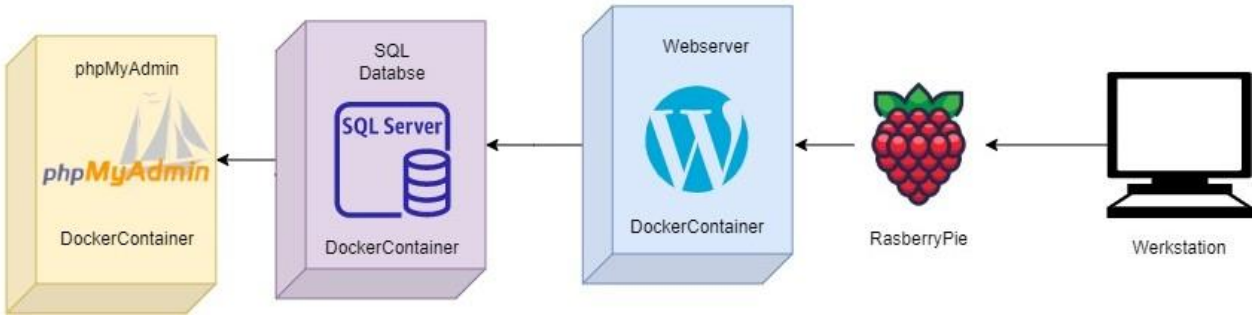
Risicoanalyse(Organisatie)

Inhoud Infra challenge

Voordat ik begin met de risicoanalyse beschrijf ik eerst mijn gehele project want dat is waar de risicoanalyse over zal gaan. Ik ga een phising website maken met daarin spyware de applicatie doet zich voor als een anti virus maar in de werkelijkheid scannend het je ip adres host name mac adres en interfaces. Vervolgens word deze informatie opgestuurd naar een database

Ontwerp



De sql server dient voor het opslaan van de webservers data. PhpMyAdmin zal ervoor zorgen dat ik makkelijk door de data kan snuffelen. Tot slot dient de raspberry pi voor het fysiek hosten en beheren van al deze docker containers. Het werkstation zal via rdp verbinding maken met de Pi.

Opmaak risicoanalyse

Omdat dit onderwerp het stelen en misbruiken van andermans data betreft zal ik het onderwerp ethiek behandelen. Daarnaast is het ook van belang om mijn idee te beschermen van mensen die wel kwade bedoelingen hebben. Ook zal ik laten zien wat voor schade aangericht kan worden wanneer de desbetreffende data in de handen van een cyber crimineel komt. Om in kaart te brengen wat de mogelijke risico's zijn aangaande het beheren van mijn project zal ik een biv matrix toepassen waarin ik de verschillende soorten maatregelen zal indelen op type risico. Vervolgens zal ik een top 10 maken van de zwaarste risico's en hier zal ik vervolgens maatregelen op verzinnen. Tot slot zal ik de risico's van het project ook blootstellen

Risico meter

Ethiek

Ethiek word volgens Van Dale gedefinieerd als "*het geheel van morele principes. Het woord 'moreel' wordt in het woordenboek genoemd als een bijvoeglijk naamwoord, gegrond op het innerlijk gevoel van goed en kwaad*." Omdat ethiek rust op een innerlijk gevoel wat bij de ene individu aanzienlijk anders kan zijn dan bij de andere. Kan ik niet conform de seculiere normen en waarde van onze huidige samenleving bewijzen wat goed en slecht is. Wat ik wel kan en ga doen is de ethische kwesties die indruisen op mijn project terug refereren aan de Nederlandse wet want het is deze wetgeving waaronder mijn project valt. Ongeacht mijn persoonlijke kijk hierop want die is irrelevant in de huidige situatie.

De phishing website

Op de website ejure (informatieportal voor IT-recht) staat "*Dan is er ook nog artikel 225 Sr, valsheid in geschrifte. Om mensen succesvol om de tuin te leiden zal de phisher immers mogelijk gebruik maken van vervalste certificaten, diploma's, of andere geschriften*." Artikel 225 is voldoende bewijs om aan te tonen dat alleen al de phising website verboden is en dus volgens de Nederlandse overheid onethisch

Het scannen van iemands computer gegevens

Bovendien staat op dezelfde website het volgende "***Als tweede is er het artikel over computervredebreuk, namelijk artikel 138ab Sr. Wanneer een phisher een computer zonder toestemming binnendringt kan hij op grond van artikel 138ab lid 1 Sr veroordeeld worden, of hij zich nu voordoet als de oorspronkelijke gebruiker, of door gebruik van malware zoals een trojan. Als de phisher na het binnendringen van de computer ook nog gegevens overneemt, aftapt, of opneemt, treedt de strafverzwarende omstandigheid van lid 2 ook in***" Dit laat zien dat ook het scannen van de ip adres en andere data gewoon niet toegestaan is.

Het blijkt dat mijn project vooral indruist op privacy omdat het eigenlijk spyware is. Maar wat is nu de reden van al die weten die privacy proberen te waarborgen? Volgens de website van de autoriteit persoonsgegevens zijn er 3 centralen punten.

Het volk – Uit onderzoek blijkt dat 94% van de mensen in Nederland zich zorgen maakt wat betreft de veiligheid van hun persoonsgegevens.

Belang van privacy – Privacy is een grondrecht die jou laat zijn wie je wilt zijn. Door privacy word je niet benadeeld door fouten die je in het verleden hebt gemaakt. Het zorgt ervoor dat men zich veilig voelt omdat je niet steeds in de gaten word gehouden. En dat je zeggenschap hebt over je persoons gegevens.

Risico's – Mensen kunnen last krijgen van identiteit' s fraude waar ze jaren last van hebben. Bedrijven krijgen data van mensen zonder dat die mensen dit weten waardoor die gebruikers niet oproep kunnen doen tot hun privacy rechten en dus een stukje autonomie verliezen.

Na het realiseren van de bovenstaande punten is het dus van groot belang dat mijn idee beschermde wordt

Impact	Kans		
	Hoog	Midden	Laag
Hoog	25	15	8
Midden	15	8	6
Laag	8	6	1

Risico's

Beschikbaarheid : Menselijke bedreigingen	Risico waarde
1. Plan word gestolen en misbruikt	25
2. Perongelijk data scannen van onschuldige slachtoffer	25

De reden dat deze risico's zo hoog zijn is omdat ze ethisch zoo onverantwoordelijk zijn, dat het gevolg het einde kan betekenen van iemands IT carrière in cybersecurity.

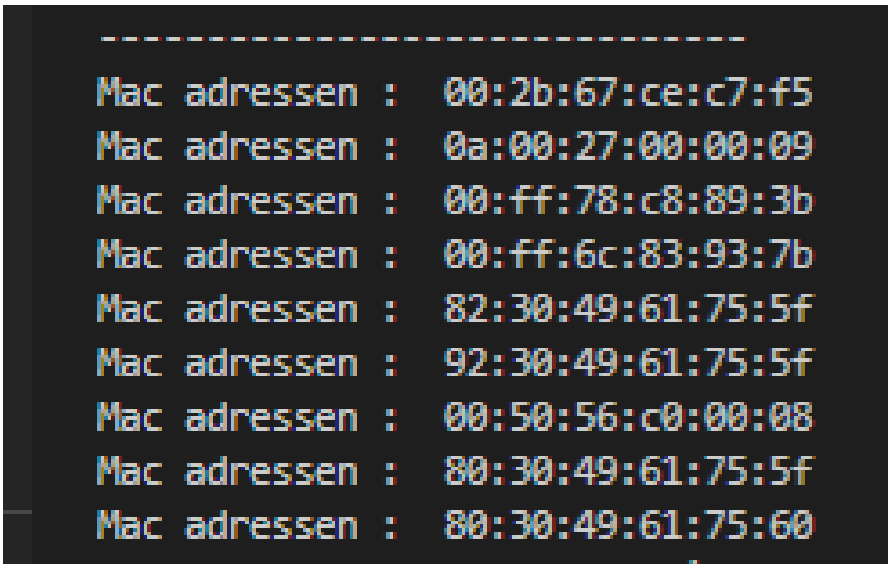
Maatregelen							
risico	maatregel	Repressies	preventief	Detectief	Corectief	Voor maatregelen	Na maatregelen
Plan word gestolen en misbruikt	1. Kritieke infomormatie niet delen. De gebruikte libraries in code dienen geheim te blijven. En de gebruikte bronnen tijdens het maken van de applicatie		1			-25	4
Perongelijk data stelen van onschuldigen	1.Database offline houden hierdoor kan de data die de app scanned niet doorgestuurd worden naar de werkmachine van de aanvaller 2. Geen poort open laten die data schrijft naar de locale database. 3. Malware website offline laten		1 t/m 3			-25	4

Aanvalsanalyse

In dit hoofdstuk zal ik uitwerken wat er allemaal gedaan kan worden met de gescande data

Mijn app scannend de volgende gegevens

```
145.93.141.21:58633
error :  <nil>
------------------------------
We want the interface name that has the current IP address
MUST NOT be binded to 127.0.0.1
------------------------------
[ 0 ] Ethernet > fe80::25fc:7f46:9364:b606/64
[ 1 ] Ethernet > 169.254.182.6/16
[ 0 ] OpenVPN Wintun > fe80::8448:7299:5049:e068/64
[ 1 ] OpenVPN Wintun > 169.254.224.104/16
[ 0 ] VirtualBox Host-Only Network > fe80::cc9f:e9a6:d363:e264/64
[ 1 ] VirtualBox Host-Only Network > 192.168.56.1/24
[ 0 ] Ethernet 3 > fe80::ed75:c41d:f3a1:ac15/64
[ 1 ] Ethernet 3 > 169.254.172.21/16
[ 0 ] OpenVPN TAP-Windows6 > fe80::a4a7:2b46:cbb6:9b97/64
[ 1 ] OpenVPN TAP-Windows6 > 169.254.155.151/16
[ 0 ] LAN-verbinding* 9 > fe80::94ee:fdd0:a13a:c156/64
[ 1 ] LAN-verbinding* 9 > 169.254.193.86/16
[ 0 ] LAN-verbinding* 10 > fe80::3868:db9:7c7b:d8f8/64
[ 1 ] LAN-verbinding* 10 > 169.254.216.248/16
[ 0 ] VMware Network Adapter VMnet8 > fe80::2548:8447:64ac:6b6f/64
[ 1 ] VMware Network Adapter VMnet8 > 192.168.234.1/24
[ 0 ] Wi-Fi > fe80::f4fa:8a3a:cf76:e6b2/64
[ 1 ] Wi-Fi > 145.93.141.21/21
[ 0 ] Bluetooth-netwerkverbinding > fe80::9d2a:9674:860c:b0fb/64
[ 1 ] Bluetooth-netwerkverbinding > 169.254.176.251/16
Use name :  Bluetooth-netwerkverbinding
[ 0 ] Loopback Pseudo-Interface 1 > ::1/128
[ 1 ] Loopback Pseudo-Interface 1 > 127.0.0.1/8
```



De bovenstaand lijst aan data bestaat uit drie delen.

1. **Ip adres**
2. **Mac adres**
3. **Netwerk interfaces**

Over de eerste twee onderwerpen zal ik duidelijke risico's geven.

Over het derde punt namelijk "Netwerk interfaces" ga ik niet directe risico's geven omdat de netwerk interfaces slechts een beter beeld geven van iemands netwerk. Hierdoor kunnen de kwetsbaarheden van de Ip adressen en mac adressen op meerdere plekken in het netwerk worden toegepast. De netwerk interfaces functioneren als een soort kaart die de hacker kan gebruiken om te navigeren over iemands netwerk en dus meerde apparaten op iemands netwerk aanvallen.

Beschikbaarheid : Technische bedreiginen

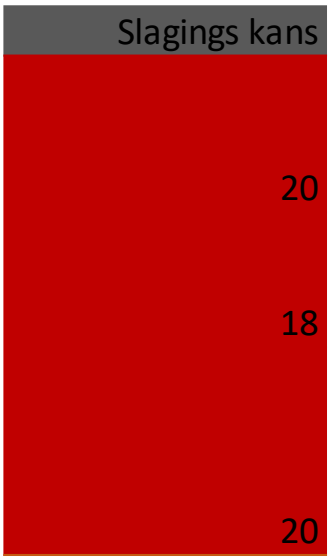
1. Ddos : Door iemands ip extreem vaak te pingen kan je het netwerk van de tegenstander uitschakkelen
2. Toegang tot services blokker d.m.v. IP addressen misbruiken.

Integriteit : Technische bedreigingen

1. Iemand erin luizen voor misdaaden: Een hacker kan op andermans IP bijvoorbeeld kinderporne downloaden zodat de politie vervolgens het slachtoffer de schuld geeft.

2. Copy right schendingen : Een hacker kan met de public ip van het slachtoffer bijvoorbeeld iligaal muziek en films - Downloaden waardoor copy right wetten worden geschend

Vertrouwbaarheid : Technische bedreigingen



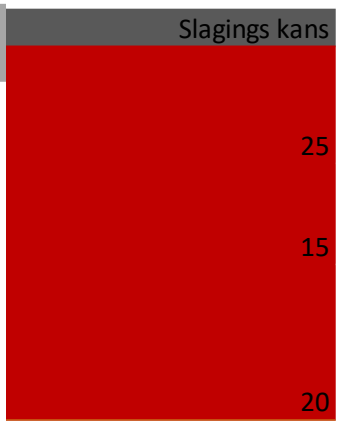
1. Publieke Ip van het slachtoffer word verkocht op het dark web.

2. ISP manipuleren : Wanneer een hacker de ip adres van het slachtoffer heeft bemachted kan de hacker vervolgens de desbetreffende ISP traceren en deze vervolgens misleiden d.m.v phising bijvoorbeeld. Hierdoor kan de hacke persoonlijke informatie zoals bank gegevns van de ISP extraheren

3. Locatie : Een hacker kan d.m.v jouw ip jouw locatie achterhalen.

Dit zijn de zaken die gedaan kunnen worden met iemands IP. Maar hoe laten we iemand daadwerkelijk ons antivirus downloaden?

Menselijke bedreigingen



1. IP grabber : Klikken op een onveilige link

2. Spyware downloaden

3. Social engineering : Een aanvaller kan werknemer op dusdanige wijze beinvloeden dat de Ip overzichtelijk word voor de aanvaller

Conclusie

Ict is een superkracht en dat zeg ik zonder een enkele twijfel in mijn lichaam. En in mijn challange komt dit naar voren. Ik heb namenlijk 6 maanden pas echt serieus gewerkt aan infra. En ik ben nu al instaat om een malware app te deployen op een phising website. Laatstaan wat iemand zou kunnen doen met 10 jaar ervaring in infra.

VIRUS OP UW COMPUTER GESCANNED !!

CLICK ONMIDDELIJK OP DE ONDERSTAANDE KNOPPEN EN DOWNLOAD DE ANTI VIRUS

Windows Linux

Dat doen we met een trojan horse om de mens te misleiden door het downloaden van onze malware. Toch is en blijft de mens de zwakste schakel in cybersecurity er moeten toch meer manierenzijn, om de IP adres van mensen te verwerven.

Riscoanalyse betreffende het product

Beschikbaarheid

Beschikbaarheid : Technische bedreiginen	Kans	Impact	Risico waarde
1. Docker (dataverlies)- Omdat docker een virtuele directory heeft verlies je al je data wanneer de container word gerestart	1. 4	4	16
2. Raspberry Pi stroom uitval- De pi die dus allen servers runt vereist stroom van de stopcontacten op school. Wanneer de pi dus van plek moet verhuizen zullen de servers voor een korte tijd neer zijn	2. 3	3	9
3. Verbinding verbroken - De pi is verbonden via de ethernet kabel met de router die gehost is inVmware op mijn laptop. Als er dus iets mis is met mijn laptop of Vmware of de kabel werken de servers niet meer	3. 3	3	9

Beschikbaarheid : Mensenlijke bedreiginen

	Kans	Impact	Risico waarde
1.	4	4	16
2.	4	4	16
3.	4	4	16

1. Simpele wachtwoord voor Wordpress gebruiken.
2. Simpele wachtwoord voor Raspberry pi gebruiken.
3. Vekeerde configuratie van docker compose- Een methode om docker containers te creeren en aan elkaar te verbinden is docker compose wanneer een fout in de configuratie is kunnen allen services neergaan

Integriteit : Technische bedreigingen	Kans	Impact	Risico waarde
1. Onveldoende update van Pi : Dit kan leiden tot ongewenste indringing van een cybercrimineel	4	4	16
	5	5	25
2. Zorg ervoor dat sudo een wachtwoord vereist. -Sudo is de root gebruiker in linux.	4	2	8
3. Kernal exploitatie - De kernal van allen docker containers worden gedeeld met de host. Dus wanneer een aanvaller een docker container heeft aangetast kan diezelfde hacker de host kernel aanvallen	3	4	12
4. Geen HTTPS certificaat toepassen bij de phpmyadmin login pagina	5	5	25
5. Remote desktope service weinig security patches. - Sinds het begin van rdp zijn er veel kwetbaarheden gevonden echter worden deze kwetbaarheden naulijks ge-patched			

Integriteit : Menselijke bedreigingen

	Kans	Impact	Risico waarde
1.	2	10	20
2.	2	8	16

1. Downloaden van onvelige image's - Om een docker container te gebruiker moet eerst de image van die container gedown-load worden vanuit het internet. Het kan dus zo zijn dat de image malware bevat

2. Pi user gebruiken - Pi user is de standaard gebruiker die bij pi os word mee geinstaleerd het is dus een doelwit voor bruut force hacking

Veiligheid : Technische bedreigingen

	Kans	Impact	Risico waarde
1.	3	5	15
2.	5	2	10
3.	4	4	16
3.	4	3	15

1. Phplogin url is door hacker makkelijk te vinden.

2. Zichtbare root login Phpmyadmin

3. SQL installatie test producten bewaren.
Tijdens het installeren installeert mysql dummy accounts en database's. De aanwezigheid van deze accounts kan al een mogelijke ingangs-punt zijn voor hackers.

4. Pi staat direct verbonden aan het in -ternet

Veiligheid : Menselijke bedreigingen

	Kans	Impact	Risico waarde
1.	4	4	16
2.	5	3	15
3.	4	3	12

1. Wordpress open login - Door slechts /wp-admin te typen kan een aanvaller al de de gebruiksnaam en ww invullen voor de admin rechten van de site
2. Computer die is aan blijven staan word aangetast

3. Te wenig toegangs regels - De verantw-oordelijke voor de Wordpress website kan Ook in de sql server komen

Maatregelen tegen de zwaarste bedreigingen

Maatregelen							
risico	maatregel	Repressies	preventief	Detectief	Corectief	Voor maatregelen	Na maatregelen
Docker dataverlies	1.Docker-volumes	1			1	-16	1
Verkeerde configuratie docker compose	1.Image maken 2.Image uploaden naar docker hub	1 t/m 2			1 t/m 2	-16	1
Simpele wachtwoorden gebruiken	1. Zinnen gebruiken als wachtwoorden inplaats van woorden 2. Wachtwoorden op papier op schrijven en veilig bewaren	2	1 t/m 2		2	-25	4
Onveldoende update van PI	1.Automatische upate installeren op de pi. 2. Handmatig updaten		1 t/m 2			-16	4
Pi staat direct verbonden aan het internet.	1. Pfsense router voor de pi zetten. Dit zal dienen als een extra firewall.		1			-15	4
Kwetbaarheden in remote desktop	1. Open Vpn gebruiken 2. Vscosity Vpn gebruiken		1 t/m 2			-16	4
Pi user gebruiken	1. Pi user verwijderen eigen gebruiker toevoegen		1			16	2
Sql test producten bewaren	1. Allen test producten verwijderen en eigen producten toevoegen		1			-16	4
Phplogin url is door hackers makkelijk te vinde	1.Veranderen van default url		1			-16	4
Wordpress login url beschermen	1.Url aanpassebn		1			-16	4