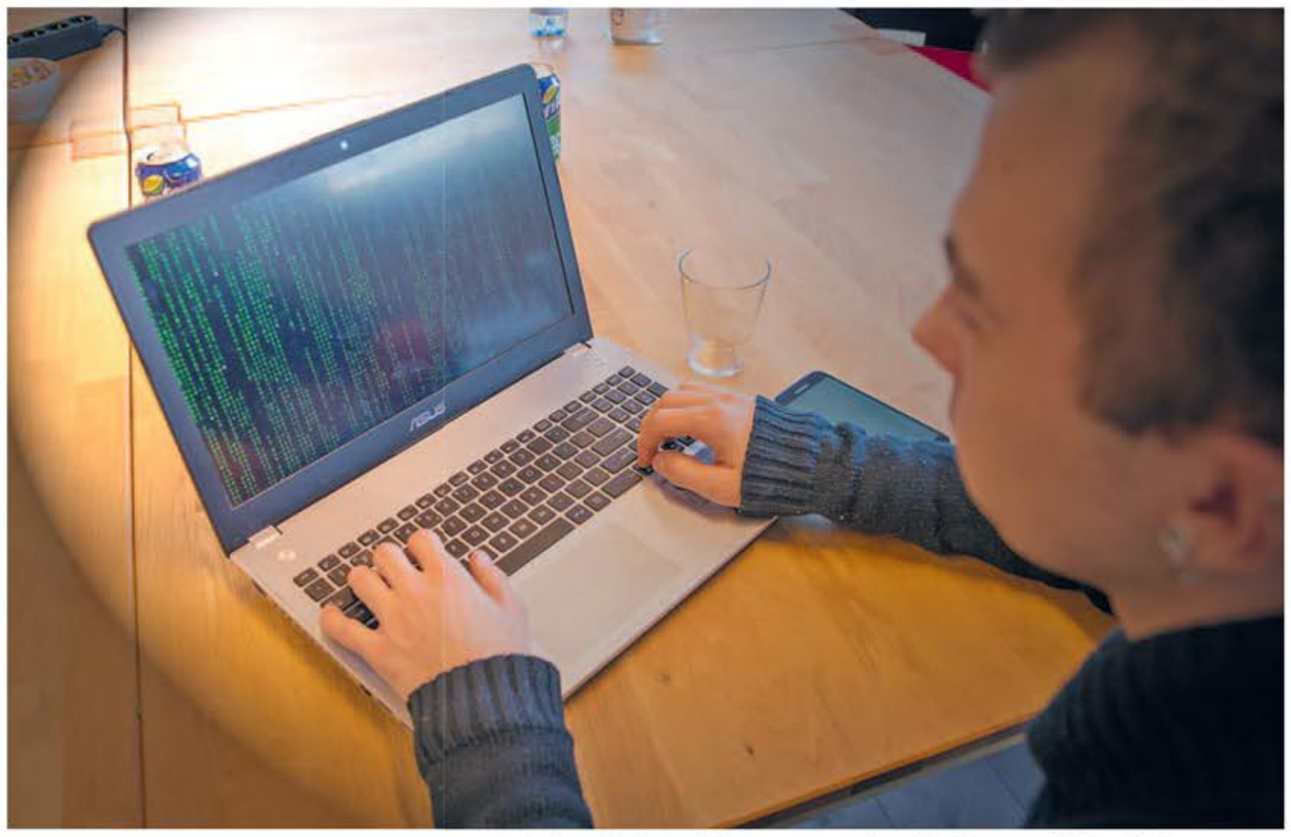
Klantgegevens uit een slecht beveiligde webshop halen, is voor Patrick de Brouwer een peulenschil.

HANS-LUKAS ZUURMAN BEELD HANS-LUKAS ZUURMAN

Nepshops gaan altijd op vrijdagmiddag online

internetshoppen

Producten kopen we steeds vaker online. Lekker makkelijk. Het *Nederlands Dagblad* speurt in een serie artikelen naar de wereld die schuilgaat achter de webshop. Vandaag deel 2: veiligheid.



Professioneel hacker Patrick de Brouwer controleert of webshops goed zijn beveiligd.

Zijn vingers glijden in razend tempo over de toetsen. Gevonden informatie over de werking van een website wordt direct ingezet om nieuwe onderzoekspogingen te ondernemen. Een webshop waarvan de beveiliging niet deugt, is door ethisch hacker Patrick de Brouwer (25) zo gevonden. Ietwat onderuitgezakt speurt hij met licht gefronste wenkbrauwen het wereldwijde web af.

De Brouwer werkt sinds 2010 als docent bij de Security Academy in Woerden. Daar worden mensen opgeleid om digitale inbrekers buiten de deur te houden. 'Ik zoek een willekeurige webshop met een simpele kwetsbaarheid waardoor ik in de database kan kijken', vertelt hij. Even later is het raak. Een online winkel voor technische vakliteratuur blijkt niet goed beveiligd. De Brouwer wijst op de adresbalk in de internetbrowser en zegt: 'Er staat geen "https" voor het adres van de website en ik zie geen pictogram van een gesloten slotje in de adresbalk staan. Dat betekent dat iedereen die op hetzelfde wifi-netwerk zit, stiekem kan meelezen met de gegevens die ik verstuur als ik een boek bestel. Om ervoor te zorgen dat alleen verkoper en de koper weten wat er besteld is, moeten de gegevens versleuteld verstuurd worden.'

creditcardgegevens

Volgens De Brouwer is het een kwestie van een aantal slimme commando's invoeren om de database van de boekensite te bereiken en zelfs het beheer ervan over te nemen. Als hij zou willen, kan hij binnen tien minuten alle klantgegevens uit de database kopiëren. Zonder dat iemand het weet. 'Dit bedrijf krijgt een waarschuwing van mij. Wat hier fout is, is nog vrij basis', concludeert hij na een snelle test.
Hoe je bedrijven kunt 'hacken' laat De Brouwer deelnemers geregeld zien tijdens trainingen die hij geeft in de digitale oefenomgeving van de Security Academy. 'Ik demonstreer hoe je het beheer van een site overneemt en kunt nagaan of er creditcardgegevens te vinden zijn. Voor klanten is het niet fijn als een online winkel slecht beveiligd is. Het gaat immers ook om hun gegevens die op straat kunnen komen te liggen.' Het daadwerkelijk online afrekenen gaat vaak via externe partijen als een creditcardmaatschappij, PayPal of iDeal. De Brouwer: 'Ik weet dat betalingsmogelijkheden via internet geregeld worden onderzocht door een goede hacker. Daar mag je op vertrouwen. En gaat het een keer mis, dan komt dat vrij snel aan het licht.'

KvK-register

Volgens De Brouwer beveiligen webshops hun site lang niet altijd voldoende, omdat het versleutelen van informatie rekenkracht op de server kost en gepaard gaat met de nodige investeringen. 'Het kan echter voorkomen dat de hele site niet goed beveiligd is, behalve het deel waar je privacygevoelige informatie in moet vullen.' Goed kijken op welke site je je bevindt, is ook een vereiste om problemen te voorkomen, weet De Brouwer. 'Je kunt namelijk ook ongemerkt op een door criminelen gemaakte kopie van een site belanden. Je wilt bijvoorbeeld naar mediamarkt.nl, maar tikt in: medilamarkt.nl. Daar gokken ze dan op.'
Woordvoerder Joyce Donat van de Consumentenbond herkent ervaringen van klanten met nepwebshops. Ze ziet de meldingen vaak voorbijkomen. 'Meestal brengen criminelen deze shops op vrijdagmiddag online en zijn ze 's maandags weer verdwenen. Typografie en plaatjes van websites van een bekend bedrijf worden gekopieerd voor de nepsite. Je bestelt er iets, betaalt het keurig, maar er wordt niets geleverd. Voor de mensen die tussentijds argwaan hebben gekregen, melden de criminelen vaak netjes een telefoonnummer van een bedrijf. Maar ze zorgen er wel voor dat er op dat moment een telefoonbeantwoorder aanstaat. Want tja, het is wel weekend, hè?'

De nepshops worden vaak via advertentiesites als Marktplaats aangeprezen. Donat vervolgt: 'Let goed op: de deal die wordt aangeboden is vaak te goed om waar te zijn. Maar ook criminelen worden steeds slimmer: ze prijzen een populair artikel zodanig af dat het een goede deal lijkt. Check daarom altijd of het artikel elders te vinden is. Als het overal uitverkocht is, maar déze winkel heeft er nog genoeg, is dat verdacht en moet je op je hoede zijn.'
Of een site een vangnet van een crimineel is of niet, is vaak al te controleren via zoekmachines als Google. 'Tik de exacte bedrijfsnaam in om te zien of-ie bestaat. Krijg je geen vermeldingen en geen positieve of negatieve meldingen, dan is de kans groot dat het bedrijf nep is', legt Donat uit. De Brouwer vult aan: 'Controleren of het bedrijf ingeschreven staat in het register van de Kamer van Koophandel (KvK) is ook een optie. Controleer via het online KvK-register met wie je in zee gaat. Elke webshop moet een KvK-nummer hebben. Ook wanneer er alleen een 06-nummer op de site staat in plaats van een vast nummer is er reden om extra alert te zijn. Of bel het nummer om te kijken of het werkt. In het algemeen geldt: hoe meer informatie je van tevoren hebt, des te beter het is.'

keurmerk

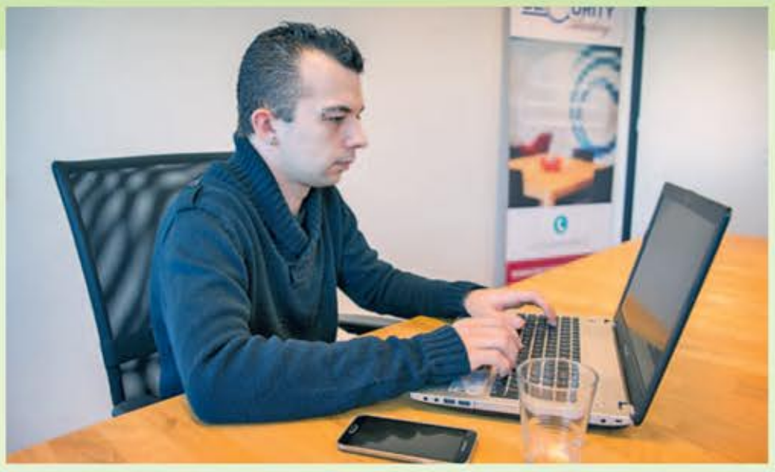
Donat wijst op de site opgeletopinternet.nl. 'Daar staan de actuele meldingen over fraude met websites. We zien dat het vooral voorkomt met verkoop van mobiele telefoons, laptops en tablets. Maar ook andere zaken als bakfietsen en parfums komen voorbij.' Donat signaleert dat nepwebshops ook geregeld gebruikmaken van logo's van keurmerken om de klant te overtuigen dat het goed zit. 'Shops zetten bijvoorbeeld het logo van keurmerk Thuiswinkel op hun site, maar als je erop klikt, word je niet doorgelinkt naar hun website of beland je op een site over het keurmerk die de criminelen zelf gemaakt hebben.' Dat laat volgens Donat direct zien dat criminelen steeds gewiekster te werk gaan. Ons advies is: ga naar de site van Thuiswinkel.org en controleer alleen dáár of de webshop bevoegd is het keurmerk te voeren.'

Blijf als websitegebruiker alert, onderstreept ook De Brouwer. 'Het gebruikmaken van een openbare wifi-hotspot bij een dierentuin of restaurant is populair, maar een hacker kan de verbinding omleiden waardoor verstuurde informatie op zijn computer terechtkomt. Hij kan tevens de naam van de hotspot in een uitnodigende naam veranderen en je zo verleiden daarop in te loggen.' De Brouwer herinnert zich een sessie die hij gaf in 'een grote onderwijsinstelling op universitair niveau'. Het wifi-netwerk was daar geheel onbeveiligd. Al het internetverkeer van docenten en studenten werd onversleuteld verstuurd. 'We hebben toen snel de ICT-afdeling ingeseind. Die hebben het collega van ons vervolgens ook gevolgd.'

F12

De Brouwer is intussen weer aan het surfen. Hij komt op een site van een aan de weg timmerend online-warenhuis. 'Je ziet dat deze website om 'cookies' vraagt', zegt ethisch hacker. 'Dat doen alle sites overigens. Cookies zijn kleine bestandjes waarin gegevens over jouw gedrag op de site worden opgeslagen. Druk op F12 en je ziet welke cookies je hebt toegestaan. Je ziet dan dat er op de achtergrond meer over jouw internetgedrag verstuurd wordt dan je denkt. Het is belangrijk geregeld te checken of je privacy niet in het geding is. De site van dit grote warenhuis legt precies uit wat welke cookie doet. Dat lijkt op zich sympathiek, maar is ook weer niet al te slim. Want voor een hacker is dat interessante informatie.' Als een hacker de werking van het cookie weet te beïnvloeden, kan hij de internetverbinding tussen de klant en het bedrijf manipuleren. 'Je kunt dan bestellingen plaatsen en bepalen waar het afgeleverd wordt. Je laat de factuur naar het huisadres sturen en de aflevering in een leegstaand kantoor dat je tijdelijk gebruikt voor het opvangen van bestellingen. Zo makkelijk is het', zegt De Brouwer. Als professional kent hij de zwakke punten van het internet als geen ander. 'Het blijft altijd een gok om veilig online te kunnen kopen, er zijn zo veel punten waar je op zou moeten letten. Je moet het maar net allemaal weten.' Zelf bestelt hij niet vaak goederen online. 'Ik ben iemand die iets toch gelijk in zijn handen wil hebben.' ■

'Je wilt bijvoorbeeld naar mediamarkt.nl, maar tikt medilamarkt.nl.'



'ik mag niet alle hack-trucjes gebruiken'

'Ik mag kietelen, maar niet schoppen. Ik mag dus zeker niet alles maar doen wat ik wil', vertelt ethisch hacker Patrick de Brouwer over zijn werk voor de Security Academy. Volgens hem zijn 'serieuze bedrijven' geregeld nog kwetsbaar op internet voor mensen die kwaad willen. En dat geldt ook voor webshops. 'Bedrijven geven soms te veel informatie over hun systemen prijs. Als ze met een verouderde versie werken, zoeken hackers de gebreken ervan. Zo komen ze vaak binnen.' Hij weet dat hackers altijd van alles proberen. Zelf deed hij dat ook. 'Vanaf mijn dertiende ben ik al bezig met computers. Vooral programmeren vond ik interessant. Ik ontdekte dat je er niet alleen leuke dingen mee kon maken voor op het internet, maar ook zaken slopen op servers van scholen of overheden. Daardoor kon je iets naar je hand zetten. Hoe kun je iets zodanig manipuleren dat eruit komt wat je wilt hebben? Het ging mij er niet om schade te veroorzaken, het was puur de kick. Het gevoel dat je toch even wilt binnenkijken, ook al staat op het pand 'verboden toegang'. Ik ben daardoor acht keer afgesloten geweest van internet door mijn provider. Je zoekt natuurlijk de grenzen op. En natuurlijk ken ik trucjes om binnen te komen. Maar die kan en wil ik niet gebruiken, anders draai je zo de bak in.' Uiteindelijk besloot hij daarom zijn kennis in te zetten om bedrijven te helpen lekken tijdig te dichten en trainingen te gaan geven.