HOE HET INTERNET VEILIGER WORDT DOOR *'RESPONSIBLE DISCLOSURE'*

Vaak genoeg lees ik in de media over grote bedrijven die onveilig zijn, een grote leverancier of organisatie die weer gehackt is of hoe we het allemaal anders moeten doen omdat we anders onveilig zijn. Het goede werk dat honderden ethische hackers verrichten blijft echter onderbelicht.

Tekst: *Mischa Rick van Geelen*

Via zoekmachines zoals Shodan, dat de Google van het Internet of Things genoemd wordt, kun je een duidelijk overzicht krijgen van wat er eigenlijk allemaal met het internet verbonden is. Shodan zoekt dagelijks grote delen van het internet af naar nieuwe apparaten die onvoldoende of helemaal niet beveiligd zijn.

Veel van de apparaten op Shodan zijn bijvoorbeeld beveiligingscamera's, alarmsystemen, temperatuurregelaars of water- en oliepompen. Maar ook apparaten voor het besturen van industriële systemen, zoals windmolens of noodaggregaten. Vaak zijn deze systemen niet eens beveiligd met een wachtwoord.

Een praktisch voorbeeld hiervan is RandomVNC.net, een website die screenshots toont van open computers die verbonden zijn met het internet. Via een grafische interface kun je door ruim tweeduizend onbeveiligde computers heen klikken. Iedereen die van het bestaan weet zou deze apparaten kunnen besturen. Hierdoor wordt onze samenleving kwetsbaar voor aanvallen van staatsactoren, activistische organisaties en cybercriminelen.

In een poging deze risico's terug te dringen is 'Responsible Disclosure' bedacht.

'RESPONSIBLE DISCLOSURE'

De term Responsible Disclosure (of RD) is bedacht in samenwerking met Floor Terra. Het beleid wordt actief uitgedragen door het Nationaal Cyber Security Centrum (NCSC). Dit onderdeel van het ministerie


© WALTER KALLENBACH

van Justitie en Veiligheid heeft ten doel het knooppunt voor het digitale domein te zijn voor overheidsinstellingen en bedrijven in Nederland. De bedoeling is om hackers die een lek hebben gevonden bij een organisatie de mogelijkheid te bieden dat te melden en daarvoor ook een ludieke beloning te krijgen, zoals bijvoorbeeld een T-shirt, cadeaubon of soms geld. Organisaties kunnen een zogenaamd RD-beleid op hun website zetten, waarin ze duidelijk vermelden tot hoever een hacker mag gaan en met wie de hacker contact kan opnemen als een lek is gevonden. Het beleid geeft hackers dus de mogelijkheid de lekken die ze vinden te melden, zodat de organisatie deze kan oplossen zonder dat hackers bang hoeven te zijn voor juridische en strafrechtelijke gevolgen. Het beleid is de afgelopen jaren steeds populairder geworden bij hackers.

MELDINGEN

Inmiddels staat de teller van mijn meldingen richting organisaties op 500+, waaronder bijvoorbeeld ook Ahoy Rotterdam waar verschillende wifirouters waren verbonden met het internet zonder wachtwoord. Dit zorgde ervoor dat al het verkeer af te luisteren was van degene die gebruik maakte van het wifinetwerk. Na samen met Joost Schellevis van NOS het lek te hebben gemeld, werd het snel opgelost.

Ook grote organisaties als Apple, Google of Facebook hebben zogenoemde 'bug-bounty' programma's opgezet, om zo de platformen veiliger te maken. Vaak geeft dit soort tech-bedrijven hoge beloningen voor het melden van lekken, oplopend tot wel 20.000 euro per melding.

In mijn inmiddels meer dan vijfhonderd ervaringen met 'Responsible Disclosure' weet ik dat veel organisaties die een melding krijgen in eerste instantie vaak niet goed weten hoe ze moeten reageren. Terwijl grotere organisaties, zoals banken, overheid en grote ondernemingen in Nederland, vaker meldingen hebben gehad over de digitale veiligheid van de organisatie.

Na een simpele uitleg over wat 'Responsible Disclosure' is, snappen veel organisaties vaak al de intentie erachter en nemen ze het advies ter harte.

'Responsible Disclosure' werkt. Bij alle organisaties waar ik sta, adviseer ik dan ook zo'n beleid in te voeren om hun digitale domein veiliger te maken.

info@speakersacademy.nl