

Labo Chapter 1: Security General



Team nummer: 1TINh_2	Teamleden: 1. Aleyna Arslan 2. Stef Swinnen 3. Rasmus Leseberg 4. Tomas Soors
------------------------------------	--

Team nummer: 1TINh_2	Teamleden: 1. Aleyna Arslan 2. Stef Swinnen 3. Rasmus Leseberg 4. Tomas Soors
------------------------------------	--

Teamleden:

- ### Teamleden:

Inhoudsopgave Labo Chapter 1

Inhoudsopgave

1. Terminologie & Jargon	4
2. Cybersecurity	6
3. Analyseer jezelf	9
4. The Security Cube.....	14
4.1 Casus	14
4.2 Security goals	15
5. Password & password policy	27
5.2 Herhalingsvariatie en een paswoord.....	28
5.2.1 Bijhorende vragen.....	28
5.3 Passwordmanager + vragen.....	29
5.4 2FA	29
5.5 Wachtwoord policy	30
5.6 Conclusie	30
6. Data with a hash	31
7. Backup.....	33
8. Countermeasures technology	36
9. THM - Searching the internet.....	38
10. OSINT Lodrimed	41
11 THM - Principles of Security	45

Tijdsbesteding Labo Chapter 1

	Tomas	Stef	Aleyna	Rasmus	TOTAAL
Deelopdracht	Opdracht 1 Opdracht 5.4 Opdracht 9	Opdracht 4.1 Opdracht 5.3.1 Opdracht 10	Opdracht 2 Opdracht 5.3 Opdracht 5.5 Opdracht 5.6 Opdracht 7 Opdracht 4.2	Opdracht 6 Opdracht 5.2 Opdracht 5.6 Opdracht 8 Opdracht 11 Opdracht 4.2	
Inschatting	3 uur	3 uur	8 uur	6 uur	12
Gezamenlijke taken *	Opdracht 3 Opdracht 5.1 Opdracht 5.1.1	Opdracht 3 Opdracht 5.1 Opdracht 5.1.1	Opdracht 3 Opdracht 5.1 Opdracht 5.1.1 Verantwoordelijk voor controle & opmaak	Opdracht 3 Opdracht 5.1 Opdracht 5.1.1 Verantwoordelijk voor controle	
TOTAAL	8 uur	9 uur	25 uur	15 uur	

1. Terminologie & Jargon

Opdracht gemaakt door: Tomas

Exploit: volledig gebruik maken van de gegeven hulpbronnen en dergelijke.

Attack: een aanval op een netwerk of een database.

Countermeasure: de tegenmaatregelen die genomen worden tegen aanvallen, om de veiligheid van de informatie en bestanden te verzekeren.

Risk: de kans van blootstelling of verliezen als resultaat van een cyber aanval op de organisatie.

Gap analysis: het proces dat bedrijven gebruiken om de huidige performance te vergelijken met de gewilde performance van de netwerken of dergelijke.

Threat: de verschillende aanvallen met malicieuze bedoelingen die op een onwettige manier probeert toegang te krijgen tot gegevens, digitale operaties probeert te verstoren of informatie probeert te bemachtigen.

Vulnerability: interne controles of implementatie die kan worden misbruikt of geactiveerd door een persoon met slechte bedoelingen.

Interception(threat): waarbij een niet-geautoriseerd persoon toegang krijgt tot privé of confidential informatie.

Interruption(threat): waarbij een bepaalde service op het netwerk van het bedrijf, wordt belemmerd of volledig onbruikbaar gemaakt voor echte gebruikers van deze service.

Modification(threat): een niet geautoriseerde gebruiker die niet alleen toegang krijgt tot de data van een bedrijf, maar deze ook gaat aanpassen, bijvoorbeeld de data transfer dwarsbomen.

Cybersecurity: de staat van beveiliging tegen strafbaar of ongeoorloofd gebruik van elektronische gegevens, met de maatregelen die worden genomen om dit te bereiken

Breaches: eender welke binnenvall in het netwerk, waarbij iemand niet- geautoriseerd toegang krijgt tot data, software, computers, of eender welk toestel dat zich in het netwerk bevindt.

Weaknesses: een bepaalde positie waar het netwerk of de computer kwetsbaar is waar bepaalde mensen misbruik van kunnen maken.

Malicious: iets dat bedoeld is om schade aan te richten, of wraak nemen op een bepaalde persoon of groep van personen.

Malware: is een bestand of code, geleverd over een netwerk, die bepaalde netwerken of computers kan infecteren, verkennen of technisch gezien wat dan ook kan doen naar de wil van de aanvaller.

Hacker: iemand die toegang probeert te krijgen tot de gegevens van iemand anders, via het gebruik van computers en een netwerk, en als dit op illegale wijze wordt gedaan is dit strafbaar.

WHH: ook wel ethical hacker genoemd, is iemand die op bedrijfsniveau wordt ingeschakeld om kwetsbaarheden te vinden in een systeem, en gaan volledig legaal te werk.

BHH: iemand die met malicieuze intenties op pad gaat om netwerken en computers binnen te dringen en deze informatie te vergaren. En dit wordt altijd gedaan op illegale wijze zonder toestemming van de eigenaars van het netwerk of de computer

GHH: iemand die beide black en white hat activiteiten uitvoert, ze zoeken meestal naar kwetsbaarheden in het systeem zonder dat de eigenaar van het bedrijf dit doorheeft. Dit is meestal op illegaal niveau, maar niet met slechte bedoelingen.

Cybercrime as a service: Is een platform waar mensen zoals hackers of malware developers, hun services en programma's aanbieden als een service voor developers of mensen op de dark web.

Script kiddie: is een persoon die op zoek gaat naar bepaalde scripts of webshells of andere dingen om bepaalde toepassingen uit te voeren zoals een andere computer hacken. Zonder dat ze de expertise hebben om zelf een script te schrijven.

Hacktivists: een persoon die op basis van computer gerelateerde services of via het internet protest gaat voeren. Door bepaalde informaticasystemen aan te vallen om deze buiten werking te stellen/

Cyber criminals: een individueel of teamverband dat technologie gaat gebruiken om malicieuze activiteiten of illegale activiteiten uit te voeren om bijvoorbeeld menselijke kwetsbaarheden te misbruiken om data te stelen.

Ethical hacking: is een door het bedrijf geautoriseerde methode om de mogelijke datalekken en bedreigingen in een netwerk te identificeren op basis van het omzeilen van de systeembeveiliging of dergelijke.

Zero-Day: is een kwetsbaarheid in de software of netwerk, waar de softwareontwikkelaars of netwerkbeheerders zelf nog niet van af weten, of pas zijn achter gekomen.

Confidentiality: waarbij de data, informatie of bronnen beveiligd zijn van niet-geautoriseerde toegang of het bekijken van deze bronnen door niet geautoriseerd personen.

VPN: Virtual Private Network, is een geëncrypteerde connectie van een toestel naar een netwerk over het internet. Deze connectie helpt het verzekeren dat gevoelige data veilig gestuurd of overgedragen wordt

Firewall: een beveiliging op netwerk vlak om verkeer over het internet vanbinnen, buiten tegen te houden, of zelfs in een privé netwerk zelf, met de bedoeling om binnen of buiten verkeer te stoppen tot het gebruik van slechte bedoelingen.

CERT: Computer Emergency Response Team, is een groep van experts op vlak van online security, die verantwoordelijk zijn voor het beschermen en te detecteren op incidenten op cybersecurity, om hier dan op de juiste manier op te reageren.

CSIRT: Computer Security Incident Response Team, met als hoofdzakelijke doelstelling om bepaalde cyber aanvallen aan te tonen en deze aan te pakken op de beste en meest efficiënte manier.

2. Cybersecurity

Opdracht gemaakt door: Aleyna

2.1) Oekraïne getroffen door cyberaanval: sites ministerie en banken offline = Emi Van de Ven, E. V. V. (2022, 16 februari). Oekraïne getroffen door cyberaanval: sites ministerie en banken offline. VPN Gids.

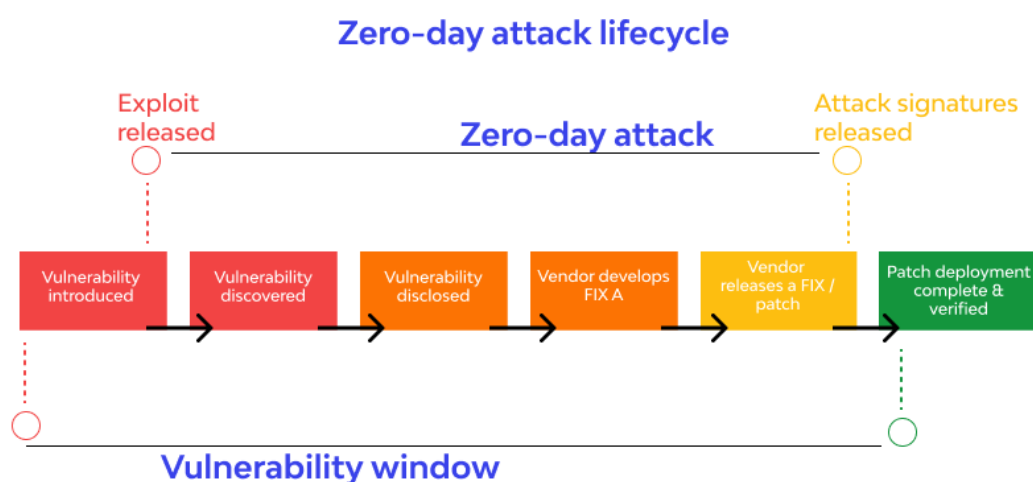
<https://www.vpngids.nl/nieuws/oekraïne-getroffen-door-cyberaanval-sites-ministerie-en-banken-offline/>

- **Omschrijving:** Door een cyberattack dat plaatsvond in Oekraïne zijn er 2 banken en het ministerie van Defensie getroffen. Door de overbelasting van het netwerk waren de websites van deze instanties offline. Deze cyberattack vond plaats via een DDoS-attack, bij dit soort aanvallen worden websites overrompeld met bezoekers die voornamelijk afkomstig zijn van botnets. Waar de aanval vandaan komt is nog niet bekend, maar de Oekraïense autoriteiten vermoeden dat Rusland hierachter zit.
- **Incident date:** 15 februari 2022
- **Affected organization:** 2 Oekraïense banken en het ministerie van Defensie
- **Who is the victim + how many victims:** Eindgebruikers die gebruik willen maken van de diensten van het ministerie van Defensie, en de banken.
- **What was taken? What was the motive:** Er is niets gestolen. De aanval vond plaats om enkel en alleen chaos en destabilisatie te veroorzaken.
- **What exploits were used:** Geen
- **Describe the vulnerability:** Geen of slechte anti-DDoS mitigation. Een DDoS-attack kan ook plaatsvinden omdat er geen voorbereiding is op een aanval. Door securitysoftware te installeren of door gebruik te maken van de security alerts die verzonden worden via de hostingprovider, kunnen organisaties op de hoogte worden gesteld wanneer er een aanval plaatsvindt, op deze manier kan de organisatie of de hostingprovider actie ondernemen om de sites te beschermen tegen de aanval.
- **How do you protect yourself:** Het is in principe onmogelijk voor een organisatie om zich volledig te beschermen tegen DDoS-aanvallen, hoe goed de hostingprovider ook is. Wat een goede hostingprovider wel doet, is zorgen voor een goede firewall, die de kans op een aanval verkleint, maar niet helemaal uitschakelt. Ze bieden ook tools die kunnen worden gebruikt om een DDoS-aanval te stoppen nadat deze is gestart, zoals IP-blokkering. Om uw organisatie beter te beschermen tegen DDoS-aanvallen, moet u een uitgebreid netwerk gebruiken dat de intelligentiedatabase van aanvallen op andere sites over de hele wereld kan gebruiken om aanvallen te voorspellen en zoals eerder vermeld de IP's waarvan ze afkomstig zijn, te blokkeren.

2.2) 1200 kwetsbare servers in Nederland door zeroday exploits in MS Exchange = Anton Mous, A. M. (2021, 17 maart). 1200 kwetsbare servers in Nederland door zeroday exploits in Microsoft Exchange. VPN Gids.

<https://www.vpngids.nl/nieuws/1200-kwetsbare-servers-in-nederland-door-zeroday-exploits-in-microsoft-exchange/>

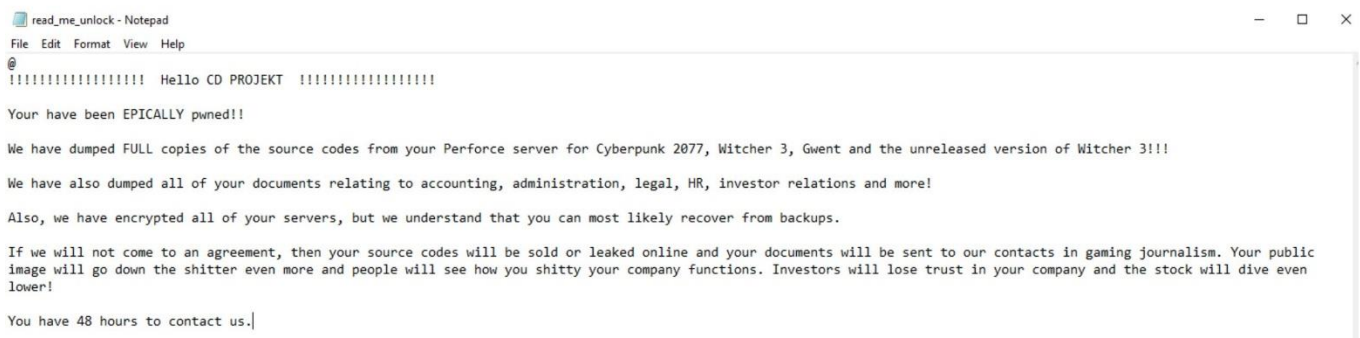
- **Omschrijving:** Microsoft Exchange servers bevatte 4 zeroday exploits. Een heleboel bedrijven in Europa, Azië en de VS hebben geleden door de vulnerabilities van MS Exchange. Een van de getroffen is European Banking Authority (EBA), via deze exploits hebben hackers de e-mailserver van het bedrijf geïnfecterd en hebben persoonlijke- en bedrijfsgevoelige informatie gestolen. In Nederland hadden 90 procent van de bedrijven een patch voor MS Exchange al geïnstalleerd, waardoor er op minimaal 1200 servers de update nog niet is uitgevoerd.
- **Incident date:** 3 januari 2021
- **Affected organization:** Microsoft
- **Who is the victim + how many victims:** Eindgebruikers en bedrijven die gebruik maken van Microsoft Exchange.
- **What was taken? What was the motive:** Gebruikt om gefraudeerde mails te versturen om zo gevoelige bedrijfsgegevens te verzamelen.
- **What exploits were used:** Zeroday exploits
- **Describe the vulnerability:** CVE-2021-26855. Het eerste doelwit in deze aanvalsketen is de Exchange On-premise-server, die niet-vertrouwde verbindingen van externe bronnen kan ontvangen. Bovendien moet op de Exchange-server Microsoft Exchange Server 2013, 2016 of 2019 worden uitgevoerd.
- **How do you protect yourself:** De enige oplossing die toepasbaar is op dit voorbeeld, zijn software updates en vooral security patches te installeren.



Figuur 1: Zero-day Attack Lifecycle

2.3) CD PROJEKT slachtoffer van gijzelsoftware = Anton Mous, A. M. (2021, februari 9). CD PROJEKT slachtoffer van gijzelsoftware. VPN Gids. <https://www.vpngids.nl/nieuws/cd-project-slachtoffer-van-gijzelsoftware/>

- **Omschrijving:** een hacker wist toegang te krijgen tot het interne netwerk van CD PROJEKT Capital Group, waar hij vertrouwelijke informatie stal en in ruil om losgeld vroeg. Een aantal apparaten binnen het netwerk van CD PROJEKT werd hierdoor versleuteld met ransomware, maar het bedrijf in kwestie weigerde te onderhandelen met hackers. De gamestudio gaf aan dat alle back-ups nog intact waren en zijn begonnen met het herstellen van het netwerk en data.



```
read_me_unlock - Notepad
File Edit Format View Help
@
!!!!!!!!!!!!!!!!!!!! Hello CD PROJEKT !!!!!!!!!!!!!!!!!!!!!
Your have been EPICALLY pwneD!!
We have dumped FULL copies of the source codes from your Perforce server for Cyberpunk 2077, Witcher 3, Gwent and the unreleased version of Witcher 3!!!
We have also dumped all of your documents relating to accounting, administration, legal, HR, investor relations and more!
Also, we have encrypted all of your servers, but we understand that you can most likely recover from backups.
If we will not come to an agreement, then your source codes will be sold or leaked online and your documents will be sent to our contacts in gaming journalism. Your public
image will go down the shitter even more and people will see how you shitty your company functions. Investors will lose trust in your company and the stock will dive even
lower!
You have 48 hours to contact us. |
```

- **Incident date:** 8 februari 2021
- **Affected organization:** CD PROJEKT Capital Group
- **Who is the victim + how many victims:** De eigenaars (Marcin Iwiński en Michał Kiciński) van het bedrijf CD PROJEKT Capital Group
- **What was taken? What was the motive:** De cyber criminelen dreigen om de broncode van bekende games zoals Cyberpunk 2077, Witcher 3, Gwent en de unreleased versie van Witcher 3 te leaken of te verkopen aan de concurrent. Ook hebben ze documenten gerelateerd aan boekhouding, administratie, HR, relaties met investeerders in hun bezit.
- **What exploits were used:** Geen
- **Describe the vulnerability:** Het maakt niet uit hoe goed je netwerk is beveiligd, als een van de medewerkers binnen het bedrijf in een phishing mailtje trapt, kunnen criminelen alsnog toegang krijgen tot het bedrijfsnetwerk, wat in dit voorbeeld waarschijnlijk het geval was.
- **How do you protect yourself:** Om dit soort attacks te voorkomen is het verstandig om regelmatig software updates uit te voeren, bij dit soort aanvallen zijn meestal grote bedrijven het doelwit, dus het personeel moet extra op hun hoede zijn tegen phishing mails en scams. Het installeren van antivirus- of antiransomsoftware kan ook helpen en wat je zeker niet moet vergeten is het online- en offline back-uppen van essentiële/gevoelige data.

3. Analyseer jezelf

Opdracht gemaakt door: Aleyna, Stef, Tomas en Rasmus

- **Aleyna Arslan:**

Hoe ben ik in aanmerking gekomen met cybersecurity?

Een 6-tal jaar geleden ben ik in aanmerking gekomen met cybersecurity toen ik online aan het gamen was. Iemand had mij een link gestuurd dat mij doorverwees naar Twitter, maar een IP-logger bleek te zijn. Hier was ik toen uiteraard niet van op de hoogte tot dat hij begon te dreigen met een DDos attack. Ik had uit schrik mijn computer afgesloten en hoopte dat er niks zou gebeuren, wat ook het geval was. Het bleef enkel bij gebluf. Hierna ben ik voorzichtiger omgegaan met dit soort situaties, en heb ik niet meer op onbetrouwbare links geklikt.

HaveIBeenPwnd?

Mijn persoonlijk e-mailadres is terug te vinden in de breach van Canva. Het bedrijf heeft mij hier niet van op de hoogte gesteld. Mijn wachtwoorden zijn opgeslagen in een Password Manager, daar heb ik een waarschuwing van gekregen dat Canva een datalek had en dat mijn wachtwoord veranderd zou moeten worden. Voor dat ik hiervan wist, was er ook al op mijn Canva account ingelogd en was mijn wachtwoord gewijzigd maar mijn e-mailadres was nog altijd hetzelfde, zo heb ik zelf mijn wachtwoord nog kunnen resetten.

Password policy:

Ik probeer voor elke website een ander wachtwoord te gebruiken, dit doe ik door een automatisch wachtwoord te genereren die voldoet aan de password policy, zo ben ik zeker dat mijn wachtwoord niet makkelijk te raden is. Moest het zijn dat ik in het verleden een makkelijk wachtwoord heb gebruikt of mijn wachtwoord in een dataleak zit, dan word ik hiervan op de hoogte gebracht via mijn Password Manager en pas ik het wachtwoord aan. Op platformen waar ik veel persoonlijke informatie op heb staan, zoals iCloud en mijn mailaccounts verander ik mijn wachtwoorden regelmatig.

5 tips aan studenten over cybersecurity:

Als student is het belangrijk dat we onze gevoelige informatie niet zomaar verspreiden. Het is belangrijk dat je controle voert over alles wat tegen je gebruikt kan worden door een partij dat slechte bedoelingen heeft. Onder studenten is het gebruik van sociale media enorm populair, daarom lijkt het me verstandig om je accounts te beveiligen met complexe wachtwoorden die cijfers, letters en speciale tekens bevatten. Daarnaast is het ook van belang dat je 2FA gebruikt voor mocht iemand je wachtwoord toch raden, niet door 2FA geraakt. Op deze manier word je ook op de hoogte gesteld dat er iemand een inlogpoging probeerde te doen op je account en kun je die verder beveiligen. Houd je gegevens ook regelmatig up to date door een back-up te maken van je smartphone of je laptop, moest er iets gebeuren waardoor je je gegevens verliest, kun je ze altijd recoveren. Als we iets downloaden via de App Store dan doen we dat meestal zonder de terms & conditions te lezen. Op het eerste gezicht lijkt dit onschuldig, maar er kan ook meer achter zitten, zoals toegang vragen tot je microfoon en camera, terwijl dit vaak niet nodig is.

Gevolgen voor slechte omgang met cybersecurity:

Onjuiste cybersecurity kan ernstige gevolgen hebben. Denk aan een bedrijf dat zeer succesvol is. Als ze het doelwit zijn van een cyberaanval, kan het een grote kost zijn om de schade te herstellen, maar dat is niet het enige. Het verliest op deze manier ook klanten en veroorzaakt uiteindelijk financiële schade. Sommige van deze bedrijven bewaren gevoelige klantgegevens, als die gegevens worden misbruikt, is het bedrijf in kwestie niet voldoende beschermd tegen cyberaanvallen met als gevolg hoge boetes en strenge wetgeving



Figuur 2: Five Reasons Why Cybersecurity is Important for Businesses

Je kunt dit voorkomen door het personeel goed op te leiden. Want dit is hoe cyber criminelen de kluis openkraken. Het personeel moet verstandig omgaan met onlineverkeer, denk aan e-mails. We ontvangen dagelijks honderden mails wat op het eerste gezicht onschuldig blijken te zijn. Er moet maar een iemand zijn die erin trapt, door op een link te klikken die toegang verleent aan de cyber criminelen om zich op het netwerk aan te sluiten en zo gevoelige informatie te stelen, of het systeem te corrupten. Wat ook belangrijk is dat je je software en systeem regelmatig up to date houdt, zodat de bugs die erin zitten, gefixed zijn en minder kans is op vulnerabilities. Een firewall is een van de efficiëntste manieren om het netwerk te beveiligen en uiteraard is het ook belangrijk om data die bedrijven beschikken te back-upen voor als er toch een cyberattack plaatsvindt, er zo weinig mogelijk downtime of dataverlies is. Het WiFi-netwerk beveiligen is een van de belangrijkste dingen die je voor je bedrijf kunt doen. Wat als er een device verbinding heeft gemaakt met een netwerk dat geïnfecteerd is? Als dit device vervolgens verbinding maakt met het netwerk van het bedrijf, loopt het systeem een ernstig risico.

- **Stef Swinnen:**

Hoe ben ik in aanmerking gekomen met cybersecurity?

Dit semester is voor mij de eerste keer dat ik iets bijleer over cybersecurity. Wel heb ik al regelmatig phishing mails gehad waar ik niet op ben ingegaan. Hetzelfde met berichten of telefoontjes. Tot nu toe vind ik het heel interessant en ik ben gedreven om er meer over te leren in dit vak.

Ik probeer op elk account dat ik maak een ander wachtwoord te verzinnen, zo blijft alles van elkaar gescheiden en kan iemand niet zomaar op aanmelden met mijn gegevens.

HaveIBeenPwnd?

Zowel mijn gsm-nummer als persoonlijke e-mail zijn nog niet gepwned. Ik probeer daarom overal andere wachtwoorden voor te verzinnen. Voor mijn pincodes probeer ik om de zoveel tijd ook eens voor verandering te zorgen, dan blijft alles zeker veilig.

5 tips aan studenten over cybersecurity:

- Je wachtwoorden opslaan in een passwordmanager
- Zo weinig mogelijk op onbeveiligde wifi-netwerken inloggen
- Open geen mails of berichten die je niet vertrouwd
- Scan je apparaten regelmatig op virussen
- Gebruik multi-factor authenticatie bij het aanmelden

Gevolgen voor slechte omgang met cybersecurity:

Voor jezelf kan het heel vervelend zijn om gehacked te worden, je kan vaak niet meer op je account inloggen en er kunnen op bijvoorbeeld sociale media berichten worden geplaatst die je niet wil. Op ander soort accounts zoals de bank kan er geld van je rekening verdwijnen en nog veel meer. Voor bedrijven kan het leiden tot dataleaks, fouten in de software en nog veel meer. Het is dus belangrijk dat je jezelf goed beveiligt tegen cyberaanvallen om dit allemaal te voorkomen. Je kan er best voor zorgen dat alle apps op je computer goed beveiligt zijn met paswoorden, dit kan je nog versterken door multifactor authenticatie. Het is ook aangeraden om te bepalen wie er wel of geen toegang heeft tot je data, dit kan je bijvoorbeeld op sociale media instellen. Natuurlijk is het belangrijk om je software up to date te houden en backups te nemen

- **Rasmus Leseberg:**

Ik neem cybersecurity persoonlijk voor mezelf vrij serieus, en probeer voor elke account die ik online heb een ander wachtwoord te bedenken, waarvan de complexiteit redelijk hoog is. Password Managers vertrouw ik tot nu toe niet helemaal, dus maak ik er momenteel geen gebruik van, dus schrijf liever mijn paswoorden op en bewaar ze in een zekere locatie thuis, en bewaar geen kopie daarvan op mijn laptop. Misschien zal mijn mening over passwordmanagers aan de hand van dit vak veranderen. Ik verander mijn paswoorden minimaal 1x per jaar, en ik denk dat ik vanaf nu (aanhoud van wat ik al geleerd heb van dit eerste hoofdstuk) password generators ga gebruiken.

Ik ontvang vaker wel phishing attempts via SMS of email. In Denemarken, België en Nederland waren dat het vaakst tot nu toe pogingen om mijn digitale identificatie (ItsMe, ...) te krijgen. In Denemarken trapte ik een keer erin, omdat ik niet wist dat de overheid geen update-informatie via SMS verstuurde over 'Nem-ID' (ItsMe voor Denen). Dat heeft toen 2 weken geduurd om voor mij een nieuwe digitale ID aan te vragen, en te ontvangen.

HavelbeenPwned?

Mijn gsm-nummer en persoonlijke email niet (protonmail), mijn gmail komt 1x voor in 1 data breach bij Lumin PDF wat toen in april 2019 een data breach had. Ik werd toen niet op de hoogte gesteld, maar ik heb geen account meer bij die service.

Top 5 tips aan medestudenten over cybersecurity:

- Maak voor elke account online/offline een ander password aan
- Gebruik meerdere emailadressen voor verschillende accounts
- Gebruik een VPN wanneer mogelijk
- Zorg dat alle wachtwoorden redelijk complex zijn
- Geef nooit persoonlijke informatie verder aan onbekende mensen online, en pas op voor pogingen tot phishing.

Gevolgen voor slechte omgang met cybersecurity:

- 1. Voor mezelf:** Verlies van data, afpersing, identiteitsdiefstal
- 2. Bedrijven:** Afpersing, tijdelijke shut-down, verlies van data, enorme kosten
- 3. Maatschappij:** Black-outs, geen water/energie, verlies van data, levensgevaar voor sommigen (ziekenhuizen), enorme kosten.

Maatregelen die ik zou kunnen nemen: IPS/IDS/Antivirus/VPN/Firewalls goed gebruiken, een goede password policy implementeren, nooit dingen downloaden/openen die ik niet vertrouw

Maatregelen die bedrijven zouden kunnen nemen: Goede IT specialisten inhuren, afhankelijk van grootte bedrijf ook een cyber security task force aanmaken met mensen die verstand hebben. Ook moeten bedrijven in cybersecurity investeren.

Maatregelen die de maatschappij zou kunnen nemen: De nieuwe en huidige generaties opleiden over cyber security, of op scholen, hogescholen, universiteiten, of met cursussen. IT-specialisten inhuren voor het beheren van belangrijke digitale infrastructuur, voorbereid zijn op cyberwarfare door middel van IT afdelingen van het militair.

- **Tomas Soors:**

Eerste ontmoeting met cybersecurity

Ik ben zelf al een paar keer in contact gekomen met phishing of smishing. Maar ik ben er zelf nooit echt in getrapt, mijn familieleden daarentegen zijn er zelf al een paar keer in getrapt. Zoals een fake trojaans paard dat men wou verwijderen voor een bepaald bedrag, wat uiteindelijk niet waar bleek te zijn. Maar mensen komen wel vaker naar mij toe om te vragen of iets echt is of niet. En ik denk dat dit mij wel een duwtje in deze richting heeft gegeven. Want ik ben zelf heel erg geïnteresseerd in cybersecurity. En wil hier graag over bijleren om zelf uiteindelijk in deze sector te kunnen werken.

HaveIBeenPwnd?

Beide mijn persoonlijke email, en mijn gsm-nummer zijn alle twee niet gepwned. Daarentegen zijn al mijn andere email adressen en dergelijke ook niet gepwned. Als het op mijn wachtwoorden en pincodes aankomt ben ik misschien niet echt de meest creatieve persoon op de wereld, maar ik heb wel veel aparte, maar tegelijkertijd gelijkaardige wachtwoorden, mijn pincodes daarentegen is misschien niet echt verschillend. Maar hier probeer ik zelf verandering in te brengen. Ik probeer mijn familieleden ook vaker aan te raden om verschillende wachtwoorden te gebruiken voor hun email en hun andere profielen, en zij volgen mijn advies wel op. Ik maak zelf geen gebruik van een passwordmanager, omdat ik niet zo immens veel verschillende wachtwoorden heb, maar ik zou deze misschien wel willen beginnen gebruiken om mijn veiligheid te vergroten online

5 tips aan medestudenten over cybersecurity:

Voor iedereen die het internet gebruikt is het belangrijk om je veiligheid te vergroten. Want je kan nooit weten wie of wat er om de hoek licht te loeren om misbruik te maken van je informatie.

De belangrijkste tips die ik zou kunnen geven voor mijn medestudent, of wie dan ook is:

- Het gebruik maken van verschillende wachtwoorden op elke mogelijk inlogmogelijkheid.
- Een passwordmanager gebruiken om deze wachtwoorden in op te slaan.
- Een goed antivirus downloaden, of anti-malware software (ik gebruik persoonlijk malwarebytes als antivirus of antimalware software)
- Bij het aanmelden op een publiek netwerk, altijd proberen gebruik te maken van een VPN.
- Regelmatig een back up maken van de verschillende documenten op je systemen.

Gevolgen voor slechte omgang met cybersecurity:

Je veiligheid is nooit gegarandeerd, je eigen verstand is ook een grote factor bij je veiligheid online. Dus wees altijd op je hoede, en als je iets niet zeker weet, vraag om hulp bij iemand die je vertrouwt, en er misschien meer verstand van heeft dan jij zelf. Als je zelf deze maatregelen niet goed neemt, is je risico op een breach of dergelijke vele malen groter. Als de veiligheid van jouw informatie of die van het bedrijf wordt aangepast, gestolen of dergelijke, kan dit zeer grote gevolgen op jou en het bedrijf zelf, dit kan de reputatie van jou op de proef stellen, en de gevoelige informatie van het bedrijf kan misbruikt worden om het bedrijf zelf in de grond te boren. De veiligheid van het systeem is 1 ding, maar zoals ik al eerder heb vermeld, de manier waarmee je omgaat met deze informatie is ook van groot belang, dus je attentie en alertheid is zeker zo belangrijk als de cyber security van het netwerk.

4. The Security Cube

Opdracht gemaakt door: Stef, Aleyna, Rasmus

4.1 Casus

Dimension 1: Security Principles

- **Confidentiality:**

90% van de bedrijven in Nederland die Microsoft Exchange gebruiken hebben alles al geüpdatet zodat de servers veilig zijn, dat wil zeggen dat er nog minimaal 1200 servers kwetsbaar zijn voor mogelijk gehackt te worden. Door de update te doen zou alle data van de gebruikers van Microsoft Exchange beter beveiligd worden.

- **Integrity:**

Het NCSC, Nationaal Cyber Security Centrum, adviseert om de nieuwe scripts opnieuw te bekijken en testen om er mogelijks kwaadaardige code uit te halen, zo blijven de gegevens veilig en uit handen van hackers.

- **Availability:**

Microsoft stelde een tool beschikbaar, security patches, die snel en makkelijk de problemen kon oplossen.

Dimension 2: Information States

- **Data in Transit:**

De mailboxen van de bedrijven zijn opgeslagen op de een server van MS Exchange. Die servers zijn privé per bedrijf en worden onderhouden door de servermanagers.

- **Data in Storage:**

De data in rest zijn alle mailboxen van bedrijven die gebruik maken van MS Exchange. Dit is het hoofddoel van de hackers omdat de data niet in beweging is over het netwerk.

- **Data in Process:**

Volgens de NCSC worden de gehackte mailboxen verkocht op de zwarte markt.

Dimension 3: Security Safeguards

- **Technologies:**

Er wordt aangeraden dat de systeembeheerders de software van MS Exchange updaten om erger te voorkomen. Ook wordt er aangeraden alle scripts te checken op fouten of kwaadaardige code.

- **Policies, Procedures and Guidelines:**

Er werd een tool beschikbaar gesteld om de zeodays snel en makkelijk weg te krijgen, later werd er een patch uitgevoerd om het probleem op te lossen.

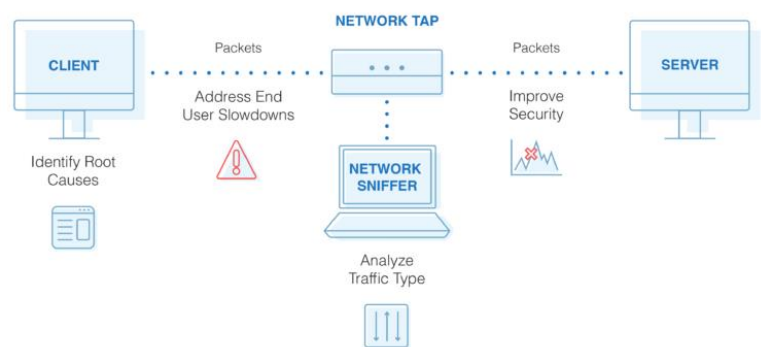
- **Users of Cyberspace:**

De gebruikers van de mailboxen die werken op de MS Exchange server konden er niet veel aan doen, het probleem moest opgelost worden door de serverbeheerders.

4.2 Security goals

1. Network Sniffing

Network Sniffing is een programma dat gebruikt kan worden om dataverkeer op een netwerk te bekijken en te analyseren.



Network Sniffing & The McCumber Cube

1st Dimension: The Principles of Security

Confidentiality – netwerkpakketten die niet geëncrypteerd zijn kunnen opnieuw worden samengesteld en in hun geheel worden gelezen.

Integrity – de gegevens zijn niet integer aangezien de attacker er ook toegang tot heeft.

Availability – het netwerkverkeer is niet beveiligd en is toegankelijk voor verschillende soorten apparaten.

2nd Dimension: The States of Data

Data in Transit – de netwerkpakketten worden uitgewisseld

Data in Process – gegevens die gewijzigd kunnen worden door de attacker

Data in Storage – data dat binnen het netwerkverkeer wordt bijgehouden & opgeslagen.

Figuur 3: Network Sniffing

3rd Dimension: Cybersecurity Safeguards

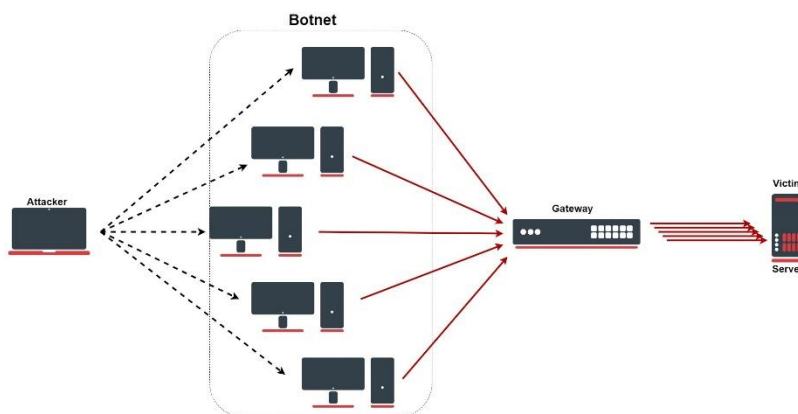
Technologies – gebruik een VPN, als het netwerk wordt "gesniffed" zorgt de VPN dat de datapakketten onbruikbaar worden.

Policies, Procedures and Guidelines – gebruik geen openbare wifinetwerken, deze zijn niet beveiligd en makkelijk toegankelijk voor hackers.

Users of Cyberspace – informeer je over dit soort aanvallen en neem de geschikte maatregelen om je ervoor te beschermen.

2. DDoS Attack

DDoS staat voor Distributed Denial of Service, dit is een cyberaanval dat heel veel verkeer doorstuurt naar netwerken met behulp van botnets. Dit soort aanvallen kunnen ervoor zorgen dat het netwerk vertraagt of zelfs plat ligt.



Figuur 4: DDoS Attack

1st Dimension: The Principles of Security

Confidentiality – een DDoS op zich beïnvloedt de confidentiality niet. Mits het als een afleidingsmaneuver wordt gebruikt om een andere aanval uit te voeren.

Integrity – de integriteit van data verandert niet door een DDoS attack.

Availability – een DDoS attack beïnvloedt voornamelijk Availability, door het verkeer dat verstuurd wordt naar de servers, kunnen netwerken niet available zijn op het gewenste moment.

2nd Dimension: The States of Data

Data in Transit – de packets die over het netwerk worden uitgewisseld.

Data in Process – de gegevens worden verwerkt door een CPU of RAM.

Data in Storage – data dat opgeslagen is op de servers.

3rd Dimension: Cybersecurity Safeguards

Technologies – Het is erg moeilijk een DDoS attack te diagnosticeren. Daarom wordt het aangeraden Anti-DDoS Protection services te gebruiken, op deze manier wordt het verkeer geïnspecteerd door cloud servers.

Policies, Procedures and Guidelines – DDoS mitigation services gebruiken.

Users of Cyberspace – de enige manier om je te beschermen tegen een DDoS attack is door gebruik te maken van Anti-DDoS Protection. Moest er een DDoS attack plaatsvinden, identificeer het type aanval, welke tool werd gebruikt om de aanval uit te voeren, houd elke stap bij en kies een goede DDoS mitigation service.

3. Rogue WiFi Access Point

Een Rogue WiFi Access Point of te wel 'Silent Killer' is een access point dat wordt geïnstalleerd op een beveiligd WiFi-netwerk zonder de toestemming van de eigenaar. Dit is een makkelijke manier om WiFi-netwerken te hacken.

1st Dimension: The Principles of Security

Confidentiality – wanneer de aanvaller eigenaar is van de access point, kan hij gegevens die door dat WiFi-netwerk stromen opvangen, deze gegevens kunnen geleaked worden.

Integrity – wanneer er een actieve interception plaatsvindt, kan de hacker gegevens manipuleren door ze te wijzigen.

Availability – bij het plaatsen van een Rogue WiFi Access Point, is het netwerk nog altijd toegankelijk voor de gebruikers.

2nd Dimension: The States of Data

Data in Transit – de data die door het WiFi-netwerk stromen kunnen verloren geraken door manipulatie van de attacker.

Data in Process – gegevens kunnen gewijzigd worden door de attacker, met andere woorden, ze zijn niet integer.

Data in Storage – de attacker heeft geen toegang tot data dat op fysieke locaties is opgeslagen.

3rd Dimension: Cybersecurity Safeguards

Technologies – door gebruik te maken van VPN's of HTTPS kunnen we ons tegen dit soort aanvallen beveiligen.

Policies, Procedures and Guidelines – stel een no-exception policy op tegen het gebruik van draadloze internetverbindingen.

Users of Cyberspace – het is verstandig om twee keer na te denken over gratis draadloze wifi-netwerken op publieke plaatsen zoals café's of luchthavens.

4. Electromagnetic Pulse (EMP)

Dit is een aanval gebaseerd op een electromagnetisch veld, het legt al de communicatie plat en kan de hardware beschadigen.

1st Dimension: The Principles of Security

Confidentiality – wanneer er een EMP attack plaatsvindt, wordt de hardware zodanig vernietigd, dat het bijna onmogelijk is deze te herstellen. Toch is er een kleine kans dat moederborden en hardeschijven hersteld kunnen worden, als deze herstelling plaatsvindt door de attacker, is er een kans dat hij in bezit komt van data, deze data kan vervolgens leaked of verkocht worden.

Integrity – de gegevens zijn integer, want een EMP wijzigt niks in data.

Availability – een EMP attack legt alles plat, alle hardware en elektronica is onbruikbaar. Denk aan bankingdiensten, hier kan je geen gebruik van maken als er een EMP attack plaatsvindt.

2nd Dimension: The States of Data

Data in Transit – wanneer er een EMP attack plaatsvindt, zijn de gegevens niet in beweging. Deze liggen stil.

Data in Process – geen data wordt verwerkt omdat alle elektronica en hardware vernietigd is.

Data in Storage – data dat op fysieke locatie is opgeslagen zoals op harde schijven, kunnen hersteld worden, maar dit is niet gegarandeerd.

3rd Dimension: Cybersecurity Safeguards

Technologies – een Faraday cage kan sommige elektronica beschermen tegen storingen. Een Faraday cage is vernoemd achter wetenschapper Michael Faraday en is simpel gezegd aluminiumfolie, op deze manier worden elektromagnetische stralingen geblokkeerd.

Policies, Procedures and Guidelines – er zijn geen richtlijnen die gevolgd kunnen worden tegen EMP's, het is ook niet bewezen dat EMP's mensen lichamelijk beïnvloeden, wat je elektronica betreft, gebruik een Faraday cage zoals boven vermeld.

Users of Cyberspace – er valt niet veel te doen tegen een EMP.

5. Social Engineering

De hacker gebruikt een techniek die gebruik maakt van de zwakste schakel in een systeem, namelijk de mens. Hij gebruikt dus de karaktereigenschappen van een mens, nieuwsgierigheid, hebzucht, angst...

1st Dimension: The Principles of Security

Confidentiality – via social engineering krijgt de hacker toegang tot persoonlijke gegevens van de persoon die in de val wordt gelokt. Ook kunnen er gegevens gestolen worden in dit proces.

Integrity – gegevens kunnen hun integriteit verliezen sinds de manipulator deze data kan corrupten.

Availability – afhankelijk van de hacker, als hij toegang krijgt tot accounts waarna hij de wachtwoorden wijzigt, kan het de availability van deze diensten voor de eigenaar beperken.

2nd Dimension: The States of Data

Data in Transit – de attacker maakt gebruik van manipulatietechnieken om toegang tot gegevens te krijgen.

Data in Process – de attacker die in bezit komt van de gestolen data, hier mogelijk wijzigingen in brengt.

Data in Storage – gegevens van de gebruiker die op fysieke locaties zijn opgeslagen zoals een NAS of hardeschijf zijn beschermd tegen diefstal van de attacker.

3rd Dimension: Cybersecurity Safeguards

Technologies – update je anti-virus/anti-malware software regelmatig. Scan het systeem op infecties. Maak gebruik van MFA, op deze manier ben je zeker dat je accounts beschermd zijn tegen attackers die een inlogpoging proberen te doen.

Policies, Procedures and Guidelines – door mails te filteren, komen ongewenste mails in je spam terecht, zo kun je onderscheid maken tussen legitieme en scam mails.

Users of Cyberspace – gebruik je gezond verstand en trap niet zomaar in winacties die je via mail ontvangt, mensen kunnen misbruik maken van je naïviteit. Sommige aanbiedingen zijn veel te mooi om waar te zijn, daarom is het geen feit.



Figuur 5: Social Engineering Life Cycle

6. Ransomware

Letterlijk vertaald als gijzelsoftware. Dit wordt door hackers gebruikt als chantagemiddel in de onlinewereld. Ransomware is malware die een systeem blokkeert en de gebruikers er geld voor vraagt om het systeem te bevrijden.



Figuur 6: Ransomware

1st Dimension: The Principles of Security

Confidentiality – sinds de aanvaller toegang heeft tot de gegevens van de persoon of organisatie in kwestie, zijn de gegevens niet meer confidential.

Integrity – gegevens verliezen hun integriteit, sinds de attacker hier toegang tot heeft en ze kan wijzigen/saboteren.

Availability – wanneer je in aanmerking komt met ransomware, versleuteld de attacker je gegevens, je kunt er pas terug aan als je de gijzelaar een som van bedrag betaald.

2nd Dimension: The States of Data

Data in Transit – gegevens zijn niet in beweging wanneer er een malicious attack zoals ransom plaatsvindt.

Data in Process – attackers richten zich soms op specifieke data, om ze vervolgens te verkopen aan een derde partij.

Data in Storage – door gegevens die in rest zijn te encrypteren maak je ze ongebruikbaar voor attackers.

3rd Dimension: Cybersecurity Safeguards

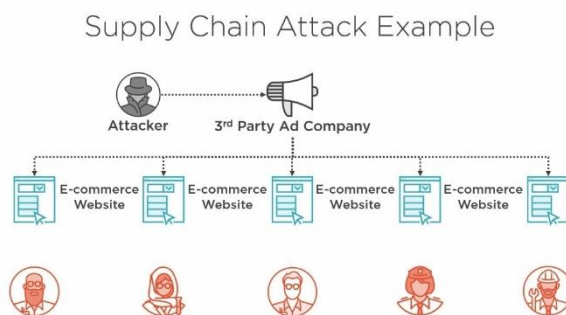
Technologies – houd je software regelmatig up to date, zodat er bugfixes zijn en minder zwakke punten in het systeem zitten. Wanneer er exploits zijn, voer security patches uit.

Policies, Procedures and Guidelines – gebruik een defence in depth strategie, dit is het plaatsen van verdedigingslayers met verschillende mitigations op elke layer. Dit helpt malware op tijd te detecteren.

Users of Cyberspace – gebruik je gezond verstand. Download geen applicaties van bronnen die je niet vertrouwd en unofficial zijn.

7. Supply Chain Attack

Supply chain-aanvallen zijn een opkomend soort dreiging die gericht is op softwareontwikkelaars en software leveranciers. Het doel is om toegang te krijgen tot broncodes, processen fals op te bouwen of mechanismen bij te werken door legitieme apps te infecteren en malware te verspreiden.



Figuur 7: Supply Chain Attack Example

1st Dimension: The Principles of Security

Confidentiality – de broncodes en gegevens van de software developers worden blootgesteld aan de invaller, de confidentiality van de data wordt misbruikt en bewust gesaboteerd.

Integrity – de data zal niet integer zijn tussen aanvaller en ontwikkelaar, en dat is de bedoeling van de aanvaller.

Availability – doordat de broncodes en opmaak van legitieme apps aangetast wordt, zal dit betekenen dat de apps in kwestie, of de informatie die misbruikt wordt, tijdelijk buiten gebruik zal zijn, totdat de schade is herstelt. Meestal zullen de aanvallers losgeld vragen.

2nd Dimension: The States of Data

Data in Transit – er zou data in beweging kunnen zijn, het is afhankelijk van de context. In het geval dat een Supply Chain Attack live is, en het gaat over een app die live ook in gebruik is, met gegevens die constant in transit zijn door de cloud, dan is er een kwestie van 'sync-time', tussen developer, gebruiker en aanvaller. De aanval heeft in dat voorbeeld geval 'transit'.

Data in Process – dit zou meestal het doelwit zijn van een Supply Chain Attack, om Data in Process te vernietigen of wijzigen. Bijvoorbeeld door apps of websites die nog in constructie zijn aan te vallen.

Data in Storage – backups of rollbacks van eerdere versies zouden behulpzaam kunnen zijn in het geval van een Supply Chain Attack. De eerdere versies zouden 'in rest' zijn.

3rd Dimension: Cybersecurity Safeguards

Technologies – honeytokens implementeren, een goede PAM (Privileged Access Management) structuur, Zero trust Architectuur (ZTA) invoeren, mogelijke 'insider threats' identificeren. (Kost, Edward)

Policies, Procedures and Guidelines – een implementatie van strenge data security regels binnen het bedrijf is van belang. Er zijn geen officiële guidelines, de verantwoordelijkheid ligt bij het bedrijf.

Users of Cyberspace – software developers / leveranciers te goed te trainen tegen dit soort aanvallen is belangrijk, en zal de integriteit van het bedrijf helpen.

8. Aardbeving

Een plotseling gewelddadig schudden van de grond, wat typisch grote vernietiging veroorzaakt, als gevolg van bewegingen in de aardkorst of vulkanische activiteit.

1st Dimension: The Principles of Security

Confidentiality – door natuurlijke incidenten zoals een aarbeving, zullen de betroffene landen/maatschappijen de handen vol hebben met het herstellen van hun (digitale) infrastructuur. Daardoor zijn ze tijdelijk kwetsbaar (Vulnerability), en zouden cyber attacks mogelijk minder aandacht trekken.

Integrity – n.v.t

Availability – data centres, telefonmasten, militaire infrastructuur, en infrastructuur in het geheel zou beschadigd zijn, data wordt op deze manier beschadigd en/of verwijderd.

2nd Dimension: The States of Data

Data in Transit – data in transit zou kunnen onderbroken worden, als de receivers/forwarders/senders power cuts meemaken, of als gehele gebouwen vernietigd worden als gevolg van de aardbedving.

Data in Process – hetzelfde geldt voor data in storage en data in process.

Data in Storage – hardware die gegevens opslaat, kan door aardbevingen worden beschadigd. Het hangt af van de ernst van de aardbeving. In sommige gevallen wordt de hardware niet beïnvloed, als dit het geval is, is er een kans om de hardware te herstellen en de gegevens te redden.

3rd Dimension: Cybersecurity Safeguards

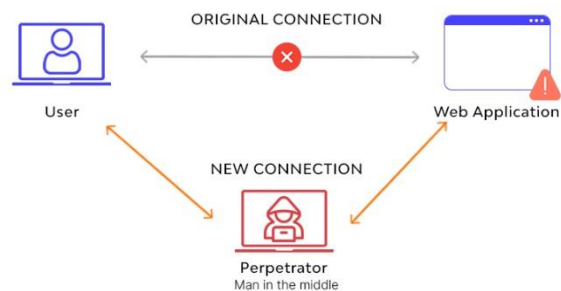
Technologies – isolatie systemen en ‘dampers’, die vibraties reduceren in gebouwen zouden behulpzaam kunnen zijn.

Policies, Procedures and Guidelines – een sterke backup policy via niet alleen de cloud, maar ook hardware wat op beveiligde, zekere locaties bewaard wordt, in locaties die misschien zelfs aardbeving bestendig zouden zijn.

Users of Cyberspace – backup, backup, backup.

9. Man in the Middle Attack

Een 'Man in the Middle Attack' omschrijft een cyberaanval waarbij de aanvaller in het geheim de communicatie doorgeeft en mogelijk wijzigt tussen twee partijen die denken dat ze rechtstreeks met elkaar communiceren, omdat de aanvaller zich tussen de twee partijen heeft ingevoegd.



Figuur 8: Man in the Middle Attack

1st Dimension: The Principles of Security

Confidentiality – de confidentiality tussen de gebruiker en de tegenpartij, of het nou een web applicatie/server is of een ander persoon, word gecompromitteerd, en als gevolg is data confidentiality breached.

Integrity – de integriteit van data te beschadigen, is het doel van een Man in the Middle Attack. Om de 'boodschap' (of het nou een boodschap, of een data packet, of iets anders is) te wijzigen, en gewijzigd door te sturen aan de ontvanger is de bedoeling.

Availability – een Man in the Middle Attack gaat soms onbemerkt. Soms (als het om simpele gebruikers gaat), hebben de gebruikers niet door dat iemand hun berichten aan het beïnvloeden is. De 'Availability', schijnt dus onveranderd.

2nd Dimension: The States of Data

Data in Transit – hier gaat een Man in the Middle te werk. Het gaat erom, de data in transit te beïnvloeden, zodat de ontvanger van de data een gewijzigd bericht, of gewijzigde informatie ontvangt.

Data in Process – door de Data in Process te beshouwen, als Man in the Middle, is mogelijk om de data in kwestie te beïnvloeden, zodat het niet opgemerkt wordt, welke wijzigingen worden doorgevoerd. Afhankelijk van de context zou een Man in the Middle onbemerkt kunnen opereren, als die een goed begrip heeft van de Data in Process.

Data in Storage – dit is meestal niet het doelwit van een Man in the Middle attack.

3rd Dimension: Cybersecurity Safeguards

Technologies – volgende maatregelen zouden kunnen helpen: VPN, SSL connectie, Endpoint Security, MFA.

Policies, Procedures and Guidelines – Het handhaven van een sterk encrypterings-mechanisme op draadloze toegangspunten voorkomt dat ongewenste gebruikers zich bij uw netwerk aansluiten door gewoon in de buurt te zijn.

Users of Cyberspace – simpele gebruikers kunnen zichzelf op de hoogte stellen van hoe je een Man in the Middle attack zou kunnen identificeren, door middel van informatieve videos/cursussen/opzoeken. Software ontwikkelaars en gevorderde gebruikers dienen hierin gebtraind en opgeleid te zijn.

10. Lock your Device

Het is mogelijk om een schermvergrendeling in te stellen op de device in kwestie. Elke keer het apparaat inschakelt of het scherm activeert, wordt er gevraagd om het apparaat te ontgrendelen, meestal met een pincode, patroon of wachtwoord, maar ook met Gezichtsherkenning of Fingerprint.

1st Dimension: The Principles of Security

Confidentiality – het beveiliging van een device heeft als doel om de confidentiality van data te bewaren. Dit is dus de dimensie in kwestie. Als een device niet goed beveiligd is, zou de data erop kunnen worden misbruikt.

Integrity – device Integrity is heel belangrijk, als iemand zonder een cyberanval een device zou kunnen ontgrendelen, omdat de 'Confidentiality' van de Device niet 'confidential' meer is, dan kan dit soms zware gevolgen hebben voor de person/en in kwestie.

Availability – een goede 'confidentiality-policy' zou kunnen helpen om de availability van de data in kwestie te beperken. Op die manier zou niemand zonder een cyberanval de integriteit van de device in gevaar kunnen brengen.

2nd Dimension: The States of Data

Data in Transit – een goede lock your device policy heeft meestal een effect op Data in Process en Data in Storage, het heeft minder invloed op Data in Transit. De redenen hiervoor is dat als er een goede lock your device policy bestaat, dan zal de Data in Transit zonder een cyberanval niet beïnvloed zijn, omdat de gebruiker zelf de Data in Transit beheerd.

Data in Process – als een device ontgrendeld word door iemand die normaalgesproken geen toegang daarvoor zouden moeten hebben, dan zou dit tot data verlies of vernietiging kunnen leiden. Ook zou een kwaadaardig persoon identificatie gegevens kunnen misbruiken om bij andere portalen/apps/plekken binnen te raken.

Data in Storage – hetzelfde geldt voor Data in Storage. Gevoelige informatie of beelden zouden gebruikt kunnen worden voor chantage, of in ruil tegen losgeld.

3rd Dimension: Cybersecurity Safeguards

Technologies – MFA, 2FA, Face recognition, Complexe pincodes, pattern codes, Fingerprint, complexe wachtwoorden volgens de password policy.

Policies, Procedures and Guidelines – complexe wachtwoorden gebruiken die voldoen aan de password policy, en MFA gebruiken.

Users of Cyberspace – dit geldt voor alle users of cyberspace. Als iemand toegang zou hebben tot de device in kwestie, zonder daarbij een cyberaanval te plegen, of als de password policy heel slecht is, dan is dit de makkelijkste manier om data te verliezen of in een ongemakkelijke situatie te belanden.

11. Phishing

Phishing is een vorm van 'social engineering'-aanval die vaak wordt gebruikt om gebruikersgegevens te stelen, waaronder inloggegevens en creditcardnummers. Het komt voor wanneer een aanvaller, die zich voordoeft als een vertrouwde entiteit, een slachtoffer verleidt om een e-mail, DM, of sms-bericht te openen.

1st Dimension: The Principles of Security

Confidentiality – het idee van 'confidentiality' speelt hierbij een belangrijke rol, het gaat namelijk om vertrouwen tussen twee of meer partijen. Typisch worden oudere mensen hiermee aangevallen, door middel van email meestal, omdat ze weinig/minder weten over cyber security. Als een kwaadaardig persoon/groep een andere entiteit ervan overtuigd, hun credit card informatie door te sturen bij voorbeeld, omdat ze een verhaal verzinnen over een familie-lid, dan zou dit de data confidentiality van het slachtoffer in kwestie consequent beïnvloeden.

Integrity – de integriteit van de data behorend tot het slachtoffer in een phishing attack is als gevolg gecompromitteerd.

Availability – laten we een credit card als voorbeeld nemen, van een persoon, die die informatie verstrekt online aan iemand anders (de 'phisher'). Het uiteindelijke gevolg van een phishing attack zou dan zijn, dat het slachtoffer hun credit card laat blokkeren, uiteindelijk geld heeft verloren, en een nieuwe credit card moet aanvragen. Het slachtoffer zal tijdelijk geen credit card kunnen gebruiken.

2nd Dimension: The States of Data

Data in Transit – de 'transit' van data, zou het verstrekken van informatie kunnen zijn, wat tussen slachtoffer en aanvaller plaats vindt. Verder wordt de data die verstrekt wordt niet beïnvloed van de aanvaller, omdat dit niet nodig is.

Data in Process – een benadering van data in process zou het opbouwen van vertrouwen kunnen zijn, wat tussen de partijen gebeurt. Veel voorbeelden van phishing attacks via de telefoon/email, gaan soms urenlang door, omdat de aanvaller eerst vertrouwen moet opbouwen tussen hunzelf en het slachtoffer.

Data in Storage – phishing is gericht op data in storage, geheime, beveiligde data die alleen de gebruiker daarvan toegang tot heeft te stelen.

3rd Dimension: Cybersecurity Safeguards

Technologies – Phone Number Identifiers, die bepaalde nummers automatisch als 'Potential Fraud/Spam' identificeren, voordat je opneemt. Ook goed geprogrammeerde spam filters.

Policies, Procedures and Guidelines – Nooit persoonlijke informatie verstrekken aan onbekende mensen online.

Users of Cyberspace – Mensen worden steeds alerter ten overzicht van phishing attacks, maar de attacks worden ook moeilijker te identificeren. Daarom is het belangrijk dat mensen zichzelf hierover informeren en trainen, zodat ze weten wat ze moeten doen, in het geval van een phishing attack.

12. Computer Virus

Een computerprogramma is een stukje code dat wordt gebruikt om uw systeem te beschadigen.



Figuur 9: Computer Virus Scam

1st Dimension: The Principles of Security

Confidentiality – de confidentiality van data wordt aangetast wanneer het systeem corrupt wordt door een computervirus. De bestanden kunnen worden vernietigd en aangetast. In tegenstelling tot andere kwaadaardige aanvallen zijn deze virussen uniek omdat ze zichzelf dupliceren.

Integrity – in het geval van computervirussen kunnen we niet spreken over integriteit van gegevens. Deze gegevens kunnen worden gekopieerd naar andere systemen.

Availability – wanneer de gegevens door het virus worden vernietigd, zijn deze ook niet meer beschikbaar voor de eindgebruiker tenzij hij/zij er een backup van heeft.

2nd Dimension: The States of Data

Data in Transit – in dit geval zou data in transit, de gegevens die van een systeem naar een ander systeem gekopieerd worden zijn.

Data in Process – data in process, is het infecteren van het virus in het systeem. Dit kan gebeuren op verschillende manieren zoals virussen in gedeelde bestanden, virussen die het systeem corrupten via软件下载s, etc.

Data in Storage – het virus beïnvloedt de gegevens die op het systeem zijn opgeslagen, deze gegevens worden gesaboteerd en kunnen onbeschikbaar gesteld worden voor de eindgebruiker.

3rd Dimension: Cybersecurity Safeguards

Technologies – maak gebruik van anti-virus bescherming. Er zijn verschillende programma's op de markt die goede bescherming tegen virussen en malware bieden.

Policies, Procedures and Guidelines – stel een no-exception policy op, probeer zo bewust mogelijk gebruik te maken van de cyberwereld.

Users of Cyberspace – als u niet weet waar mails vandaan komen, open de bijlage niet. Dit is een manier om het virus te computer te laten infecteren, wanneer er pop-ups verschijnen met als waarschuwing dat uw systeem is beschadigd met virussen, trap er niet in. Dit zorgt voor de infectie zelf.

5. Password & password policy

Opdracht gemaakt door: Aleyna, Stef, Tomas en Rasmus

- Aleyna Arslan:

Wachtwoorden	Makkelijk te onthouden	Moeilijk te raden	Moeilijk voor een programma	Complexiteit
SvnFI0w3rGo3sW!ld1411!?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Redelijk
6M,}G#PknPqF&k4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Redelijk	Hoog
"~&*hZ87dYQ/Hz}	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Redelijk	Hoog
higher chair whistle importance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Laag
cowboy given might found	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Laag

- Stef Swinnen:

Wachtwoorden	Makkelijk te onthouden	Moeilijk te raden	Moeilijk voor een programma	Complexiteit
TrµàTTàçkM3B*tç\$	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Laag
UT*hCHwm*6sPrH-c	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Hoog
MZCc2sCW#D6RUcU-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Hoog
levelaccountsummeruncle	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Laag
Shelfcommonriceengine	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Laag

- Rasmus Leseberg:

Wachtwoorden	Makkelijk te onthouden	Moeilijk te raden	Moeilijk voor een programma	Complexiteit
\$%Haftpflchtversicherung2022!	<input checked="" type="checkbox"/> (Voor Duitsers)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Redelijk
p`N7g9pBW`xx#3A6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Redelijk	Hoog
F8b29,'uBX)ecdyC	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Redelijk	Hoog
alivesudden supperpair	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Laag
driverexperienceshoutweed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Laag

- Tomas Soors

Wachtwoorden	Makkelijk te onthouden	Moeilijk te raden	Moeilijk voor een programma	Complexiteit
%Lokomotief1995*\$	☑	☑	☑	Laag
5v4BFKjZgJ*E@d9Y	✗	☑	☑	Hoog
GLHEQ@6#pmLe6Qwe5RL7	✗	☑	☑	Hoog
fifteen all organization exist	☑	✗	✗	Laag
new white frighten medicine	☑	✗	✗	Laag

5.2 Herhalingsvariatie en een paswoord

Aantal karakters	2 (binair)	10 (decimaal)	26	128 (ASCII)	16 (hexa)
4	$2^4 = 8$	$10^4 = 10000$	$26^4 = 456976$	$128^4 = 268435456$	$16^4 = 65536$
8	$2^8 = 256$	$10^8 = 100000000$	$26^8 = 2.09e11$	$128^8 = 7.21e16$	$16^8 = 4294967296$
12	$2^{12} = 4096$	$10^{12} = 1e12$	$26^{12} = 9.54e16$	$128^{12} = 1.93e25$	$16^{12} = 2.81e14$
20	$2^{20} = 1048576$	$10^{20} = 1e20$	$26^{20} = 1.99e28$	$128^{20} = 1.39e42$	$16^{20} = 1.21e24$
80	$2^{80} = 1.21e24$	$10^{80} = 1e80$	$26^{80} = 1.57e113$	$128^{80} = 3.77e168$	$16^{80} = 2.14e96$
128	$2^{128} = 3.4e38$	$10^{128} = 1e128$	$26^{128} = 1.31e181$	$128^{128} = 5.28e269$	$16^{128} = 1.34e154$
200	$2^{200} = 1.6e60$	$10^{200} = 1e200$	$26^{200} = 9.88e282$	$128^{200} = \text{N/A. Te groot.}$	$16^{200} = 6.67e240$

5.2.1 Bijhorende vragen

Vraag 1:

Het is belangrijk om een grote herhalingsvariatie te hebben bij een password omdat het dan moeilijker is om te cracken.

Vraag 2:

Uit de tabel is het duidelijk te zien het aantal combinaties van karakters bij een password groter wordt, naar mate van de aantal karakters. Afhankelijk van het type karakters zullen de variaties groeien naar n^p , waar n het aantal karakters van de password is, en p de hoeveelheid aan mogelijke karakters.

Vraag 3:

Voorbeeld van twee verschillende methoden; 'Dictionary Crack' en 'Brute Force Crack'. Dictionary Crack gebruikt een lijst van veel gebruikte paswoorden, woorden substitutie, of patroonherkenning om makkelijkere paswoorden te cracken. Nadat de passwordfile is gedecrypteerd, gaat een dictionary attack strings en variaties daarvan testen.

Voor een Brute Force Crack: De hedendaagse processors van zelfs 'goedkopere' PC's zijn capabel genoeg om miljarden aan paswoorden te cracken ("*Stay Secure: See How Password Crackers Work - Keeper Blog.*") Een Brute Force Crack probeert elke mogelijke combinatie te berekenen en die te testen. De 'Electronic Frontier Foundation' heeft een 250,000\$ DES cracking machine (genoemd 'Deep Crack') gebouwd in 1998, die in de loop van een paar dagen 2^{56} variaties van keys kon testen ("*Eff Des Cracker.*") om paswoorden te cracken.

Linux voorbeeld van vandaag veel gebruikt wordt: John the Ripper.

Vraag 4: Password Entropy is een maatstaf voor hoe onvoorspelbaar en onradbaar een wachtwoord is.

5.3 Passwordmanager + vragen



Figuur 10: LastPass

Mijn persoonlijke voorkeur gaat naar LastPass. Ik gebruik deze passwordmanager al een tijdje en ben er tevreden over. We kennen het allemaal, als je een goede password policy hebt komt het voor dat je voor elk platform een

ander wachtwoord hebt. Deze wachtwoorden zijn niet altijd even makkelijk om te onthouden. LastPass slaat je wachtwoorden op door ze te encrypteren met de laatste encryptie algoritmen (AES-256, PBKDF2 SHA-256 en salted hashes). Het enige wat je moet onthouden is je masterpassword, die toegang verleent tot de applicatie waar al je andere wachtwoorden zijn opgeslagen. Deze passwordmanager biedt ook een Premium functie aan, deze functie ondersteund fingerprint readers zoals Windows Biometric Framework, wanneer deze functie is ingeschakeld, heb je je masterpassword niet meer nodig en kan je inloggen met je vingerafdruk.

5.4 2FA

Vraag 1

We gebruiken wachtwoorden voor alles. Alles wat we online hebben staan zoals ons sociaal leven, onze bank apps, is allemaal toegankelijk door deze wachtwoorden, maar dit blijkt niet zo veilig te zijn, want het heeft maar 1 phishing mail nodig om deze informatie in de foute handen te laten vallen, en dat is waar we two factor authentication gebruiken (of 2FA wat ik ga gebruiken in de rest van deze uitleg). 2FA voegt eigenlijk een 2^{de} manier van authenticatie toe aan een inlogmethode, zoals de naam zelf suggereert. Eerst hebben we iets nodig wat je weet, zoals je password of pincode, en dan iets wat je nodig hebt, zoals je gsm of een keycard. Als je deze 2 combineert maak je het vele malen moeilijker voor hackers om je informatie te kraken.

Vraag 2

Als we alleen een wachtwoord gebruiken. Dit geeft de hackers maar 1 ding om te vinden om al onze informatie te kunnen stelen, bij 2FA daarentegen, gebruiken we een soort van authenticatie van een random gegenereerd nummer of code, of een online app of je mobiel device die een confirmatie vraagt. En dit kan een hacker veel moeilijker onderscheppen. Dus dit maakt 2FA een stuk veiliger en verkleint de kans dat hackers toegang krijgen tot je gegevens.

Vraag 3

Bij 2FA gebruiken we 2 verschillende manieren van authenticatie in 1 oplossing, in vergelijking met 2SV, waar je eigenlijk gewoon nog een 2de stap moet doen na het gebruiken van je wachtwoord, zoals een captcha of “im not a robot” pagina.

Vraag 4

Je kan dit eigenlijk zo goed als overal toepassen in deze tijd, bij je bank app, of bij je burgerprofiel. Het wordt ook gebruikt op verschillende sociale platformen zoals Discord, of Twitter. Daarbij komen dan ook de game engines zoals Origin of Steam.

5.5 Wachtwoord policy

Voor studenten raad ik een wachtwoordlengte van minimum 6 tot 8 karakters aan. Deze wachtwoorden moeten minstens één alfanumeriek (hoofdletter en kleine letter), één numeriek en één niet-alfanumeriek teken bevatten. Als we het over de complexiteit van deze wachtwoorden hebben, dan is het dubbel. Want als de student slechts 6-8 tekens gebruikt, zou ongeveer 27% van het totaal aan mogelijke wachtwoorden voldoen aan de complexiteitsvereiste. Ik raad het iedereen af om op schoolplatformen wachtwoorden te gebruiken die eerder op andere platformen gebruikt zijn. Dit geldt in principe voor alles. Het beste is om op elk platform een apart wachtwoord te gebruiken. Dit kan misschien moeilijk te onthouden zijn maar hier komen passwordmanagers van pas. Het is begrijpelijk dat niet iedereen direct een voorstander is voor passwordmanagers, deze kun je dan vervangen door je wachtwoorden ergens te noteren en veilig te bewaren. Voor het creëren van passwords lijkt mij het verstandigste om een random wachtwoord te genereren via een tool, we krijgen nogal snel de neiging om in onze wachtwoorden namen van onze geliefden te gebruiken of nog erger – ons eigen naam -, dit is makkelijk te raden, dus zeker een afdrader! Het regelmatig wijzigen van wachtwoorden is ook essentieel, voor geval van dataleaks.

5.6 Conclusie

Hoe meer random en ‘non-human-readable’ het wachtwoord is, en hoe meer combinaties van letters en speciale tekens er gebruikt worden, hoe moeilijker het wachtwoord zal zijn om te cracken. Als herkenbare woorden gebruikt worden voor een wachtwoord, is het meestal veel makkelijker om dit te cracken met hulp van een Dictionary Attack. De best-practice voor wachtwoorden is in het geheel: maak een ander wachtwoord aan voor elke platform wat je online/offline gebruikt, voldoende aan de password policy (minstens 8 chars, 1 hoofdletter, getallen, en symbolen), en sla deze wachtwoorden op een veilige plek op. Waar mogelijk, gebruik 2FA om een extra laag security aan het autorisatieproces toe te voegen. De gevolgen van slecht wachtwoord beheer, of het hergebruik van wachtwoorden voor meerdere platforms zou kunnen leiden tot diefstal, identiteitsfraude, loss of data of persoonlijke assets, en nog veel ergere gebeurtenissen. Het is dus echter heel belangrijk dat iedereen een goede password policy beheert.

6. Data with a hash

Opdracht gemaakt door: **Rasmus**

Opdracht 1: MD5 vergelijkingsscript

```
$pad1 = Read-Host "Geef het eerste pad"
$pad2 = Read-Host "Geef het tweede pad"

$pad1md5 = Get-FileHash $pad1 -Algorithm MD5
$pad2md5 = Get-FileHash $pad2 -Algorithm MD5

$pad1md5
$pad2md5

If ($pad1md5.Hash -ne $pad2md5.Hash)
{
    Write-Host ("De checksums zijn niet hetzelfde")
}
Else
{
    Write-Host ("De checksums zijn hetzelfde")
}
```

Opdracht 2:

```
PS C:\Users\Administrator> C:\Users\Administrator\Documents\Scripts\MD5 vergelijker.ps1
Geef het eerste pad: C:\Users\Administrator\Documents\Scripts\bestand_1.txt
Geef het tweede pad: C:\Users\Administrator\Documents\Scripts\bestand_1_gewijzigd.txt
```

Algorithm	Hash	Path
-----	----	----
MD5	E0D620814C3AB5BEECFE4069D309D39C	C:\Users\Administrator\Documents\Scripts\bestand_1.txt
MD5	8CCB088FB717137245A86F3FD9C32D89	C:\Users\Administrator\Documents\Scripts\bestand_1_gewijzigd.txt

De checksums zijn niet hetzelfde

Opdracht 2c

Algorithm	Hash	Path
-----	----	----
MD5	E0D620814C3AB5BEECFE4069D309D39C	C:\Users\Administrator\Documents\Scripts\bestand_1.pdf
MD5	501D520EE9465F94866C2EFD74DA166C	C:\Users\Administrator\Documents\Scripts\bestand_1.zip

De checksums zijn niet hetzelfde

Vragen:

1. Hashing is een deel van de 'CIA Triad' dimensie van de John Mccumber Cube. Om specifiek te zijn valt het onder Data Integrity (oftewel *Integrity* van Confidentiality/Integrity/Availability).
2. Een hash verandert wanneer de inhoud van een bestand gewijzigd wordt. Veranderen van de naam of locatie van een file heeft geen invloed op de MD5 hash. Wat wel verschillende hashes zou genereren is als de inhoud van een tekstbestand omgezet wordt naar een pdf-bestand. Dit is omdat het file formaat een deel is van de file inhoud, en dus ook een rol speelt bij het genereren van een hash. (*Michael Shnitzer*)
3. Bron die gebruikt werd voor geheel vraag 3: (*Shacklett, Mary E., and Peter Loshin.*)

a. Nadeel van MD5

MD5 is beperkt tot 128 bits, wat het makkelijker maakt om te kraken in vergelijking met andere hash formaten die later kwamen.

b. Is MD5 een secure algoritme? (Uitbreiding van nadelen)

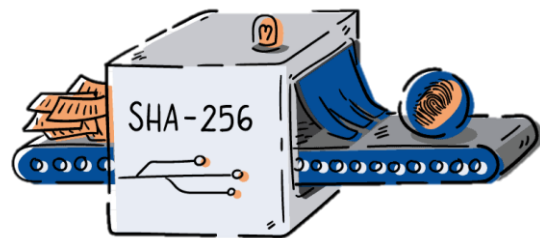
MD5-hashes worden niet langer als cryptografisch veilige methoden beschouwd en zouden volgens de IETF (Internet Engineering Task Force) niet moeten worden gebruikt voor cryptografische authenticatie: In 2011 publiceerde IETF RFC 6151, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", waarin een aantal recente aanvallen op MD5-hashes werden genoemd. Er werd een voorbeeld genoemd die binnen een minuut of minder hash-botsingen genereerde op een standaard notebook, en een ander voorbeeld die een botsing in slechts 10 seconden kon genereren op een 2,6 gigahertz Pentium 4-systeem.

c. Waar wordt MD5 gebruikt?

De meest gebruikelijke toepassing van het MD5-algoritme is voor het controleren van de integriteit van bestanden na een overdracht. Door voor en na een bestandsoverdracht een MD5-bestand te genereren, is het mogelijk om eventuele corruptie te identificeren. MD5 wordt ook nog steeds gebruikt om wachtwoorden op te slaan in sommige databases, zelfs als het niet langer veilig is.

d. Wat zijn alternatieven voor MD5

- SHA-1 (Secure Hash Algorithm)
- SHA-2 code family: SHA-224, SHA-256
- Cyclic Redundancy Checks (CRC)



Figuur 11: SHA-256

4. Bij het overdragen van files worden checksums gegenereerd die gebruikt worden om te checken of de inhoud van een file dezelfde is nadat de transfer compleet is. Als de checksums verschillend zijn, dan is de file gewijzigd of corrupted. MD5 werd in het verleden ook gebruikt (misschien in sommige gevallen tegenwoordig nog) om wachtwoorden ge-hashed op te slaan in databases.
5. Passwords worden op verschillende manieren opgeslagen in databases en servers. Of in plain tekst, of met 'outdated' hash encryptie (MD5, SHA-1), of met huidig relevante hash encryptie (SHA-2 bij voorbeeld). Ook wordt 'Salt' en 'Pepper' gebruikt om een extra hash te genereren boven op de eerste hash-methode die gebruikt wordt. Op die manier zouden twee identieke passwords verschillende gekombineerde hash values hebben (*"How to Securely Store Passwords in Database."*). Het belang van een hash (of meerdere) is natuurlijk om de veiligheid van het wachtwoord zeker te stellen, zodat een data breach niet het resultaat zou zijn van een aanval op de server/database.
6. De eerder benoemde password policy is nog steeds relevant. Als een wachtwoord gebruikt wordt, wat in de top 1000 wachtwoorden lijst voorkomt, dan zou een Dictionary Attack heel makkelijk binnen enkele seconden een hash vergelijking kunnen maken. Als een wachtwoord lang en complex is, dan stijgen de herhalingsvariaties exponentieel. Als de passwords met outdated hash encryptie op de database opgeslagen zijn, dan zal het tegenwoordig ook geen probleem zijn om die te kraken. Het wordt pas moeilijk als SHA-2 wordt gebruikt met Salt en Pepper. Een interessante tabel die bij meerdere bronnen te vinden was illustreert hoelang het zou duren om een password te cracken afhankelijk van de complexiteit daarvan. Of de berekeningen helemaal juist zijn kan ik helaas niet zeggen, het punt is, hoe complexer je password, hoe langer zal het duren om het te kraken: Stand 2021

7. Backup

Opdracht gemaakt door: Aleyna

Vraag 1:

Backup is een deel van de CIA TRIAD, die onder 'Availability' valt. Het is belangrijk dat gegevens ten alle tijden beschikbaar zijn. Daarom is dit principe noodzakelijk voor de beschikbaarheid van data te handhaven.

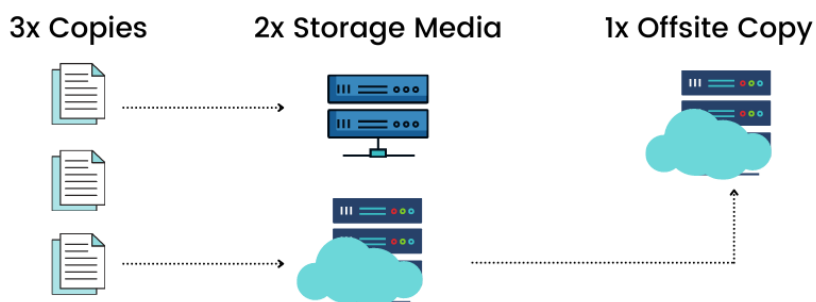
Vraag 2:

Om te beginnen is het belangrijk om te weten welke soorten backups er zijn:

1. Een volledige backup
2. Een incrementele backup
3. Een differentiële backup

Veel bedrijven in de IT-sector handhaven de **3-2-1** regel als het neerkomt op backupper van data. De **3-2-1** regel wil zeggen dat het bedrijf **3** kopieën van data moet hebben op **2** locaties waarvan **1** op een externe locatie.

3-2-1 Backup Strategy



Figuur 12: Backup Strategy



Figuur 13: Backup

harddisk of USB bij de hand hebt. Voor de beste resultaten worden er op regelmatige basis backups gemaakt om de hoeveelheid gegevens die tussen backups verloren gaat tot een minimum te beperken. Dus hoe meer tijd er verstrijkt tussen backupkopieën, hoe groter de kans op een gegevensverlies bij het herstellen van een backup.

Voor alledaagse gebruikers, die niet over al te gevoelige informatie beschikken, raad ik de Cloud aan. Het zorgt er niet alleen voor dat je snel toegang hebt tot je files, maar maakt het ook mogelijk om deze data op een der welke locatie te bereiken met slechts internetverbinding. Geen fan van de Cloud? Geen zorgen, je kunt je files ook backupper door ze naar een externe harde schijf of een USB-stick te kopiëren, op deze manier geraak je aan je files door de harddisk of USB op je computer of laptop aan te sluiten. Ook een makkelijke manier om aan je gegevens te komen, maar het nadeel is dat je zoals in de Cloud niet meteen aan de files kunt geraken mits je je

Vraag 3:

	Cloud	Lokaal	Externe harde schijf
Voordelen	<ul style="list-style-type: none"> ▪ Beveiliging: cloud opslag is veiliger dan lokale opslag door gebruik van encryptie-algoritmen ▪ Toegankelijkheid: geeft overal toegang tot data, het enige dat nodig is, is internetverbinding ▪ Herstel: in geval van een hardware storing, is de data toegankelijk in de cloud 	<ul style="list-style-type: none"> ▪ Letterlijk bij de hand ▪ Altijd op de hoogte van waar je data zich bevindt ▪ De privacy van je gegevens zijn beter beheersbaar 	<ul style="list-style-type: none"> ▪ Snelle backup ▪ Niet afhankelijk van internetverbinding
Nadelen	<ul style="list-style-type: none"> ▪ Afhankelijk van de snelheid van je internetverbinding ▪ Je geeft je backup uit handen aan een derde partij ▪ Afhankelijk van bandbreedte ▪ Het is een automatisch proces 	<ul style="list-style-type: none"> ▪ Kans dat de hardware defect geraakt ▪ Hoge kosten voor het aanschaffen van een lokale storage (bvb. NAS) ▪ De backups moeten op een fysieke plaats opgeslagen worden zoals bij je thuis, op kantoor, etc... (hier heb je de juiste ruimte en ventilatie voor nodig) 	<ul style="list-style-type: none"> ▪ Kan kapotgaan ▪ Gevoelig voor diefstal ▪ Goedkopere varianten van harde schijven kunnen crashen, waarbij als volgt de data niet altijd hersteld kan worden
Kost in apparatuur	<ul style="list-style-type: none"> ▪ Geen apparatuur nodig, enkel een maandelijks abonnement voor uitbreiding van opslag 	<ul style="list-style-type: none"> ▪ Eenmalig bedrag. Je kunt de storage uitbreiden door de schijven te vervangen (extra kosten) 	<ul style="list-style-type: none"> ▪ Eenmalig bedrag waarvan de prijs afhankelijk is van de grootte van de schijf
Onderhoud	<ul style="list-style-type: none"> ▪ Wordt onderhouden door de cloudprovider 	<ul style="list-style-type: none"> ▪ Via software: (bv. Synology heeft hyperbackup etc. en Veeam met cloudlocatie/NAS) 	<ul style="list-style-type: none"> ▪ Via software: (bv. Veeam doormiddel van backup repositories)
Betrouwbaarheid	<ul style="list-style-type: none"> ▪ Heel betrouwbaar 	<ul style="list-style-type: none"> ▪ Zo betrouwbaar als dat je het configureert, denk aan RAID 	<ul style="list-style-type: none"> ▪ Niet zo betrouwbaar: HDD-defect = backup weg

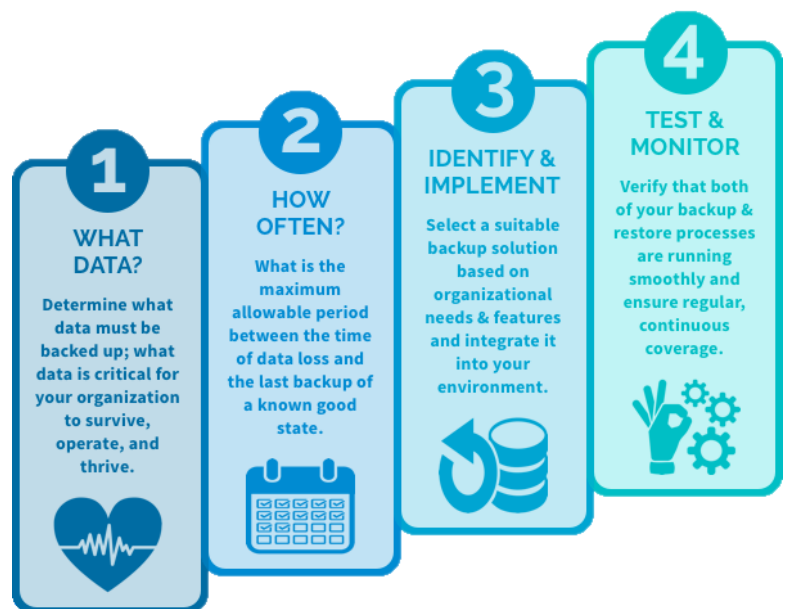
Vraag 4:

De beste backup policy die ik medestudenten kan aanraden is:

Studenten beschikken over belangrijke data voor school. Daarom is het belangrijk deze data goed te bewaren. Computer of hardeschijfstoringen komen regelmatig voor, dit kan ten slotte leiden tot een onvoldoende als je de kwijtgeraakte data niet kunt herstellen, niet alle lectoren/professoren zijn even begripvol voor dit soort situaties, uiteindelijk is het de taak van de student zijn gegevens goed op te slaan. Komt het toch voor dat de student zijn data verloren heeft door een computer of hardeschijfstoring en ze niet kan herstellen, dan lijkt het me verstandig contact op te nemen met de ICT-dienst van de instelling. Maar het hoeft allemaal niet zo ver te komen als je een goede backup policy handhaaft.

Daarom is het is verstandig om volgende 4 stappen te volgen bij het back-up van data:

1. Bepaal van welke gegevens je een backup wil maken
2. Bepaal hoe vaak er een backup van deze gegevens gemaakt moet worden
3. Identificeer en implementeer geschikte backup en hersteloplossing
4. Test je backup systeem



Figuur 14: Backup stappenplan

Alle studenten krijgen bij hun inschrijving via Office 365 2TB opslag in OneDrive. Dit is een goede manier om je files voor school te back-uppen naar de Cloud, zo geraak je aan je data waar en wanneer je ze maar nodig hebt. Het is belangrijk om de data op regelmatige basis te back-uppen. OneDrive maakt het ook mogelijk om samen te werken met medestudenten, zo kun je in SharePoint bestanden samen editen en vervolgens opslaan in de Cloud. Je kunt van deze dienst gebruik maken zolang je student bent aan de PXL.

Als we spreken over het back-uppen van persoonlijke informatie, dan zijn er 2 mogelijkheden:

1. Cloud
2. Externe harde schijf

Niet alle studenten zijn fan van de cloud omdat ze hun gegevens aan een derde partij toevertrouwen, voor die studenten zou ik aanraden om hun gegevens op een externe harde schijf op te slaan. Houd er echter rekening mee dat op deze manier alleen u verantwoordelijk bent voor uw gegevens. Bij diefstal of een beschadigde harde schijf ben je je gegevens kwijt. Je hebt ook alleen toegang tot je bestanden als je de schijf bij de hand hebt, dus het biedt geen externe toegang zoals de cloud.

Ten slotte zijn er verschillende manieren om een back-up van gegevens te maken, dit is aan de student om te beslissen. Voor sommigen is de cloud een prima oplossing, voor anderen een externe schijf en sommigen hebben zelfs een NAS in huis. Ze hebben allemaal hun eigen kwaliteiten.

8. Countermeasures technology

Opdracht gemaakt door: Rasmus

• Firewall

Doel: Het primaire doel van een firewall is om bedreigende verkeer en datapakketten te blokkeren en tegelijkertijd legitiem verkeer door te laten.

Verklaring: Er zijn verschillende manieren waarop firewalls te werk gaan: Oftewel met packet filtering, waarbij datapakketten die proberen een netwerk binnen te raken door een reeks filters moeten gaan, waarbij stukken van de datapakketten die al van tevoren af geïdentificeerd waren als bedreigend, verwijderd worden. Firewalls kunnen ook als een proxy-service gebruikt worden als een soort 'in-between', waarbij de firewall een directe connectie tussen de device en de incoming packets verhindert.

Voorbeeld: Windows Defender Firewall is de system default firewall die geïnstalleerd is op Windows devices. Anti-virus programmas zoals Bitdefender/McAfee/Kaspersky hebben hun eigen firewall, die de default Windows Defender Firewall uitschakelt, en voor deze overneemt.

Hoe maken ze een omgeving veiliger: Firewalls maken de omgeving op verschillende manieren veiliger, namelijk tegen backdoor-attacks, in sommige gevallen tegen denial of service attacks, tegen spam en remote log-ins, en natuurlijk tegen virussen.

• Vulnerability Scanners

Doel: Vulnerability Scanners maken het mogelijk voor bedrijven (of jezelf) om de netwerken en systemen te scannen voor potentiële beveiligingsproblemen.

Verklaring: In tegenstelling tot antivirussoftware wat elke netwerkfile scant, scant een vulnerability scanner specifieke interfaces, externe/interne IP-adressen, porten en services voor kwetsbaarheden.

Voorbeeld: Nmap, Nexpose, OpenVAS, SAINT

Hoe maken ze een omgeving veiliger: Vulnerability scanners genereren doorgaans een uitgebreid rapport van gevonden kwetsbaarheden en geven referenties voor verder onderzoek naar deze kwetsbaarheden. Sommige bieden zelfs aanwijzingen voor het oplossen van het probleem. Op deze manier kan men zijn eigen device, of het netwerk in gebruik veiliger maken.

• IDS

Doel: Intrusion Detection System (IDS) is een detectiesoftware dat is ontworpen om kwaadaardige acties te detecteren.

Verklaring: Dit wordt bereikt door informatie die wordt verzameld uit verschillende systemen en netwerkbronnen, die vervolgens wordt geanalyseerd op beveiligingsproblemen. IDS wordt over het algemeen ingezet met als doel het bewaken en analyseren van gebruikers- en systeemactiviteit, het controleren van systeemconfiguraties en kwetsbaarheden, het beoordelen van de integriteit van kritieke systeem- en gegevensbestanden, het uitvoeren van statistische analyses van activiteitspatronen op basis van de overeenstemming met bekende aanvallen, het detecteren van abnormale activiteit en besturingssystemen controleren.

Voorbeeld: Suricata, Stealthwatch, OSSEC

Hoe maken ze een omgeving veiliger: Een IDS fungeert als een aanpasbare beveiligingstechnologie voor systeembeveiliging nadat traditionele technologieën/software falen. Dit zou handig kunnen zijn als een extra maatregel naast een Antivirusprogramma.

- IPS

Doel: Om het netwerk te beveiligen, bedreigingen aan het netwerk te detecteren en te voorkomen.

Verklaring: Een Intrusion Prevention System (IPS) is een vorm van netwerkbeveiliging die werkt om geïdentificeerde bedreigingen te detecteren en te **voorkomen**. Het voorkomen gedeelte is een belangrijk verschil tussen een IPS en een IDS. De IPS rapporteert gebeurtenissen aan systeembeheerders en neemt preventieve maatregelen, zoals het sluiten van ports, en het configureren van firewalls om toekomstige aanvallen te voorkomen.

Voorbeeld: Splunk, Sagan, Zeek, OSSEC

Hoe maken ze een omgeving veiliger: Door het netwerk te beveiligen biedt een IPS een extra maatregel naast Antivirussoftware voor de device om een lokaal netwerk, of andere soorten netwerken, te beveiligen.

- VPN

Doel: Een VPN geeft je online privacy en anonimiteit door gebruik te maken van een virtueel prive netwerk, gehosted door een publieke internet connectie.

Verklaring: VPN is een Virtual Private Network dat werkt als een intermitterende service tussen u en uw hostsite. Het kan een veilige modus bieden om op internet te surfen, omdat het u privacy en gegevensbeveiliging biedt. Bij correct gebruik helpt een VPN uw verbindingen veilig te houden en uw apparaat te beschermen.

Voorbeeld: NordVPN, Bitdefender VPN, ProtonVPN, ExpressVPN

Hoe maken ze een omgeving veiliger: Door gebruik te maken van een VPN is uw IP-adres, en de meeste andere netwerkgegevens niet onmiddellijk zichtbaar voor personen die daarin interesse zouden hebben. Dit werkt als extra bescherming voor uw thuis/bedrijf netwerk.

- Virusscanner

Doel: Antivirussoftware helpt uw computer te beschermen tegen malware, virussen, en andere nare bedreigingen.

Verklaring: Antivirussoftware kijkt naar gegevens - webpagina's, bestanden, software, applicaties - die via het netwerk naar uw apparaten komen. Het zoekt naar bekende bedreigingen en bewaakt het gedrag van alle programma's, waarbij verdacht gedrag wordt geflagged. Het probeert malware zo snel mogelijk te blokkeren of te verwijderen.

Voorbeeld: Kaspersky, Bitdefender, McAfee, Avast

Hoe maken ze een omgeving veiliger: Het is een goede, zeer toegankelijke methode om jezelf en je device te beveiligen tegen ongewenste malware, virussen, en andere nare bedreigingen. Voor zelfs de meest onervaren gebruiker zou een Antivirusprogramma hanteerbaar zijn, wat het een goed product voor 'the masses' maakt.

9. THM - Searching the internet.

Opdracht gemaakt door: Tomas

1. Example Research Question

Bij de eerste opgave, hebben ze ons laten ondervinden hoe je te werk moet gaan om opzoek werk te doen op het internet zelf over verschillende topics, en dat je keywords moet gebruiken om tot je resultaat te geraken. Dus bij de eerste vraag gingen we bij elke deelvraag de keywords eruit halen en deze in een zoekmachine zoals google Chrome of Firefox ingeven.

Answer the questions below

What is the CVE for the 2020 Cross-Site Scripting (XSS) vulnerability found in WPForms?

CVE-2020-10385

Correct Answer

There was a Local Privilege Escalation vulnerability found in the *Debian* version of Apache Tomcat, back in 2016. What's the CVE for this vulnerability?

CVE-2016-1240

Correct Answer

What is the very first CVE found in the VLC media player?

CVE-2007-0017

Correct Answer

If you wanted to exploit a 2020 buffer overflow in the sudo program, which CVE would you use?

CVE-2019-18634

Correct Answer

2. Vulnerability Searching

Bij deze vraag hebben ze ons uitgelegd over de verschillende manieren waarmee hackers of WHH weakpoints of vulnerabilities in een software of website kunnen misbruiken. Hierbij gaven ze ons 3 verschillende websites. Waarvan ExploitDB waar alle verschillende scripts of programma's staan, die dan misbruik kunnen maken van deze vulnerabilities. En NVD en CVE mitre zijn beide vulnerability databases waar de verschillende CVE's staan opgesteld in een lijst, met elk hun unieke CVE. Dus voor elke deelvraag gingen we op elk van deze pagina's opzoek naar de CVE's, waarbij we ook de keywords uit de vraag gingen halen en gingen ingeven op de filters van de zoekpagina's om achter de CVE's te komen.

Answer the questions below

In the Burp Suite Program that ships with Kali Linux, what mode would you use to manually send a request (often repeating a captured request numerous times)?

Correct Answer

 Hint

What hash format are modern Windows login passwords stored in?

Correct Answer

 Hint

What are automated tasks called in Linux?

Correct Answer

 Hint

What number base could you use as a shorthand for base 2 (binary)?

Correct Answer

 Hint

If a password hash starts with \$6\$, what format is it (Unix variant)?

Correct Answer

 Hint

3. Manual Pages

Bij deze vraag gaven ze ons de uitleg over de man pages op Linux, en hoe je tewerk moet gaan met deze manpages. En ik denk dat man pages voor zichzelf spreken, dit zijn manuals of handleidingen van de verschillende tools op Linux. En bij elke deelvraag gingen we op de man pages kijken naar welke switch we nodig hadden bij welke functie van een tool. Buiten de laatste, want hier moesten we een commando opgeven in plaats van een switch. Dus hier gingen we op zoek naar een combinatie van de verschillende switches, dus hier gingen we alle switches af om te kijken welke het gewilde resultaat zouden geven.

Answer the questions below

SCP is a tool used to copy files from one computer to another.

What switch would you use to copy an entire directory?

Correct Answer

 Hint

fdisk is a command used to view and alter the partitioning scheme used on your hard drive.

What switch would you use to list the current partitions?

Correct Answer

nano is an easy-to-use text editor for Linux. There are arguably better editors (Vim, being the obvious choice); however, nano is a great one to start with.

What switch would you use to make a backup when opening a file with nano?

Correct Answer

Netcat is a basic tool used to manually send and receive network requests.

What **command** would you use to start netcat in listen mode, using port 12345?

Correct Answer

 Hint



Congratulations

You've completed the room!

 Share on Twitter

 Share on Facebook

 Share on LinkedIn

[Leave feedback](#)

10. OSINT Lodrimed

Opdracht gemaakt door: Stef

- **Flag 1:**

PXL{You_Are_On_The_Right_Path}



De eerste flag was makkelijk te vinden. in de browser geef je 'lodrimed' in en klik je op de eerste link. Daar kwam je op een pagina die verwees naar Twitter waar de flag te vinden was in de eerste tweet.

- **Flag 2:**

PXL{Ernest!}

Intro

<https://twitter.com/LoDriMed1>

PXL{Ernest!}



Lodrimed



Studeerde aan Hogeschool PXL



Dierentraining



Hondenshows



Hengelsport

In verdere tweets stond de naam Ernest Vanderbauwen. Deze naam moest ingegeven worden in google om zo op zijn Facebookpagina te komen. Hier stond de volgende flag aangegeven.

- **Flag 3:**

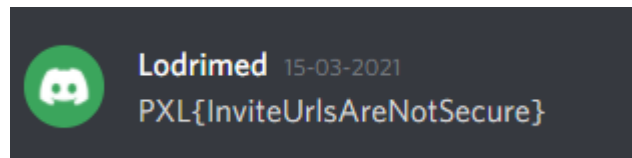
`PXL{We_Should_Not_Be_Here}`

Chat is momenteel uitgeschakeld. Je kan geen nieuwe berichten sturen. PXL{We_Should_Not_Be_Here}

Al zocht je verder in de foto's van deze gebruiker kon je een link aflezen uit één van deze foto's: lodrimed.tk/login.html. Na deze in te geven in de browser kwam je op een login pagina van de intranet website. Hier moest je inloggen met de naam ernest.vanderbauwen en het wachtwoord Artemis. Na het inloggen kwam je in de intranet chat met Sonny, onder de chat stond de flag.

- **Flag 4:**

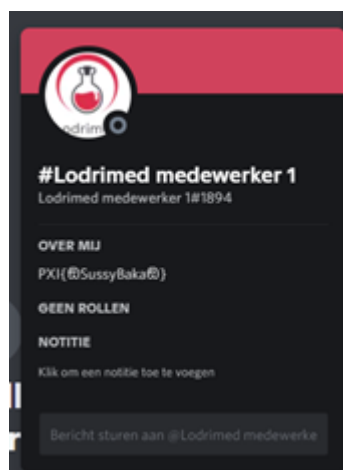
`PXL{InviteUrlsAreNotSecure}`



In de chat daarentegen stond een link naar een Discord server. In het chatkanaal 'news' stond de flag aangegeven.

- **Flag 5:**

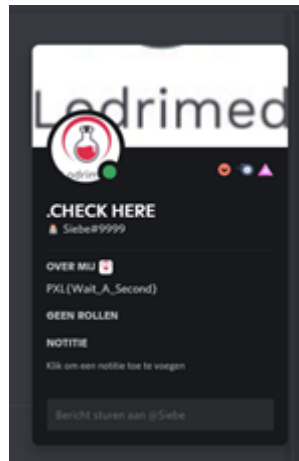
`PXI{๖SussyBaka๖}`



Door te gaan kijken bij de leden kon je 2 profielen zien met de naam .CHECK HERE en #Lodrimed medewerker. Na het aanklikken van deze namen kon je een nieuwe flag vinden.

- **Flag 6:**

PXL{Wait_A_Second}



Door te gaan kijken bij de leden kon je 2 profielen zien met de naam .CHECK HERE en #Lodrimed medewerker Na het aanklikken van deze namen kon je een nieuwe flag vinden.

- **Flag 7:**

PXL{Almost_There}

Lodrimed – Covid 19 samenstelling

PXL{Almost_There}

De laatste flag die we gevonden hebben stond in het recept, dat was te vinden door naar he chat kanaal data-sharing te gaan en het bestand te openen. Boven in het recept stond de flag.

- **Flag 8**

PXL{YOU_DID_IT}

Het geheime ingrediënt (mogelijks wel het belangrijkste) staat hier geëncrypteerd (Julius Caesar zou hier wel raad mee weten):

zvffpuvra zbrgra jr gbpu orfg rra naqre inppva yngra mnggra ;-). Qvg yvwvg
ireqnpug irry bc rra erprcg ibbe cnaarxbxra...

CKY{Lbh_Qvq_vg!}

De laatste flag stond onderaan en geëncrypteerd. De volledige encryptie was: misschien moeten we een ander vaccin laten maken. Dit lijkt verdacht veel op een recept voor pannenkoeken...

- **Conclusie**

Uit deze opdracht leer je dat je best geen indicaties geeft op sociale media die naar wachtwoorden verwijzen die je gebruikt. Als je dit niet doet kan er persoonlijke informatie of belangrijke informatie over het bedrijf makkelijk gevonden worden door een hacker die een paar simpele stappen neemt om in te loggen op je accounts. Door tekst te encrypteren zoals in het recept maak je het potentiële hackers moeilijker om bij gegevens te geraken. Het is dus vooral belangrijk om goede wachtwoorden te maken om je hier tegen te beschermen.

11 THM - Principles of Security

Opdracht gemaakt door: **Rasmus**

1. The CIA Triad

Answer the questions below

What element of the CIA triad ensures that data cannot be altered by **unauthorised** people?

Integrity

Submit

What element of the CIA triad ensures that data is available?

Availability

Submit

What element of the CIA triad ensures that data is only accessed by **authorised** people?

Confidentiality

Submit

2. Principles of Privileges

Answer the questions below

What does the acronym "PIM" stand for?

Privileged Identity Management

Submit

What does the acronym "PAM" stand for?

Privileged Access Management

Submit

If you wanted to manage the privileges a system access role had, what methodology would you use?

PAM

Submit

Hint

If you wanted to create a system role that is based on a users role/responsibilities with an organisation, what methodology is this?

PIM

Submit

Hint

3. Security Models Continued

Answer the questions below

What is the name of the model that uses the rule "can't read up, can read down"?

The Bell Lapadula Model

Submit

Hint

What is the name of the model that uses the rule "can read up, can't read down"?

The Biba Model

Submit

Hint

If you were a military, what security model would you use?

Bell Lapadula Model

Submit

Hint

If you were a software developer, what security model would the company perhaps use?

The Biba Model

Submit

Hint

4. Threat Modelling and Incident Response

What model outlines "Spoofing"?

STRIDE

Correct Answer

What does the acronym "IR" stand for?

Incident Response

Correct Answer

You are tasked with adding some measures to an application to improve the integrity of data, what STRIDE principle is this?

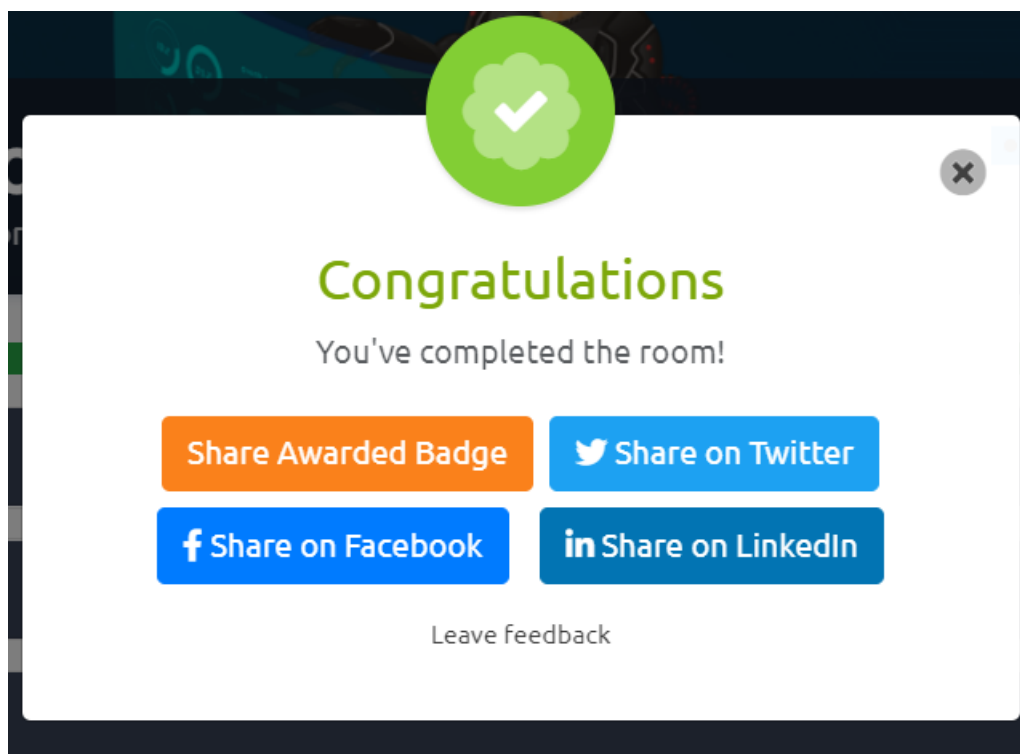
Tampering

Correct Answer

An attacker has penetrated your organisation's security and stolen data. It is your task to return the organisation to business as usual. What incident response stage is this?

Recovery

Correct Answer



Bibliografie

“Stay Secure: See How Password Crackers Work - Keeper Blog.” *Keeper Security Blog - Cybersecurity News & Product Updates*, 13 Aug. 2021, <https://www.keepersecurity.com/blog/2016/09/28/how-password-crackers-work/>.

“Eff Des Cracker.” *Wikipedia*, Wikimedia Foundation, 20 Dec. 2021, https://en.wikipedia.org/wiki/EFF_DES_cracker.

Michael ShnitzerMichael Shnitzer 2, et al. “Will Changing a File Name Affect the MD5 Hash of a File?” *Stack Overflow*, 1 Jan. 1959, <https://stackoverflow.com/questions/5055143/will-changing-a-file-name-affect-the-md5-hash-of-a-file>.

Shacklett, Mary E., and Peter Loshin. “What Is MD5 (MD5 Message-Digest Algorithm)?” *SearchSecurity*, TechTarget, 23 Aug. 2021, <https://www.techtarget.com/searchsecurity/definition/MD5>.

“How to Securely Store Passwords in Database.” *VAADATA*, 29 June 2021, <https://www.vaadata.com/blog/how-to-securely-store-passwords-in-database/>.

“Rogue Access Points (Article).” *Khan Academy*, Khan Academy, <https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:cyber-attacks/a/rogue-access-points-mitm-attacks>.

Brewin, Bob. “How to Defend Against Rogue Access Points.” *Computerworld*, 15 July 2002, www.computerworld.com/article/2577425/how-to-defend-against-rogue-access-points.html.

Conca, James. “How To Defend Against The Electromagnetic Pulse Threat By Literally Painting Over It.” *Forbes*, 10 Dec. 2021, www.forbes.com/sites/jamesconca/2021/09/27/the-electromagnetic-pulse-threatcant-we-just-paint-over-it/?sh=785d31c61883.

“What’s an Electromagnetic Pulse Attack?” *YouTube*, 25 Nov. 2011, www.youtube.com/watch?v=vurpNu84seU.

Kost, Edward. “11 Ways to Prevent Supply Chain Attacks in 2022 (Highly Effective): Upguard.” *RSS*, <https://www.upguard.com/blog/how-to-prevent-supply-chain-attacks>.

"Ransomware - Google Search." *Google*,
www.google.be/search?q=ransomware&hl=en&sxsrf=APq-WBs49zVq1j66aR_WmdWxWmYhHVUYVg:1645956613338&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjZroOa0p_2AhVkiMUKHccFASsQ_AUoAXoECAEQAw&biw=955&bih=951&dpr=1#imgrc=ESF2zetSrpQjKM&imgdii=CfUzumjuZJ03PM. Accessed 27 Feb. 2022.