Voor De Correspondent volgt technologiespecialist Chris van 't Hof de ethische hacker 0xDUDE. Waarom wil die het internet veiliger maken?

Dimitri Tokmetzis
Correspondent Veiligheidsindustrie

Portret

03.06.2016 • *Leestijd 5 - 6 minuten*

Maak kennis met 0xDUDE. Dit hele jaar speurt hij vijftien uur per dag het internet af om kwetsbaarheden in websites te vinden én ze netjes te melden. Wat vond hij de eerste maanden?

Artikelen op Wired aanpassen en chemische installaties besturen. Zo kwetsbaar is het internet

Gastcorrespondent Helpende hackers

Chris VAN 'T HOF

Eind januari treffen we elkaar eindelijk weer eens, in een lunchroom in Den Haag. Voor ethisch hacker Victor Gevers (alias 0xDUDE) is het de eerste keer deze maand dat hij zo ver van huis is. Om vijftien uur per dag lekken op te sporen en te melden,

heeft hij zich min of meer thuis opgesloten.

oxDUDE op Twitter

Hoe bevalt dat? 'Ik voel me geweldig!' zegt hij. 'Mijn vrouw verbaasde zich erover dat ik elke dag zo enthousiast opsta, om uiterlijk om zeven uur aan het werk te gaan.'

Omdat hij soms tot diep in de nacht doorgaat, vraag ik hem wat de impact op zijn gezinsleven is. Die blijkt mee te vallen. Gevers heeft zijn dagschema aangepast aan dat van de schooltijden van zijn drie kinderen. 'Eigenlijk zien ze me nu meer dan eerst.'

Voor hemzelf geeft deze intensieve hacksabbatical dus juist rust. Eindelijk kan hij zich echt focussen op al die meldingen die nog afgehandeld moeten worden. Want dat is het idee van zijn sabbatical: voormalig ambtenaar Gevers speurt een jaar lang elke dag het internet af naar kwetsbaarheden. Niet om mensen te hacken, juist om te voorkomen dat ze gehackt worden. Hij meldt zijn vondsten vervolgens discreet bij de eigenaren van de systemen.

Wat zeggen de eerste bevindingen?

Hij heeft een analyse gemaakt van de eerste vier weken: 119 meldingen van kwetsbaarheden, verspreid over 110 bedrijven in 32 landen: in totaal 9,5 terabyte aan open databronnen, oftewel 10.000.000 keer deze tekst. 65 procent van de kwetsbaarheden is inmiddels gefixt.

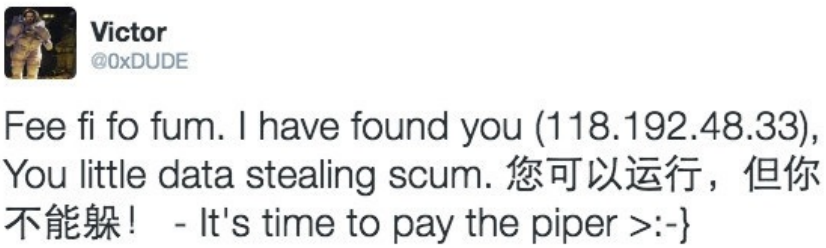
'Iemand in China was allerlei open databases van over de hele wereld aan het leegtrekken, maar

Hem valt op dat grote multinationals vaak laks reageren op zijn meldingen. Je zou verwachten dat grote bedrijven een afdeling hebben voor beveiligingsproblemen, maar blijkbaar wijzen de verschillende afdelingen vooral naar elkaar. Kleine organisaties reageren vaak wel snel op zijn meldingen.

had zelf ook zijn beveiliging niet op orde'

Verder valt hem op dat Nederlandse organisaties steeds beter reageren op zijn meldingen: lekken worden sneller gedicht, gevolgd door een ‘bedankt voor het advies.’ Uit landen als Rusland en Oekraïne hoort hij in de regel nooit wat terug, ook als het om een bank of energiecentrale gaat. De lekken worden wel gedicht.

Ook zag hij veel andere hackers op zoek naar kwetsbaarheden. En niet altijd met goede intenties. 'Iemand in China was allerlei open databases van over de hele wereld aan het leegtrekken, maar had zelf ook zijn beveiliging niet op orde. Dat heb ik gemeld bij het Chinese CERT, maar ook daar werd niet op gereageerd.' Bij hoge uitzondering meldde hij dit op Twitter.



Hoe we het in Nederland doen

Vaak ziet 0xDUDE niet één lek, maar een keten aan kwetsbaarheden: een eigenaar van de data gebruikt een applicatie van een leverancier, die de applicatie weer heeft gehost bij een provider in een ander land. 'Interessant is dat Nederlandse partijen vaak wel reageren op meldingen. Ik denk dat we ook best trots mogen zijn op hoe Nederland het doet.'

We zijn hier in Nederland inderdaad goed op weg met wat Responsible Disclosure heet: het verantwoord onthullen van kwetsbaarheden. Ook zijn er steeds meer organisaties die zich al voorbereiden op meldingen en zelfs een meldpunt openen waar helpende hackers

terechtkunnen.

De telecombedrijven, banken en Rijksoverheid openden hun meldpunten in 2014 en 2015. Daarna volgden gemeenten, ziekenhuizen en andere organisaties. Sommige loven zelfs beloningen uit.

Hoe het in het buitenland gaat

Tot zover Responsible Disclosure. Er zijn ook hackers die die procedure niet volgen en gevonden kwetsbaarheden juist publiceren zonder eerst de eigenaar van het systeem de tijd te gunnen het lek te dichten. Twitter en Pastebin staan vol met dergelijke onthullingen. Het idee achter deze Full Disclosure-benadering is dat organisaties meldingen dan niet kunnen negeren en wel moeten reageren.

0xDUDE ergert zich rot aan mensen die dat doen. Ze zorgen ervoor dat de kwetsbaarheid direct benut kan worden door kwaadwillenden en bezorgen hackers zo een slechte naam. Zo had een hacker een chemische installatie ontdekt die gewoon via internet te besturen was. Hij zette dit op Twitter met de opmerking: '*What could possibly go wrong*!?' Nou, dat laat zich wel raden: de samenstelling van mengsels aanpassen, pompen harder laten draaien, mogelijk zelfs een ontploffing tot gevolg.

Of wat te denken van babycams, de webcams die ouders gebruiken om hun kleintjes in de gaten te houden. Wat blijkt: veel van de babycams hoef je niet eens te hacken, ze staan gewoon online. 0xDUDE ontdekte dat veel inloggegevens gewoon op internet te vinden zijn, zowel die van de camera als de serviceprovider waar de data worden gehost.

Ook hier zag hij andere hackers die de open bronnen zonder waarschuwing op Twitter gooiden, compleet met linkjes naar de livebeelden. Zelf vond hij bijna 67.000 babycams online. Het is uiteraard niet te doen om elke gebruiker afzonderlijk te benaderen, dus meldde hij zijn bevindingen bij de leveranciers van de babycams en de providers die de verbindingen hosten.

Van sommige providers kreeg hij nog wel een reactie, maar geen van de leveranciers nam de moeite om hun klanten te informeren dat zij hun wachtwoord moesten wijzigen. Daarom zette hij maar een waarschuwing op zijn site en Twitter in de hoop dat de media het verder wel zouden oppakken.

Maar ook de media zelf weten lang niet altijd wat ze aan moeten met meldingen van oxDUDE. De redactie van magazine *Wired* - dat zich nota bene profileert als voorloper in de digitale wereld - had haar database al een tijdje openstaan. Zo kon je bijvoorbeeld zelf artikelen aanpassen en publiceren. Hij mailde dus het management van *Wired*, maar daar reageerde niemand. Hij besloot het daarom ludiek op te lossen en zette een Twitterpoll op over de vraag wat hij met de gevonden kwetsbaarheid moest doen. De meesten stemden voor '*Do a Full Disclosure*.'

Gelukkig kwam het niet zover, want direct na de poll reageerde @kathleencodes, technisch

manager van *Wired*. Ze beloofde via Twitter de verantwoordelijke aan te spreken en waardeerde '*the heads up*.' Inmiddels is het lek gedicht.

Steeds meer steun

Op 4 februari moest Gevers nogmaals zijn isolement verlaten. Hij werd door Surfnet, de IT-organisatie van de Nederlandse universiteiten, gevraagd naar Utrecht te komen om daar de Surf Security Award in ontvangst te nemen: 2.500 euro voor zijn bijdrage aan een veiliger internet.

Deze steun is bemoedigend en het geld is welkom, omdat hij verder niets verdient aan zijn meldingen. Hij heeft daarom een stichting opgericht: GDI.foundation, wat staat voor Global Defense of the Internet.

Steeds meer sluiten aan om hem te helpen: een ex-collega helpt met de administratie, sympathisanten geven donaties en stellen apparatuur ter beschikking. Dit jaar moet blijken of het genoeg is om het vol te houden.

In de volgende aflevering lees je hoe Gevers ook zelf steeds meer met zijn verhaal naar buiten treedt.

Lees ook: