

Hacking for Health

Dennis Baaten vraagt beveiligingsadviseurs om 'bug bounties' te doneren aan Stichting ALS Nederland.

Beveiligingsadviseur Dennis Baaten roept beroepsgenoten op om geldbeloningen die ze in hun vrije tijd verdienen met het aantonen van beveiligingslekken in bedrijfssystemen te doneren aan Stichting ALS Nederland.

Waarom deze actie?

"Het is een eerbetoon aan de vader van een van mijn beste vrienden, die eind 2012 is overleden aan de gevolgen van Amyotrofische Laterale Sclerose (ALS). Tijdens mijn studententijd in Delft had ik bijna wekelijks contact met hem. We hebben veel gelachen en mooie momenten beleefd. Daar ben ik hem dankbaar voor. Er zijn in Nederland ongeveer 1500 ALS-patiënten. Dat is een relatief kleine groep. Daardoor zijn de onderzoeksbudgetten van de farmaceutische industrie en de overheid vrijwel nihil. Verreweg het meeste wetenschappelijk onderzoek naar ALS in Nederland wordt gefinancierd door giften aan Stichting ALS Nederland."

En waarom hacken?

"Andere mensen organiseren een sponsorloop, maar doordat

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.

Wie: Dennis Baaten
Waar: Rotterdam
Wat: Hacking
Waarom: ALS-onderzoek

informatiebeveiliging mijn passie is, heb ik gekozen voor het vinden en melden van beveiligingslekken. Wanneer ik in de late uurtjes speur naar beveiligingskwetsbaarheden op websites, vind ik er altijd met gemak één of meer. Wat ik vaak tegenkom is de mogelijkheid van cross site scripting (XSS). Dat is een fout in de beveiliging van webapplicaties die veel voorkomt en ook gemakkelijk te ontdekken is. Kwaadwillenden kunnen zo'n kwetsbaarheid misbruiken om schadelijke code laten draaien



HACKING
for health

op de machines van onwetende websitebezoekers. Wanneer ik een lek vind, meld ik dat altijd netjes aan de website-administrator zodat die het op kan lossen. Ik ben niet de enige. Veel van mijn collega's doen hetzelfde in hun vrije tijd. Hen vraag ik nu om eventuele geldbeloningen deels te doneren aan onderzoek naar ALS. Maar los daarvan mogen ze ook gewoon doneren, hoor. Alle donateurs neem ik op in een online hall of fame."

Krijg je als hacker vaak beloningen?

"Soms krijg je een aardigheidje, in de vorm van een cadeaubon of T-shirt. En soms hoor ik helemaal niets, maar is het probleem na een paar weken wel verholpen. En het gebeurt ook

dat mensen enorm schrikken. Ik ben wel eens 's avonds laat opgebeld door iemand die zijn naam niet wilde noemen. Hij vroeg wantrouwig waarom ik zijn systemen onderzocht op zwakheden. Terwijl ik dat doe met heel goede bedoelingen, om het internet veiliger te maken. De angst om vervolgd te worden voor computervredebreek kan hackers ervan weerhouden om beveiligingslekken te melden bij organisaties. In sommige gevallen kiezen ze er dan voor om zwakheden anoniem openbaar te maken, zonder organisaties vooraf de kans te geven om het lek te verhelpen. Om die reden heeft het Nationaal Cyber Security Centrum (NCSC) in 2013 een leidraad ontwikkeld waarmee organisaties aan

ethisch hackers de mogelijkheid kunnen bieden om zwaktes verantwoord te melden. Eigenlijk alleen de grotere organisaties delen echt hoge premies uit aan hackers die op die manier serieuze beveiligingsproblemen melden. Dat geldt bijvoorbeeld voor Google, Twitter en Dropbox. Er bestaan zelfs officiële 'bug bounty'-platformen, zoals hackerone.com. Daar kunnen grote bedrijven de hulp inroepen van ethische hackers voor het vinden van lekken. Als die hackers vervolgens een ernstige beveiligingszwakte vinden ontvangen ze een beloning, die tot in de tienduizenden dollars kan oplopen." 

Tekst: Jolein de Rooij

SITES

- www.hackingforhealth.nl
- www.als.nl
- www.ncsc.nl/actueelResponsible+Disclosure+Leidraad