# Security 2017 Opdracht 1: Bedreigingen en terminologie

Inleveren: UITSLUITEND via Blackboard. UITSLUITEND .dccx of .pdf formaat.

**Uiterste datum: 7-5-2017, 23:59uur.**

**Vraag 1. Terminologie**

Leg kort uit wat met de volgende termen wordt bedoeld (in het kader van informatiebeveiliging). Zoek waar nodig informatie via bv internet:

|  |  |
| --- | --- |
| Term | Beschrijving |
| Kwetsbaarheid (vulnerability) | Het onvermogen (van een systeem of een eenheid) om de effecten van een vijandige omgeving te kunnen weerstaan |
| Exploit | een stukje [software](https://nl.wikipedia.org/wiki/Software) of hoeveelheid gegevens die gebruikmaakt van een [bug](https://nl.wikipedia.org/wiki/Bug_(technologie)), [glitch](https://nl.wikipedia.org/wiki/Glitch" \o "Glitch) of kwetsbaarheid in de software van een apparaat om onverwacht en door de eigenaar van het apparaat meestal ongewenst gedrag te veroorzaken op de software of hardware van dat (meestal geautomatiseerde) elektronische apparaat. |
| Advanced Persistent Threat (APT) | Een langdurige en doelgerichte cyberaanval waarbij een onbevoegd persoon onopgemerkt en langdurig toegang krijgt tot een netwerk. Het doel is om continu toegang te krijgen en gegevens te stelen. APT-aanvallen richten zich vooral op landen en organisaties. |
| Threat Model | Een proces waarbij potentiële bedreigingen geïdentificeerd, opgesomd en geprioritiseerd kunnen worden - alles vanuit het perspectief van een hypothetische aanvaller |
| Asset (Computer security) | Elke data, apparaat of ander onderdeel dat informatiegerelateerde activiteiten ondersteunt, b.v. een server (hardware) of support programma (software) |
| Security Control | Vrijwaringsmaatregelen/tegenmaatregelen om beveiligingsrisico's te vermijden, op te sporen, tegen te gaan of te minimaliseren voor fysieke eigendom, informatie, computersystemen of andere assets. |

**Vraag 2: Verzamel informatie over onderstaande bedreigingen.**

**Vul zowel het doelwit van de bedreiging in als de activiteit**

Doelwit:

Hier wordt bedoeld zowel a) het systeem wat bedreigd wordt en b) de (soort)gebruiker die bedreigd wordt.

Activiteit:

Wat doet de betreffende dreiging ? Leg kort uit op welke manier de dreiging werkt (maar alleen “verziekt het bestand” is niet voldoende)

Sources:

<https://threatpost.com/china-hackers-compromise-iraq-experts-at-national-security-think-tanks/107059/>

<https://blog.malwarebytes.com/threat-analysis/2017/03/spora-ransomware/>

<https://tweakers.net/nieuws/72580/anna-kournikova-virus-wordt-tien.html>

mede leerlingen.

|  |  |  |
| --- | --- | --- |
| Threat | Doelwit | Activiteit |
| Deep Panda | U.S. military (Iraq) | Het werkt via een commandline zodat een anti-virus programma het niet kan detecteren.  Om de 2 uur download de commandline een programma genaamd wafer die stuurt alle data naar de deep panda server en hierna delete het zichzelf weer. |
| Spora | Computer gebruikers | Je kan dit op verschillende manieren binnenkrijgen op je computer onder andere: phishing e-mails en geïnfecteerde websites.  Nadat het op je computer is terecht gekomen ecnrpyt het bestanden met extensions. Daarna komt er een pop-up van UAC op je scherm die vraagt of jij iets wil accepteren, dit is niet weg te krijgen door gewoon op nee te drukken. Pas nadat jij op ja klikt wordt er een ander system tool gerunt genaamd vssadmin voor het deleten van shadow copies. Er verschijnt nu een command line window, waaring verschillende aanpassingen worden gedaan aan de bestanden op je computer, dit bestaat onder andere uit: de pijltjes op shortcuts uitzetten en files verstoppen. Hierna plaatst hij shortcuts van de verstopte files (zonder de pijltjes op de iconen lijken deze dus op de oude files) en wanneer de gebruiker een van deze aanklikt wordt de pc op slot gezet. |
| Macchina M2 | Auto’s | Dit is een klein apparaatje dat je kan instaleren in het slachtoffer zijn/haar auto. Dit apparaatje zorgt ervoor dat de gebruiker van dit apparaat wanneer hij/zij wil controle kan overnemen van de auto. |
| Anna Kournikova (Computer worm) |  | Het Anna Kournikova-virus is een e-mailworm; het werd verzonden in een mail met het onderwerp 'Here you have, ;o)' en een bijlage met de naam 'AnnaKournikova.jpg.vbs'.  Eenmaal gestart, stuurde de worm vergelijkbare mails naar alle personen in het adresboek van het slachtoffer. |
| BadUSB (-Vulnerability) |  | Wanneer iemand een hidden virus op een USB zet die automatisch wordt overgeplaatst naar het apparaat waar deze is ingeplugd dan wordt dit een BadUSB genoemd. Dit kan verschillende soorten virussen op het apparaat zetten bijvoorbeeld een keylogger die al de ingetikte tekst opslaat en doorstuurt naar de eigenaar van de USB. |

**Vraag 3. Hieronder staan een aantal security incidents. Geef aan (kruisjes in kolom) welke security-aspecten (volgens het CIA-principe) daarbij in gevaar worden gebracht.**

Zoek waar nodig op het internet naar informatie.

|  |  |  |  |
| --- | --- | --- | --- |
| Incident | Confidentiality | Integrity | Availability |
| Datalek bij de belastingdienst | X |  |  |
| Crashen van een harde schijf |  |  | X |
| Brand in het datacenter |  |  | X |
| Verlies van een USB-stick met belangrijke data | X |  | X |
| Besmetting van laptop met een rootkit | X | X |  |
| Ontvoering van de directeur | X |  | X |
| Versleuteling door ransomware | X | X | X |
| Een DDOS-aanval |  |  | X |
| Ongeautoriseerd inloggen van een hacker | X | X |  |

? = Mogelijk. Hangt af van de situatie. Bv. bij ontvoering van de directeur, kan de confidentiality in gevaar zijn, omdat het mogelijk is dat de directeur informatie loslaat aan de ontvoerders (maar dit hoeft niet altijd zo te zijn)

**Vraag 4. Social Engineering**

Bedenk twee manieren om op de NHL **via Social Engineering** informatie of rechten te verkrijgen. Het gaat hierbij om informatie of rechten die je **als student** normaal gesproken niet hoort te krijgen.

NB: Het gaat hierbij alleen om een gedachtenexperiment. Het is niet de bedoeling dat je dit echt uitvoert!

|  |  |
| --- | --- |
| Scenario 1: | Een pas lenen van een leraar om een lokaal binnen te komen. Met deze pas kan je verschillende locaties binnenkomen waar je normaal niet bij kan. |
| Scenario 2: | Naar de administratie bellen en mijzelf voordoen als een andere student zodat ik via hun toegang kan krijgen tot hun E-mail door middel van het wachtwoord te resetten. |