Intelligence door aggregatie van open-source bronnen

April 24, 2017 | V.Toms (GDI.Foundation) & R.Spoor (SURFnet)

Buiten organisaties is meer en accuratere kennis beschikbaar over security-bedreigingen die van belang zijn voor de ICT-dienstverlening van deze organisaties. Dit komt doordat in de cloud diverse partijen specifieke remote scans uitvoeren op de ICT-infrastructuur van instellingen om te zoeken naar kwetsbaarheden. Door de vergaarde intelligence van deze partijen te aggregeren, creëer je een interessant overzicht van security-bedreigingen.

OSINT

Er zijn diverse openbare bronnen op het internet die informatie geven over kwetsbaarheden in computersystemen of gelekte gevoelige informatie op het internet. De bronnen komen aan deze informatie door bijvoorbeeld scanners te gebruiken die aan het internet verbonden apparaten checken op aangeboden ICT-services.

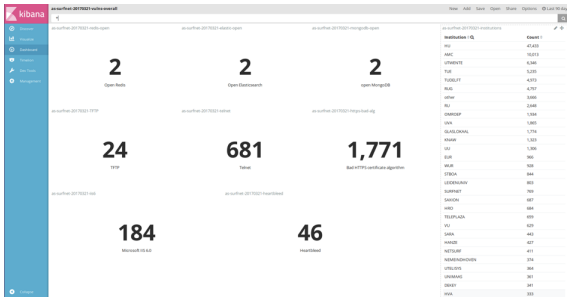
Vervolgens worden de scanresultaten opgeslagen en via een search-engine en/of API vrijelijk aangeboden aan eindgebruikers. De betrouwbaarheid en nauwkeurigheid van dit soort bronnen, die vanaf het internet naar organisaties 'kijken', overstijgt veelal de informatie die organisaties zelf hebben. Daarnaast zijn ze vaak specifiek gemaakt om bepaalde kwetsbaarheden te detecteren, en daarmee zeer nauwkeurig. Dit soort bronnen duiden we aan als Open-Source Intelligence (OSINT), omdat ze gebruikmaken van openbare informatie om intelligence te vergaren.

Ook bij SURFnet is er behoefte aan een manier om met behulp van deze bronnen nieuwe kwetsbaarheden of gelekte informatie uit de systemen van SURFnet (en aangesloten instellingen) overzichtelijk en laagdrempelig te tonen. Met als doel om een goed beeld te krijgen van de door verschillende OSINT-bronnen gedetecteerde zwakheden of kwetsbaarheden.

Dit beeld wordt gedeeld via de SCIRT-community, de CERT/CSIRT teams van de bij SURFnet aangesloten instellingen, zodat er indien nodig adequate actie kan worden ondernomen. Het delen van de informatie, kennis en kunde met de SCIRT-community zorgt ervoor dat het uiteindelijke dashboard aansluit bij informatiebehoefte.

Samenwerking

Halverwege 2016 is SURFnet samen met GDI.Foundation gestart met het ontwikkelen van een dashboard waarmee organisaties online inzicht krijgen in de actuele cyberrisico's die ze lopen en de oplossingen, maar ook in trends en (toekomstige) cyberdreigingen. GDI is een non-profit organisatie, opgericht door Vincent Toms en Victor Gevers, die als doel heeft om het internet veiliger te maken door gebruik te maken van OSINT-bronnen en responsible disclosure.



Proof of Concept

Er is een proof of concept-omgeving opgesteld waarbij op dit moment drie OSINT-bronnen, namelijk Shodan, Censys en IpInfo, gebruikt worden. De informatie uit deze bronnen wordt automatisch opgevraagd en vervolgens gestructureerd opgeslagen in een Elastic Stack omgeving bestaande uit Logstash, Elasticsearch en Kibana.

Eindgebruikers van de tool kunnen met Kibana, die de verzamelde data visualiseert, dashboards configureren die een algemeen beeld op hoog niveau geven over gevonden kwetsbaarheden binnen SURFnet en aangesloten instellingen. Ook kan informatie over getroffen IP-adressen op detail bekeken worden, zodat men over de nodige informatie beschikt om vervolgacties te ondernemen.

Dit heeft een praktische tool opgeleverd waarin te zien is welke informatie en eventuele kwetsbaarheden zichtbaar zijn voor de buitenwereld. In de toekomst wordt deze omgeving verder uitgebreid met andere OSINT-bronnen en krijgen CSIRT/CERT-leden van instellingen toegang.

Voor de SURFnet omgeving zijn een aantal specifieke kwetsbaarheden in kaart gebracht die vanaf buitenaf te zien zijn. Het betreft onder meer inzicht in de status van digitale certificaten van websites, services die niet open naar buiten horen te staan, oudere versies van services die niet meer veilig zijn en nieuwe kwetsbaarheden door recent bekend geworden bugs in services.

Samen met de SCIRT community en GDI.Foundation werkt SURFnet aan het verder uitwerken van de proof of concept-omgeving. Hier is een weergave van de proof of concept omgeving beschikbaar gesteld.

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