als hacker! Eind april lukte het onbekende hackers om in te breken in het PlayStation Network: het online netwerk van Sony's gelijknamige spelcomputer. In een tijds-panne van twee dagen wisten hackers hele databases met gebruikersgegevens leeg te trekken, inclusief creditcard-gegevens. Sony legde het online netwerk direct na ontdekking van de kraakactie plat om zo verdere schade te voorkomen. Het technologiebedrijf reserveert inmiddels 1 miljoen dollar per hack-slachtoffer, om de kosten van mogelijk misbruik van de creditcardgegevens op te vangen. Klanten die uit angst hun creditcard hebben afgesloten en een nieuwe hebben moeten aanschaffen, krijgen misschien (Sony twijfelt nog) een schadevergoeding. Klinkt netjes, maar het is toch vooral symboolpolitiek. Want zelfs al zou Sony niet voor de schade opdraaien, dan zijn het altijd nog de banken of creditcard-maatschappijen die de schade vaak ondervangen, weet ook Arjan Dasselaar, auteur van het *Handboek digitale criminaliteit*. 'In het geval van fraude met creditcards ligt de bewijslast niet bij

ONLY SONY

Sony's PlayStation ligt al heel wat langer onder vuur. De gameconsole werd in januari gekraakt door hacker GeoHot, waardoor het mogelijk werd om ook andere software op de gameconsole te gebruiken. Sony reageerde met gerechtelijke acties. Dat schoot een groep andere hackers in het verkeerde keelgat. De groep 'hacktivisten' die werkt onder de naam Anonymous legde het netwerk tijdelijk plat. De hack waarbij gebruikersgegevens gestolen zijn, is weer een andere. Hackgroep Anonymous zegt daar niets mee te maken te hebben. Vooralsnog denkt Sony daar anders over.

de consument. Als je dus gewoon netjes je afschriften in de gaten houdt en aan de bel trekt zodra je iets gekst ziet, is er niets aan de hand.'

En dat is ook precies hoe creditcardmaatschappijen erover lijken te denken. Dasselaar: 'Zij streven niet naar een situatie zonder fraude. Dat is gewoon veel te duur. Het is een kosten-batenanalyse. Daarbij kijken de maatschappijen wat het beste uitpakt voor ze. Dat doe je zelf ook. Denk maar aan je huis. Als ik naar binnen wil, kom ik wel binnen. Als je een kleerkast inhuurt en die voor de deur zet, wordt dat al veel moeilijker. Maar dat kost je dan misschien een paar honderd euro per dag. Zo is het voor bedrijven dus ook

'CREDITCARD-MAAT-SCHAPPIJEN STREVEN NIET NAAR EEN SITUATIE ZONDER FRAUDE. DAT IS GEWOON VEEL TE DUUR'

goedkoper om schade na een kraak te vergoeden, dan om een systeem helemaal waterdicht te maken.'

En dat geldt ook voor banken. Ook zij timmeren hun systeem niet helemaal dicht. En ook daar gaat het weleens mis! Zoals vorige week bij de Rabobank. Het internetbankieren daar werd lamgelegd met een zogenaamde DDoS-aanval. Bij zo'n aanval laat een hacker een hele hoop computers allemaal tegelijkertijd een website bezoeken. De server waarop de site draait, raakt daardoor overbelast waardoor de site van het net verdwijnt. En hoewel webwinkels door de lamlegging naar schatting 8 miljoen euro aan transacties zijn misgelopen, zijn er in ieder geval geen klantgegevens op



straat komen te liggen. Geen schade voor de consument dus.

Toch zit het ook bij banken niet goed, volgens Chris Verhoef, IT-hoogleraar aan de Vrije Universiteit in Amsterdam. Verhoef stipt wat andere miskleunen van vooral de Rabobank aan. Zo ging het begin april mis bij de bank, toen een deel van de internetbankierders per ongeluk de rekeninggegevens van andere klanten konden inzien. En in december vorig jaar zat er ook al een lek in het mobiel bankieren van deze bank. Dat gat werd gevonden door een 24-jarige student en werd vervolgens getest door tech-blog Webwereld.

Volgens Verhoef zijn de voorbeelden genoeg reden om voorzichtig om te

aanrichten. Van geldoverschrijving tot complete identiteitsdiefstal. En je kunt wel zeggen dat je niets te verbergen hebt, maar ook bij je huis doe je je voordeur op slot, omdat je niet wilt dat er iemand binnenkomt. Dat is bij je computer niet anders.'

BLIND VERTROUWEN?

Zodra je je gegevens zoals je creditcard-nummer op een website invoert, ben je overgeleverd aan een ander. Je hebt daarna geen zicht op je gegevens. 'De consument kan absoluut niets doen om zichzelf te beschermen. Je bent gedwongen die partijen te vertrouwen. En je kunt niet voorkomen dat ze het verkloten,' aldus de Amerikaanse beveiligingsgoeroe Bruce Schneier in een interview met game-blog Kotaku.

Maar hoe gevaarlijk het delen van je persoonlijke informatie ook kan zijn, de kans dat het fout gaat en dat je gegevens misbruikt worden, is volgens Bruce Schneier niet heel groot. 'Het gaat zo nu en dan fout, maar over het algemeen zijn we vooralsnog relatief veilig. En laten we eerlijk zijn: we moeten wel gebruik maken van het net. Welke andere opties zijn er?' Volgens Schneier is de paniek die ontstaat bij grote hacks als die van Sony aardig overtrokken. Wie er belang bij die paniek hebben? De beveiligings-bedrijven uiteraard. Het zijn de bedrijven die de gegevens van andere bedrijven beveiligen. Zij kunnen aardig cashen op de onzekerheid van bedrijven en consumenten.

Ook volgens Arjan Dasselaar is dat wel een probleem, maar kun je er bij grote instituties als iTunes, TicketBox en PayPal van uitgaan dat je gegevens redelijk veilig zijn. Al zijn er ook aardig wat uitzonderingen van mensen wier gegevens gestolen zijn en die daar veel last van ondervonden. 'In feite komen grote hacks als die bij Sony niet vaak voor. Zelf ben ik in zestien jaar tijd slechts één keer slachtoffer geworden. En toen heb ik netjes mijn geld teruggekregen van de creditcardmaatschappij. Het is redelijk veilig op internet, als je je gezond verstand gebruikt.' **VB**

BANK MET PROBLEMEN

Bij de Rabobank gaat het al lang niet lekker. De bank werd aangevallen door Conspiracy Cells of Fire (CCoF). Deze mysterieuze groep claimde drie keer een brand in het hoofdkantoor van de Rabobank in Utrecht. De AIVD doet die claim overigens af als 'nep'. CCoF zegt ook verantwoordelijk te zijn voor meerdere hack-aanvallen. De reden: volgens de groep investeert de bank in de wapenindustrie. De Rabobank ontkent dat.

springen met je eigen data. 'Zolang iedereen maar alles op het web kan zetten en jij daar je gegevens achterlaat, kun je er niet van opaan dat je gegevens veilig zijn. Met die betaalgegevens kunnen criminelen een hoop schade