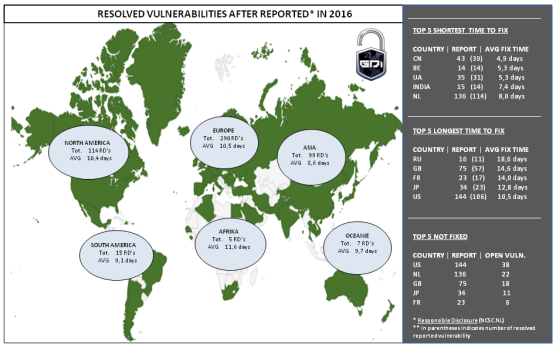
Het resultaat na 366 dagen ethisch hacken: “Security zo lek als een mandje”

January 3, 2017 | Gijs Ettes



Een jaar geleden lanceerden ethische hackers Vincent Toms en Victor Gevers van GDI.Foundation PROJECT366. Een jaar lang besteden ze vrijwel al hun vrije tijd aan het opsporen kwetsbaarheden en het voorkomen van hacks. Het resultaat: 690 ontdekte ernstige beveiligingslekken ontdekt en gerapporteerd aan meer dan 590 organisaties, verdeeld over 71 landen.

“Dat hadden er echter duizenden meer kunnen zijn gezien de lekken die we aantroffen. De verificatie van een gedetecteerde kwetsbaarheid vergt echter de nodige tijd en zorgvuldigheid”, aldus Vincent Toms van GDI.Foundation. Internationaal gezien werden in 2016 maar liefst 6324 lekken ontdekt en gerapporteerd, wat het totaal sinds 1999 op 79.172 brengt. “Ruim de helft hiervan betreft publieke exploits, die iedereen - dus ook cybercriminelen - kan misbruiken.”

In Nederland en België trof GDI.Foundation respectievelijk 136 en 14 ernstige beveiligingslekken aan. Opvallend is dat Nederlandse organisaties er gemiddeld 8 dagen over doen om na een melding tot actie over te gaan. Belgische organisaties hebben slechts 5,3 dagen nodig om een beveiligingslek te dichten. Het wereldwijde gemiddelde is 10,8 dagen, vergelijkbaar met Europa (10,5 dagen o.b.v. 366 lekken). Opvallend is dat getroffen bedrijven en organisaties in China (43 lekken) beduidend sneller reageren met respectievelijk 4,9 dagen. Helaas staan daar ook nog meldingen open waarop geen actie is ondernomen.

Gevers: “Ondanks dat niet elke organisatie even snel reageert, zijn we positief gestemd over het aantal reacties en wijze waarop gereageerd wordt. Van landen waarvan je geen reactie zou verwachten, komen vaak de leukste reacties en bedankjes.” Wat had het opgeleverd als de data was verkocht of als misbruik was gemaakt van de kwetsbaarheden? “Gezien het grote aantal lekken en de hoge autorisaties die we konden bemachtigen, hadden we met de verkoop van data gemakkelijk meerdere langdurige vakanties kunnen bekostigen.” Op zogeheten dark markets is een levendige handel in gebruikersgegevens die zijn buitgemaakt als gevolg van lekke databases.

Hoewel PROJECT366 officieel ten einde is, gaat GDI.Foundation dit jaar door met opsporen van kwetsbaarheden. “De mogelijkheden van cybercriminelen nemen nog steeds toe, en om risico’s te reduceren is een integrale en internationale aanpak noodzakelijk. Mede dankzij funding van SIDN fonds kunnen we in 2017 starten met de ontwikkeling van een security dashboard dat landen, overheden en organisaties inzicht geeft in actuele beveiligingslekken en hoe die kunnen worden gedicht. De tool geeft ook inzicht in trends en toekomstige cyberrisico’s, zodat sneller gepaste maatregelen genomen kunnen worden.”
Voor 2017 voorspelt GDI.Foundation de volgende top 5 cyberdreigingen:

1. **Mens blijft zwakste schakel.** Ook in 2017 weer op de eerste plaats als grootste dreiging. Het niet verrichten van noodzakelijk updates, de omgang met wachtwoorden en het versturen/meenemen van gevoelige documenten naar huis.
2. **Legacy & bekende kwetsbaarheden.** Dit is mede het gevolg van ons eigen handelen. Het uitbuiten van bestaande kwetsbaarheden wordt elk jaar gemakkelijker en vereist vrijwel geen technische kennis meer. Alles wat je moet weten om de kwetsbaarheden te misbruiken staat op internet, mits je weet waar je moet zoeken.
3. **IoT & Time to Market.** De markt voor IoT is booming, dankzij diverse nieuwe diensten en devices die blijven verschijnen. De mogelijkheden staan pas in de kinderschoenen en de kosten zijn bijzonder laag. Door de haast die bedrijven hebben met het uitbrengen van producten, wordt goede security vaak vergeten.
4. **Big (lekkende) Data.** Het voordeel voor cybercriminelen is dat veel privacygevoelige informatie al bijeengebracht is door een organisatie. Een wet die een opwaarts effect kan hebben op de prijs van data, is de nieuwe EU-wet “General Data Protection Regulation” (GDPR). Het gebruik van cookies voor marketing etc. wordt hierdoor bemoeilijkt, maar zal de behoefte naar informatie niet verminderen.
5. **Cybercrime as a Service.** Verdere professionalisering van internetdiensten op basis van vraag en aanbod. Cybercrime als service levert weinig risico voor de (ver)koper op en een hoge return of investment. Van ransomware tot het manipuleren van verkiezingen. Runner-up voor de top 10 van “Best betalende baan 2017”.

Lees voor meer informatie het GDI.Foundation jaarrapport 2016

Recent


UPDATE BLOG: progression (Not)Petya & WannaCry
July 8, 2017


Blog: progression (Not)Petya & WannaCry
July 5, 2017


Intelligence door aggregatie van open-source bronnen
April 24, 2017


Live demo “Cyber Security Health Check”
March 17, 2017


Ransomware seemingly hits faster than management can fix
February 17, 2017


Zo bescherm je je privacy bij het invullen van de Stemwijzer
February 7, 2017


GDI.Foundation treft eerste ransomware op Elasticsearch aan
January 15, 2017

GDI.Foundation genomineerd voor ISOC.nl Innovatie Award 2017
January 7, 2017


Het resultaat na 366 dagen ethisch hacken: “Security zo lek als een mandje”
January 3, 2017


Our Presentation GFCE (Hungary) & Lesson Learned Responsible Disclosure
May 9, 2016