

Uitgebreide trukendoos van de internetfraudeurs

Alles gecheckt? Uw computer en internetverbinding zijn veilig? Toch is het mogelijk dat u op slinkse wijze ten prooi valt aan fraudeurs.

Veiligheid Hoewel het goed is om 'drie keer te kloppen' kunt u nog meer doen om veiliger te surfen

Vincent Andriessen

Lekker op de bank, laptop op schoot. Even geld overmaken aan de webwinkel waar ik laatst een boek heb besteld. Iets minder dan vijftig euro. Ik surf naar de website van mijn bank en klik op de button waarmee ik kan inloggen in het beveiligde betaalsysteem.

Drie keer kloppen, schiet me plotse-ling te binnen. Hoe zat het ook alweer met die campagne? Allereerst: klopt mijn pc-beveiliging? Ik heb een virus-scanner die up-to-date is en de laatste tijd niets vreemds op mijn pc heeft kunnen ontdekken. De computer geeft bovendien aan dat ik ingelogd ben op mijn eigen draadloze netwerk.

Dan de website: klopt die ook? Ik kijkt naar de adresbalk. Daar staat de website van mijn bank en een klein slotje. Veilig dus. Dan, ten slotte: klopt de betaling? Ik controleert nogmaals de naam van de webwinkel, het reke-

ningnummer en het bedrag dat ik wil gaan overmaken. Allemaal in orde. Met een gerust hart druk ik op de verzendknop en sla even later de laptop weer dicht.

Een paar dagen later kan ik plotse-ling niet meer pinnen. Vreemd, er stond toch genoeg geld op mijn rekening? 's Avonds log ik nogmaals in bij de website van mijn bank. Daar kom ik er tot mijn schrik achter dat er in plaats van een klein bedrag naar de webwin- kel het tienvoudige is overgemaakt naar een onbekend bedrijfje op een Ca- ribisch eiland. Er is iets gruwelijk mis- gegaan. Hoe heeft dit kunnen gebeu- ren?

Om de zwakke schakel te vinden, is het allereerst van belang om te begrij- pen hoe ik eigenlijk vanaf mijn compu- ter thuis via internet op de website van mijn bank terechtkom als ik de do- meinnaam www.mijnbank.nl heb in- getoetst.

Het internet kan niet overweg met

de domeinnamen die wij gebruiken om naar websites te verwijzen, maar leest slechts adressen met cijfers die eruitzien als: 212.114.128.14. Die cijferreeks wordt een IP-adres genoemd. Als ik een domeinnaam heb ingetypt, wordt de naam vertaald naar zo'n IP-adres en word ik via internet de juiste kant op gestuurd. Dit wordt routing genoemd.

Bij dat 'vertalen' kan een heleboel misgaan. Een kwaadwillende kan op verschillende manieren de domeinnaam koppelen aan het verkeerde IP-adres. Daardoor kan het lijken alsof ik terecht kom op de juiste website achter de domeinnaam www.mijnbank.nl, terwijl ik eigenlijk doorgestuurd word naar een heel andere plek. Daar kan een kwaadwillende een kopie van de pagina www.mijnbank.nl hebben geplaatst die er veilig uitziet omdat hij hetzelfde slotje in de adresbank toont als ik gewend ben bij de echte website. Dat slotje toont de aanwezigheid van een zogenaamd SSL-certificaat aan (zie kader) maar het blijkt betrekkelijk eenvoudig om valse SSL-certificaten aan te vragen.

Op de kopie van www.mijnbank.nl kunnen verschillende trucjes uitgehaald worden met de gegevens die ik invoer. Zo is het mogelijk dat ik onbekommerd een bedrag denk over te maken aan het bedrijf waar ik mijn boek heb besteld, terwijl de malafide website er automatisch voor zorgt dat het bedrag en het rekeningnummer worden aangepast. Zo vliegt mijn geld niet naar de webwinkel maar het veelvoudige ervan naar een plek waar het moeilijk weer terug te krijgen is.

Er zijn vier zwakke plekken aan te

wijzen die deze vorm van fraude mogelijk maken. De kans dat deze technieken ingezet worden is reëel, maar cijfers over de omvang van het misbruik zijn er niet.

Allereerst mijn ADSL-modem, het apparaat dat internet bij me thuis brengt. Het modem is beveiligd met een inlognaam en een wachtwoord en wordt meestal geleverd met standaard inloggegevens, zoals bijvoorbeeld 'admin' of de naam van de fabrikant van het modem. Om het apparaat aan te sluiten is het niet nodig deze gegevens te wijzigen. Veel consumenten zijn na het installeren allang blij dat het apparaat werkt en laten de inloggegevens voor wat ze zijn. Dat biedt echter voor buitenstaanders de mogelijkheid om via het internet tot het modem door te dringen. Ze proberen gewoon een aantal keer toegang te verkrijgen door verschillende standaard inloggegevens op het modem uit te proberen.

Wanneer eenmaal toegang tot het modem is verkregen, is het mogelijk om de routing aan te passen. Wanneer ik daarna naar www.mijnbank.nl surf, word ik automatisch naar een ander IP-adres gestuurd zonder dat ik daar erg in heb.

Ook kan het gevaar schuilen in een op het eerste gezicht onschuldig berichtje. Zo nu en dan ontvang ik een e-mail van een onbekende met een bestandje en het bericht: klik op dit filmpje. Beter van niet. Grote kans dat ik op deze manier ongemerkt een 'trojan horse' op mijn computer installeer. Zo'n bestandje kan verschillende dingen op de computer wijzigen of vernietigen. Maar het kan ook de routing op mijn computer aanpassen zodat ik via

www.mijnbank.nl op de verkeerde plek terecht komt.

Een andere zwakke plek is mijn internetaanbieder. De routing vindt namelijk zowel plaats op mijn computer als bij mijn internetaanbieder. Wanneer er bij dat bedrijf iemand met kwade bedoelingen zit, kan hij er ook voor zorgen dat mijn internetverkeer wordt omgeleid. Bovendien kan ook een internetaanbieder het slachtoffer worden van een inbreker die van buitenaf de instellingen kan veranderen.

Ten slotte ontdekte Dan Kaminsky, een Amerikaanse beveiligingsexpert, een jaar geleden dat er een wereldwijde fout zat in de programma's (de 'domain name servers', die op de computers van mijn internetaanbieder zijn te vinden) die de domeinnamen (zoals www.mijnbank.nl) vertalen naar de juiste IP-adressen. Hierdoor kunnen kwaadwillenden via een achterdeur de

routing aanpassen. In reactie op zijn ontdekking is er software verschenen die het probleem kan oplossen. Het is echter de vraag of alle domain name servers inmiddels veilig zijn.

Betekent dit dat ik internet maar beter niet meer kan gebruiken om een betaling te doen omdat het onveilig is geworden? Nee, allerm minst. Maar er zijn wel wat extra maatregelen (zie kader) te nemen om het surfen een stuk veiliger te maken. Drie keer kloppen is een goed begin, loop regelmatig deze stappen langs. Controleer vooral ook de instellingen van uw ADSL- en kabelmodem en uw wireless router thuis. Daarmee verkleint u de kans dat u slachtoffer wordt van fraude.

Dit artikel is tot stand gekomen met de medewerking van Gruus van Woerkom van internethostingprovider Byte.nl. Byte wees enige tijd geleden op problemen die bij het routeren kunnen ontstaan.

Bron: Andriessen, V. (2009, 15 augustus). Uitgebreide trukendoos van de internetfraudeurs. *Het Financieele Dagblad*, p. 27.