Beveiligingsonderzoeker kraakt tien banken

In vroeger tijden waren rijkaards bang dat iemand hun oude sok met zilveren munten zou stelen. Tegenwoordig vrezen we voor digitale inbraken.

Beveiligingsonderzoeker Wouter van Dongen van DongIT ontdekte in november 2014 bij toeval dat er iets mis was met de beveiliging van zijn eigen bank. Toen hij de fout beter onderzocht, bleken er maar liefst negen andere Nederlandse banken ook kwetsbaar voor hetzelfde type aanval.

Hoe kwam je dit probleem op het spoor?

"Ik bezocht de website van mijn bank en kreeg een foutmelding te zien die niet voor mag komen. Ik deed niets bijzonders, maar als beveiligingsonderzoeker zag ik meteen dat er iets niet klopte. De php-foutmelding die op mijn scherm verscheen kan namelijk alleen optreden wanneer de webapplicatie van de bank niet secuur geprogrammeerd is en ook andere instellingen niet correct zijn. Daarom was er een grote kans dat de website mogelijk ook kwetsbaar was voor een 'cross-site scripting' (xss)-aanval. Via een eenvoudige test heb ik gecontroleerd of dat zo was, bij mijn eigen bank en bij andere banken. In totaal bleken tien banken vatbaar voor dit type aanval, waaronder de ING, de Rabobank en ABN Amro."

Hoe werkt een xss-aanval?

"Bij dat type aanval verleidt een kwaadwillend persoon de gebruiker ertoe om ongebruikelijke code te starten die niet correct kan worden afgehandeld door de web-applicatie. Dat kan bijvoorbeeld door de gebruiker zover te krijgen dat deze klikt op een link in een phishing-mail, of op een malafide link in een online advertentie. Omdat de bankwebsite vervolgens de ondeugdelijke code niet filtert, wordt deze uitgevoerd binnen de browser. Een aanvaller kan zo in theorie de hele banksessie manipuleren en bijvoorbeeld een nepformulier starten. Zowel bank als klant zouden ondertussen denken dat alles in orde was. De verbinding zou versleuteld verlopen, wat zichtbaar zou zijn aan het slotje in de adresbalk. En het juiste web-adres zou zichtbaar zijn. Maar doordat de aanvaller zich via de xss-aanval tussen bank en klant zou hebben gedrongen, zou deze bijvoorbeeld de inloggegevens kunnen stelen en die op de achtergrond zelf gebruiken."

Waarom maakten tien banken dezelfde fout?

"Dat verbaast mij ook. Banken hebben de best beveiligde websites van het land. Deze worden regelmatig getest door grote security-bedrijven om dit soort fouten te vinden. Maar toch worden de gevaren van xss-aanvallen onderschat. Daarnaast wordt er nog steeds heel vaak geprogrammeerd zonder vanaf het begin na te denken over mogelijke manieren waarop de code kan worden misbruikt. 'Security by design' is zeldzaam. Zo was er slechts één bank die een Content Security Policy (CSP) had ingebouwd. Daarbij stuurt de webserver van de bank instructies naar de browser over welk Javascript uitgevoerd mag worden. Vervolgens controleert de browser van de klant of een specifiek Javascript voorkomt op de 'white list' en gestart kan worden. Alleen de relatief nieuwe Knab-bank had deze extra beveiligingslaag toegevoegd aan de bankwebsite."

Is het probleem opgelost?

"Ja, inmiddels wel, bij alle banken. Al heeft het bij een deel van hen meer dan twee maanden geduurd voordat ze het probleem serieus namen. Terwijl ik ze alle informatie had gemaild, volgens de regels die ze zelf hadden opgesteld in hun 'Responsible Disclosure Beleid'. Bovendien had ik hen een stukje code gestuurd waarmee ze met eigen ogen konden zien dat ik wijzigingen kon aanbrengen op de homepage van hun hoofddomein. Ik heb overigens niets kwaadaardigs gedaan, maar wel html-elementen op de bank-website laten dansen op de Harlem Shake. Een deel van de banken reageerde overigens wel heel goed. Vooral de Rabobank en Binck vielen positief op. Zij mailden binnen twee dagen terug en losten het probleem ook snel op. En zowel van de Rabobank als van de ING heb ik vijftig euro ontvangen als bedankje."

SITES

- dongit.nl
- websecurityscan.eu
- bit.ly/1CeoDMK
- nl.wikipedia.org/wiki/Cross-site_scripting

Wie: Wouter van Dongen
Waar: Leiden
Wat: Lek in bank-websites
Waarom: Slordigheid

Oproep

Doet u iets bijzonders met uw pc? Of hebt u een handige softwareoplossing voor uw hobby bedacht? Stuur dan een e-mail met als onderwerp **'Creatief met de pc'** naar **redactie@computeridee.nl**. Wie weet komt u ermee in Computer Idee.