

Zorgen over bres in beveiliging internetbankieren

Vrijdag 7 december 2007, 11:49 - Ict-professor noemt het doorbreken van veilig geachte twee-factor authenticatie 'dramatisch'. De banken sussen: '3x kloppen en je bent veilig'.

Door **Andreas Udo de Haes**

Het circuleren van geavanceerde malware die de zogenaamde twee-factor authenticatie bij internettransacties omzeilt, zorgt voor onrust onder beveiligingexperts. Dat bleek donderdag tijdens het **Symposium Cybercrime** in Den Haag, georganiseerd door ict-platform ECP en cybercrime-onderzoekscentrum **Cycriis**.

Volgens ict-hoogleraar Bart Jacobs van de Radboud universiteit en lid van Cycriis, is deze ontwikkeling zeer zorgwekkend. "Het doorbreken van de twee-factor authenticatie middels malware is dramatisch te noemen."

De banken trachten intussen de onrust zo goed mogelijk te bedaren. "Dat de twee-factor authenticatie is 'gebroken' vind ik te zwaar aangezet." Aldus Wim Hafkamp, securitymanager van de Rabobank en voorzitter van het Financial Institutions-Information Sharing and Analysis Center (FI-ISAC), een werkgroep van de **Nederlandse Vereniging van Banken** en overheidspartijen als **NICC**, **GovCERT**, KLPD en AIVD.

Boef in de browser

Digitale privé-detective Pepijn Vissers van **Fox-IT** deed op de bijeenkomst uit de doeken dat het **internetbankieren**, sinds enige tijd wordt geteisterd door zogenaamde 'man in the browser'-aanvallen. Deze geavanceerde malware nestelt zich in de browser van onvoldoende beveiligde computers door middel van een Trojaans paard.

Zodra een gebruiker inlogt op een banksite, opent de kwaadaardige software een scherm met een foutmelding. Ondertussen zijn de criminelen al wél met de eerste code ingelogd op de banksite. Als het slachtoffer opnieuw probeert in te loggen, wordt deze code gebruikt om een frauduleuze transactie te bevestigen.

Ook de waterdicht geachte transactiebeveiliging middels edentificer- of TAN-codes, de zogenaamde twee-factor authenticatie, is hiervoor niet langer

veilig. Dit jaar zijn er al meerdere succesvolle virtuele plunderingen gerapporteerd, onder andere bij de **ABN-AMRO** en de **Postbank**.

Elsevier publiceerde recentelijk een **artikel** (betaalde toegang) over de wapenwedloop tussen cyberboeven en banken en ook Security.nl **berichtte** onlangs over het doorbreken van de twee-factor authenticatie.

3x kloppen

Hafkamp verzekerde de aanwezigen dat de banken er bovenop zitten. "Internetbankieren is nog steeds veilig en Nederland loopt hierin zelfs voorop. We hebben bovendien nog verschillende andere systemen om frauduleuze transacties te monitoren." Over hoe die systemen dan werken wilde Hafkamp niets kwijt, maar bekend is dat banken en creditcardmaatschappijen met slimme algoritmes verdachte transacties automatisch trachten te signaleren. Dit gebeurt op basis van gecombineerde variabelen als frequentie, hoogte en eindbestemming van de transacties.

Preventie en voorlichting spelen ook een cruciale rol bij de veiligheid van internetbankieren. "Alleen slecht beveiligde computers worden geïnfecteerd. Vandaar dat we ook zijn gestart met de '3 x kloppen'-campagne." Deze onlangs gestarte **voorlichtingscampagne** wijst de consument erop de computer en browser te beveiligen en de echtheid van websites te verifiëren. "Als je 3x klopt, is internetbankieren veilig", aldus Hafkamp.

Alternatieven

Wim Hafkamp benadrukte verder dat de financiële sector druk doende is met het ontwikkelen van nieuwe, nóg veiliger inlog- en authenticatieprocedures. Details hieromtrent wilde hij echter niet geven.

Globaal zijn er drie alternatieve richtingen. Ten eerste biometrische identificatiesystemen, zoals iris- en vingerafdrukscanners. Onduidelijk is echter vooralsnog in hoeverre ook deze data niet kan worden onderschept en omgeleid door malware. De uniciteit van bijvoorbeeld een 'iriscode' maakt in dat geval niets uit voor de veiligheid.

Datzelfde geldt voor een uitbreiding van de huidige twee-factor naar een drie-factor authenticatie. Ook hierbij is nog onduidelijk in hoeverre 'man in the browser'-malware niet ook 'simpelweg' ingevoerde codes kan doorsluizen. De huidige bres zit immers in de browser. Het codesysteem zelf hoeven de hackers helemaal niet te kraken.

Pepijn Vissers van Fox-IT bepleit daarom een aparte applicatie voor internetbankieren, los van de 'lekke' browsers. "Zoiets als de Girotel-software van vroeger, maar dan gebouwd volgens de laatste security-inzichten."



 **Tags:** [internetbankieren](#), [cybercrime](#), [twee-factor](#), [cycris](#).

Ads door Google

IDG Nederland is uitgever van [TechWorld](#), [Computer!Totaal](#), [ChannelWorld](#), [InfoWorld](#), [Tips & Trucs](#), [ZOOM.nl](#) en [GameZ](#).

Meer informatie: [IDG Nederland](#), [IDG Blog](#) en [IDG.com](#)