# Leeruitkomst 2: Risk Consultant

## Bewijslast: Risicoanalyse

Tijdens het analyseren van de resultaten van de pentest voor Cubics IT, heb ik een risicoanalyse gemaakt. In deze risicoanalyse staat beschreven welke risico’s gevonden zijn in het systeem van Cubics, en ook hoe groot de risico’s zijn op basis van de “kans \* impact” berekening. Daarnaast wordt beschreven hoe het risico opgelost, of verlaagd kan worden. Deze risicoanalyse staat in het pentest rapport dat wij voor Cubics geschreven hebben.

# 2. Onderzoeksmethode

A picture containing logo

Description automatically generatedTijdens de pentest is gewerkt volgens het “cyber kill chain” model. In figuur 1 wordt weergegeven hoe dit model eruit ziet. Hieronder is per stap te lezen wat het verrichte werk is. Niet iedere stap is volledig uitgevoerd. Zo is bijvoorbeeld de stap “exploitation” niet uitgevoerd, omdat schade aanrichten aan C-fence niet het doel van het project is.

Figuur 1

Afbeelding 1: De cyberkill chain

Reconnaissance.

De eerste stap is natuurlijk het verzamelen van informatie over het doelwit. Hiervoor is de website van Cubics afgespeurd voor nuttige informatie, maar ook social media platforms als LinkedIn zijn bestudeerd om informatie over de medewerkers te achterhalen. De belangrijkste bron van informatie over C-fence is Cubics zelf geweest. Cubics heeft informatie aangeboden over de werking van C-fence, en een IP-adres waarop een onderdeel gehost wordt.

Weaponization.

Nadat de benodigde informatie verzameld is, volgt het gebruiken van deze informatie. Om vanaf deze informatie tot een potentiële hack te komen, is gekeken waar mogelijk kwetsbaarheden liggen. Vervolgens is een plan opgezet om deze kwetsbaarheden bloot te leggen, en zijn de tools klaargezet die hiervoor nodig zijn.

Delivery, exploitation, installation en command&control.

Tijdens deze fase worden de “wapens” uit de vorige fase afgeleverd bij het doelwit, en de kwetsbaarheden vervolgens uitgebuit. Aangezien deze wapens vrij veel schade aan kunnen richten aan de oplossing van Cubics, worden deze stappen niet uitgevoerd. Wel is beschreven wat deze wapens zijn, en hoe ze onschadelijk gemaakt kunnen worden. Waarom deze keuzes gemaakt zijn, is later in dit verslag terug te vinden.

## 

## 2.1 Planning

Tijdens het plannen is informatie verzameld over het doelwit. De volgende onderwerpen stonden hierin centraal:

* De werking van C-fence.
* De technische infrastructuur van Cubics.
* IP-adressen waarop C-fence draait.
* Algemene informatie over Cubics als bedrijf.

Vervolgens probeerde we deze informatie te gebruiken om kwetsbaarheden te vinden in C-fence. Deze kwetsbaarheden hebben we niet geëxploiteerd omdat C-fence een live omgeving is waarvan de klanten van Cubics afhankelijk zijn om de veiligheid van hun digitale infrastructuur te waarborgen. Het is niet verantwoord om stappen te zetten die potentieel de functionaliteit van C-fence op het spel zetten.

## 2.2 Exploitatie

Door de gevonden informatie in Planning konden we beginnen met kwetsbaarheden vinden en waar mogelijk deze exploiteren. Hieronder vindt U een overzicht van de gevonden kwetsbaarheden.

Uit testcase 01 blijkt dat poort 161 op IP-adres 178.248.157.78 open staat, en gebruik maakt van SNMP. Vervolgens is gekeken of er een bekende CVE(Common Vulnerabilty and Exposures) is voor SNMP. [CVE-2002-0013](https://www.cvedetails.com/cve/CVE-2002-0013/?q=CVE-2002-0013) gaat over een kwetsbaarheid waarbij Denial of Service toegepast kan worden om privileges te krijgen over de host. De bijbehorende CVSS(Common Vulnerability Scoring System) score van deze vulnerability is 10.0. Een score van 10.0 is de hoogst mogelijke score, wat natuurlijk betekent dat van een groot risico te spreken is. Aangezien een DoS-aanval voor serieuze problemen kan zorgen, wordt deze kwetsbaarheid niet uitgebuit.

Testcase 05 gaat over het uitvoeren van een netwerkscan waarbij geprobeerd wordt om de OS van de host te achterhalen. Hieruit blijkt dat de OS van de host zeer waarschijnlijk NX-OS 6 gebruikt, een operating system van Cisco. Aangezien SNMP vooral gebruikt wordt door switches, routers en modems, sluit deze informatie goed aan op de resultaten van TC01. [CVE-2015-0718](https://www.cvedetails.com/cve-details.php?t=1&cve_id=cve-2015-0718) gaat wederom over een DoS-aanval, maar deze keer gericht op de NX-OS versies 4.0 tot 6.1, waar de OS van de geteste host dus ook onder valt.

## 2.3 Rapportering

Na de eerste twee stappen kunnen we de resultaten gaan analyseren. Onze risk rating wordt berekend met de formule:

Risico = dreiging \* kwetsbaarheid \* impact

In de onderstaande tabel wordt de risk rating nogmaal weergegeven. Hierin is visueel weergegeven hoe risico’s ingeschat worden. Hierbij staat groen voor een kleine dreiging met een lage impact, en rood voor een grote dreiging met een grote impact.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **RISICOTABEL** |  |  |  |  |  |
| **1. Bedreigingen** | **2. impact beschrijving** | **3. Impact niveau (1-5)** | **4. Kans (1-3)** | **5. Risiconiveau** | **6. Conclusie** |
| DDoS | Downtime van het systeem kan leiden tot financiële schade, reputatieschade, schade voor een klant en kosten voor incident handling | 5 | 1 | 5 | **Configureer de juiste firewall rules, creeër een verdedigings strategie, train een team en bespreek rollen, houdt software up-to-date, Vergroot de bandbreedte zodat de server voorbereid is om verkeerspieken op te vangen** |
| DoS | Downtime van het systeem kan leiden tot financiële schade, reputatieschade, schade voor een klant en kosten voor incident handling | 5 | 2 | 10 | **Update naar SNMPv3 indien dit nog niet is gedaan, configureer de juiste firewall rules.** |
| MitM | Reputatieschade door gebrek aan integriteit van verkeer | 3 | 1 | 3 | **Gebruik versleuteld verkeer door encryptie te gebruiken, maak gebruik van IPS om een MitM aanval te detecteren/blokkeren** |

Tabel 3: Risicotabel met de bevonden risico's

## Bewijslast: Business Continuity & Risk Mitigation

Business Continuity Management(BCM) is het maken van afspraken en het treffen van maatregelen met als doel de continuïteit van de werkzaamheden binnen een bedrijf te waarborgen. BCM is dus bedoeld om, in het geval van een incident, de effecten van dit incident te minimaliseren of, indien mogelijk, zelfs te voorkomen. Om goed in te kunnen schatten hoe groot de impact van een incident kan zijn, maakt men gebruik van Business impact analysis(BIA). Een BIA maakt onderscheid tussen verschillende risico’s op basis van de impact van een incident.

Risk mitigation is het voorbereiden en beperken van de effecten van een bedreiging. Er worden dus stappen genomen om de negatieve effecten van dreigingen te beperken.

### RTO en RPO

RTO, oftewel Recovery Time Objective is het streven om te voldoen aan een vooraf afgesproken hersteltijd na een incident. Een RTO van nul is natuurlijk niet haalbaar, maar een zo kort mogelijke hersteltijd is uiteraard wel het streven van ieder bedrijf. Om een RTO op te stellen moet bekend zijn hoelang het duurt om systemen opnieuw op te starten en wat de reactietijd van de IT-afdeling is. Natuurlijk geldt hierbij dat de RTO zo kort mogelijk hoort te zijn. Als het een week kost om weer volledig operationeel te zijn na een incident, loopt een bedrijf natuurlijk enorm veel geld mis, terwijl een kwartiertje te overzien is qua kosten.

Dat het systeem weer online is, betekent nog niet dat alle problemen verholpen zijn natuurlijk. Er is natuurlijk sprake van dataverlies als een systeem plotseling offline gaat. Om te voorkomen dat er teveel data en werk verloren gaat, wordt een Recovery Point Objective, oftewel RPO, afgesproken. Een RPO is het punt vanaf waar het systeem weer opgestart wordt na downtime. Een systeem wordt altijd vanaf een back-up weer opgestart, dus door zo vaak mogelijk back-ups te maken van een systeem, gaat zo min mogelijk werk verloren in het geval van een security-incident. Als de laatste back-up vijftien minuten geleden gemaakt is, raakt het bedrijf slechts vijftien minuten aan werk kwijt. Als de laatste back-up een uur geleden gemaakt is, kost het ineens een uur aan werk. Hoe meer werk er verloren gaat, hoe meer geld het kost.