Security in systemen en netwerken
Practica

Security in systemen en netwerken

Keuzedeel MBO

Practica

Jan Dolphijn

Brinkman Uitgeverij · Amsterdam · 2016

Deze practica behoren bij het boek *Security in systemen en netwerken. Keuzedeel MBO*, ISBN 978 90 5752 348 9

Redactie en opmaak: Henk Pel, Zeist

Correspondentie inzake overneming of reproductie richten aan:
Brinkman Uitgeverij, Postbus 59686, 1040 LD Amsterdam
www.brinkman-uitgeverij.nl
tel. 020-4120970, fax 020-4120972
e-mail: info@brinkman-uitgeverij.nl

Inhoud

Practicum 1.1
Klassieke encryptie

De Eerste Wereldoorlog

In 1914 brak in Europa de Eerste Wereldoorlog uit, een tijd waarin geheimen zeer belangrijk waren. Ieder land had zijn eigen encryptiemethodes.

We bespreken een veelgebruikte methode, de versleuteling die door de Amerikaan Playfair eind negentiende eeuw verder werd ontwikkeld en vaak is gebruikt in de Eerste Wereldoorlog. Deze methode is heden ten dage volledig achterhaald door de kracht van de computerprocessor.

De Playfair-versleuteling

De Playfair-versleuteling werd in 1854 uitgevonden door Charles Wheatstone. De Playfair is veel gebruikt tijdens militaire missies. Deze methode draagt de naam van Lyon Playfair, die het gebruik ervan vooral op militair gebied heeft verbreid.

Het gemak en de veiligheid van deze *poly-alfabetische substitutie* maakte van Playfair een veelgebruikte militaire versleutelingsmethode.

De versleuteling maakt gebruik van een zogenaamd Polybius-vierkant. Dit is een versleutelmethode gebaseerd op de transpositiemethode van Caesar. Het vierkant bestaat uit 5 x 5 cellen. Omdat er in het alfabet 26 letters zijn, wordt de letter J niet gebruikt en vervangen door een I – in het Engels wordt de J bijna niet gebruikt.

A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Let op: Iedere letter van het alfabet komt precies één keer voor in het vierkant.

We bedenken nu het geheime sleutelwoord, we kiezen `STALINGRAD`.

Het sleutelwoord voeren we in het vierkant in. We doen dit zo dat alle verschillende letters uit het sleutelwoord maar één keer voorkomen.

S	T	A	L	I
N	G	R	D	

Je ziet dat de A de tweede maal dat deze in het woord voorkomt is weggelaten, er komen geen dubbele letters voor.

Nu vullen we het vierkant aan met de letters uit het alfabet die nog niet in het vierkant staan. We beginnen bij de A, die staat al in het vierkant. Dan de B, die vullen we in, de C, de D staat er al in, enzovoort.

S	**T**	**A**	**L**	**I**
N	**G**	**R**	**D**	B
C	E	F	H	K
M	O	P	Q	U
V	W	X	Y	Z

Alle letters van het alfabet staan nu in het vierkant, er komen geen dubbele voor!

Oefen zelf met een vierkant, het sleutelwoord is `GRONINGEN`. Vul het vierkant aan (let op: de J wordt niet gebruikt).

G	**R**	**O**	**N**	**I**
E				
				U
V	W	X	Y	Z

Het geheime bericht dat we willen versturen is:

```
MARINE MORGEN NAAR ANTWERPEN
```

We maken van de boodschap groepjes van twee letters. We noemen zo'n groepje een *bigram.* Hier zijn twee regels van toepassing:

1 Als er twee dezelfde letters in een bigram voorkomen plaats je er een X tussen.
2 Als het laatste bigram uit één letter bestaat, voeg je een X toe.

Bijvoorbeeld BM VV MC wordt BM VX VM CX – een X tussen de V's toegevoegd en een X na de laatste enkele letter.

```
MA RI NE MO RG EN NA AR AN TW ER PE NX
```

Er zijn geen bigrammen met twee dezelfde letters, maar er is wel een oneven aantal letters, dus wordt er aan het eind een X toegevoegd.

We hebben een Polybius-vierkant samengesteld en bigrammen gemaakt. We hebben nu alle ingrediënten om de Playfair-versleuteling toe te passen.

	kolom				
rij	**S**	**T**	**A**	**L**	**I**
	N	**G**	**R**	**D**	B
	C	E	F	H	K
	M	O	P	Q	U
	V	W	X	Y	Z

De Playfair-versleuteling toepassen

Om Playfair toe te passen kijken we naar de letters in het Polybius-vierkant. Er zijn drie mogelijkheden:

- Regel 1: **Als de letters van het bigram in dezelfde rij staan, schuif je de letters 1 plek naar rechts**.

  Je versleutelt dus met de letters ernaast. `NG` wordt dus `GR`. De letter `G` staat rechts naast de `N`, en de `R` naast de `G`. Als de letter aan de rand staat zoals de `K` of `Z`, dan schuif je door naar het begin, dus `K` wordt `C` en `Z` wordt `V`.

  Voor het ontsleutelen schuif je de letters een plaats terug in de rij (naar links).

- Regel 2. **Als de letters van het bigram in dezelfde kolom staan, schuif je 1 plaats naar beneden**. Je neemt dus de letter eronder. Dus bij `TW` wordt de `T` een `G` en de `W` wordt `T`, je schuift door vanaf boven.

  Voor het ontsleutelen schuif je de letters een plaats terug in de kolom (naar boven).

- Regel 3. **Als de letters niet in dezelfde rij of kolom staan, beschouw je deze letters als de hoekpunten van een vierkant en neem je de letters van de andere hoekpunten, uit dezelfde rij**. Bijvoorbeeld `CZ` wordt `KV`. Je neemt de eerste letter, de `C`, en gaat naar de kolom waar de tweede letter staat, de `Z`. Dan kom je uit bij de `K`. Vanaf de tweede letter, de `Z`, ga je naar de kolom waar de eerste letter staat, de `C`. Dan kom je uit bij de `V`.

  `SY` wordt dus `LV` en `UG` wordt `OB`.

Terug naar onze bigrammen en het Polybius-vierkant. We versleutelen de boodschap. De eerste zeven zijn al ingevuld.

	kolom				
rij	**S**	**T**	**A**	**L**	**I**
	N	**G**	**R**	**D**	B
	C	E	F	H	K
	M	O	P	Q	U
	V	W	X	Y	Z

```
MA RI NE MO RG EN NA AR AN TW ER PE NX
PS BA GC OP DR CG RS
```

Versleutel zelf de overige bigrammen.

Playfair ontsleutelen

Ontsleutel onderstaande boodschap:

```
MBDUL KRURA OVKOB DQEPM BABDV EFQTR OMFYX
```

Sleutelwoord `MUNSTERLAND`

1 Maak bigrammen (groepeer de letters per twee).

2 Maak een Polybius-vierkant met sleutelwoord MUNSTERLAND

3 Zoek de bigrammen op in het vierkant.
   a In dezelfde rij schuif je naar links.
   b In dezelfde kolom schuif je omhoog.
   c In alle andere gevallen beschouw je de letters als hoekpunten van het vierkant – en ga ja naar de andere hoekpunten.

Gebruik onderstaand werkblad om een Playfair-encryptie uit te voeren. Doe dit in groepen van twee en wissel je ciphertekst met de sleutelwoorden in bij een ander groepje. Ontsleutel elkaars tekst.

Werkblad Playfair

Geheime boodschap:

Sleutelwoord:

5x5 Polybius-vierkant:

Bigrammen maken

Versleutelde tekst maken door middel van de Playfair-regels

Schikken in groepen van vijf tekens

Playfair ontsleutelen

Sleutelwoord:

Versleutelde tekst:

---

1 Maak het Polybius-vierkant aan de hand van het sleutelwoord.
2 Maak van de versleutelde tekst bigrammen.
3 Ontsleutel de bigrammen aan de hand van het vierkant.

Practicum 1.2
Integriteit

Informatie die door jou wordt ontvangen is correct en compleet. Je krijgt geen halve mail binnen en de tekst in de mail is ongewijzigd bij jou in de mailbox gekomen. Onderweg is er niets veranderd. Ook de informatie die van de harde schijf naar het interne geheugen wordt gekopieerd is juist en compleet. Een printopdracht, een toetsaanslag of een berekening in de calculator gaat nooit fout.

Dit gaat niet vanzelf! Het Operating System heeft een aantal manieren om te controleren of informatie goed is aangekomen.

Je hebt kennisgemaakt met de hash-waarde via de tool MAT-MD5. Deze methode stelt met 100% zekerheid vast of er wel of niet iets is gewijzigd nadat informatie is gekopieerd of verplaatst. De MD5-rekenmethode **herkent fouten, maar herstelt ze niet**.

We beginnen met het testen van de integriteit van ons eigen systeem. Met het volgende commando controleer je of jouw (verborgen) systeembestanden wel of geen fouten bevatten.

Met de opdracht `sfc /scannow` worden alle beveiligde systeembestanden gescand en beschadigde bestanden vervangen door een kopie die is opgeslagen in de map *c:\windows\System32\dllcache*.

System File Checker tool (SFC.exe)

Voer de test uit:

- Open een command prompt als administrator, typ `CMD` en *uitvoeren als*.
- Geef het commando `SFC /scannow`
- Sluit de prompt niet af tot de test is afgelopen.

Wat is het resultaat?

De System File Checker controleert of de opgeslagen systeembestanden integer zijn. Ook heeft Windows een tool die de MD5- en SHA1-waarden van bestanden kan opvragen en checken.

MD5- en SHA-waarden

Ga naar https://support.microsoft.com/en-us/kb/841290

- Download de tool FCIV (File Checksum Integrity Verifier; het bestand heet *Windows-KB841290-x86-ENU.exe*).
- Maak een map *fciv* op de C-schijf (dat wordt dus *c:\fciv*).
- Dubbelklik op het bestand *Windows-KB841290-x86-ENU.exe*.

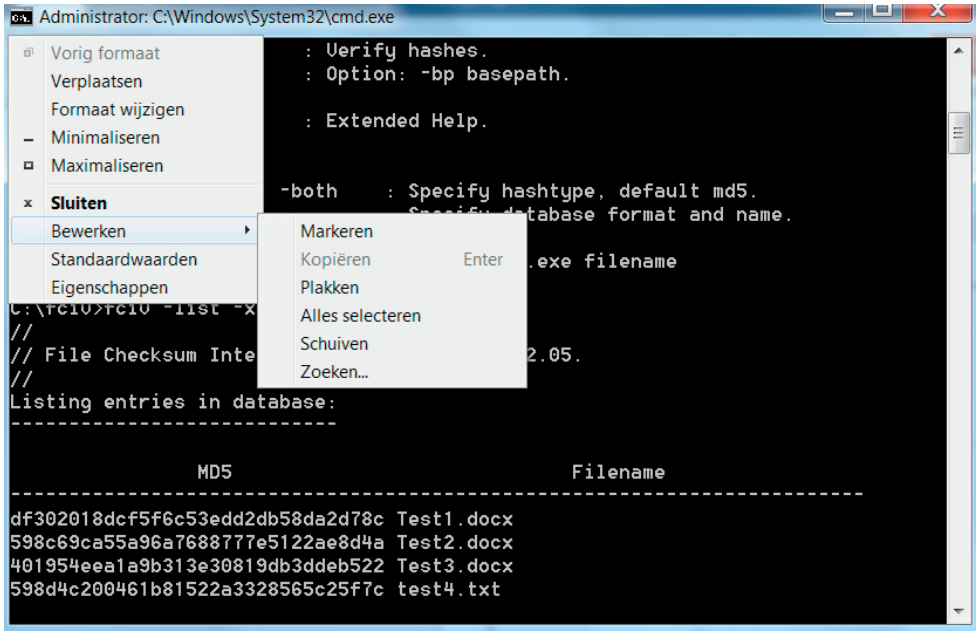
- Klik *Ja* en selecteer dan de map *c:\fciv*
- Klik *OK*.
- Check of in de map *c:\fciv* nu het bestand *fciv.exe* staat.
- Maak een map *c:\docs*.
- Open WinWord en maak vier bestanden: *test1.docx*, *test2.docx*, *test3.docx* en *test4.txt*.
- Plaats de bestanden in de map *c:\docs*.
- In elk document typ je één bestaand woord van niet meer dan 6 letters. Zorg ervoor dat ieder bestand een ander woord bevat.
- Ga naar de command prompt en open deze als administator.
- Geef het commando `c:` – er gebeurt misschien niets.
- Geef het commando `cd\fciv` – je gaat nu naar de map *fciv*.
- Geef het commando *set path=%path%;c:\fciv*
  c:\fciv is hiermee toegevoegd aan het path.
- Geef het commando `set`
  Controleer of je *c:\fciv* aan het einde ziet staan.
- Geef het commando `fciv.exe c:\docs -both -xml db.xml`
  Hiermee voeg je SHA- en MD5-waarden toe aan de database *db.xml*.
- Open nu het bestand *test2.docx*, voeg een paar letters toe aan dit bestand en sla het op.
- Sluit het bestand af.
- Open nu het bestand *test4.txt*, voeg een paar letters toe aan dit bestand en sla het op.
- Sluit het bestand af.
- Geef het commando `fciv.exe -v c:\docs -both -xml db.xml`
  Hiermee controleer je de bestanden.
- Wat is de uitkomst?
- Wijzig nu in deze bestanden de tekst weer terug naar wat het eerder was.
- Geef het commando `fciv.exe -v c:\docs -both -xml db.xml` – controleer de bestanden nogmaals.
- Wat is de uitkomst?

  Je ziet dat het txt-bestand niet meer staat vermeld, de hash-waarden zijn weer gelijk aan de oorspronkelijke waarde.
  Kun je verklaren waarom het txt-bestand weer dezelfde hash-waarde heeft als voorheen, maar het Word-document niet?

Hashkiller

- Ga naar CMD en open deze als administrator.
- Geef het commando `cd\`
- Geef het commando `cd\fciv`
- Geef het commando `fciv -list -xml -db.xml`
- Je krijgt een lijst te zien van de MD5-waarden met de bestandsnamen.
- Klik op het zwarte icoontje linksboven en kies *Bewerken* en dan *Plakken*.

- Selecteer nu met de muis de MD5 van het tekstbestand.
- Klik weer op het zwarte icoontje, kies *Bewerken* en dan *Kopiëren*.



- Ga naar de website https://hashkiller.co.uk/md5-decrypter.aspx
- Plak de MD5-waarde in het linkerscherm, vul onderin de captcha in en klik *Submit*.

Je ziet nu rechts de tekst uit je document staan. Zo niet, dan heb je een niet-bestaand woord of weinig voorkomend woord gekozen. Maak dan een nieuw tekstbestand en plaats daar een simpel woord in (hallo). Bereken de MD5-waarde van dit bestand en probeer nog een keer op de site de inhoud te bepalen door middel van de hash-waarde.

Ook wachtwoorden worden vaak in MD5-waarden opgeslagen. Met deze website kun je eenvoudig kijken of de MD5-waarde in hun database staat. Zo ja... dan is je wachtwoord gehackt.

Kraak deze waarden:

`1CCD6AF4A2CA8D765BA5BE68CAA7C2DD`

`7475E682A5142A3420CCE2287A1F871C`

LET OP: Zorg dat niemand je wachtwoorden ziet!

- Maak een tekstbestandje met je eigen wachtwoord erin.
- Bereken de MD5-waarde (met de MAT-MD5-tool).
- Kijk of deze in de hashkiller-database staat.
- Zo ja, dan is je wachtwoord niet veilig!

LET OP: Verwijder het bestandje met het wachtwoord erin (ook uit de prullenbak).

Integriteit van een schijf

Tijdens langdurig gebruik van een harde schijf kan er veel mis gaan. Je merkt er vaak niet zoveel van, maar je harde schijf kan fouten maken bij het opslaan of verwijderen van mappen en bestanden.

Als je **geen** SSD-schijf hebt:

- Ga naar CMD en open deze als administrator.
- Geef het commando `cd\`
- Geef het commando `chkdsk c:`
  Dit kan even duren.
  Als de check is afgelopen kun je controleren of je fouten in je bestandssysteem hebt staan.
  Als er fouten zijn gevonden, sluit dan al je documenten en ander werk af.
  Geef nu het commando `chkdsk c: /F /R /B` en herstart je computer.
  Na het opstarten wordt je schijf gecontroleerd.

Als je **wel een** SSD-schijf hebt:

- Ga naar CMD en open deze als administrator.
- Geef het commando `cd\`
- Geef het commando `fsutil behavior query DisableDeleteNotify`
  Als het resultaat 0 is wordt je SSD-schijf (automatisch en zonder dat dit zichtbaar is) gecontroleerd.
  Als het resultaat 1 is, geef dan het volgende commando
  `fsutil behavior set disablenotify 0`

De volgende keer als de computer wordt herstart, wordt je SSD-schijf gecheckt.

Practicum 1.3
Beschikbaarheid

In de tabel hieronder zie je de beschikbaarheid van een systeem uitgedrukt in dagen, uren, minuten en secondes. Als je een beschikbaarheid hebt van 90% dan is het systeem van de 100 minuten dat het werkt 10 minuten uit de lucht. Per jaar is het systeem dan 36,5 dag uit de lucht (werkt niet naar behoren), dat is meer dan een maand!

Availability %	Downtime per year	Downtime per month*	Downtime per week
90% ("one nine")	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
97%	10.96 days	21.6 hours	5.04 hours
98%	7.30 days	14.4 hours	3.36 hours
99% ("two nines")	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes
99.9% ("three nines")	8.76 hours	43.8 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% ("four nines")	52.56 minutes	4.32 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds
99.9999% ("six nines")	31.5 seconds	2.59 seconds	0.605 seconds
99.99999% ("seven nines")	3.15 seconds	0.259 seconds	0.0605 seconds

Als de beschikbaarheid 99,99999% is, dan is het systeem per jaar iets meer dan 3 seconden uit de lucht.

Beschikbaarheid wordt vaak uitgedrukt in een aantal negens. Een beschikbaarheid met drie negens betekent 99,9%, het aantal negens geeft een percentage weer. In de tabel zie je het aantal negens en de onbeschikbaarheid. Een uitval van eentiende procent betekent al ruim een werkdag uit de lucht.

Er zitten 24 * 365 = 8760 uren in een jaar. 1% hiervan is 87,6 uur. Een systeem met een beschikbaarheid van 95% mag dus ongepland 438 uur onbeschikbaar zijn. Dit zijn 18 volle dagen per jaar! Het andere uiterste is 99,999%, hierbij mag een systeem slechts 5 minuten per jaar uitvallen (en dat is dus inclusief de reparatie van de storing!). Een beschikbaarheid van 5 negens is de laatste jaren een onuitgesproken standaard geworden.

Een methode om de beschikbaarheid aan te geven is:

Availability = MTBF / (MTBF + MTTR) * 100%

MTBF = mean time between failures. Dit is de gemiddelde tijd tussen twee opeenvolgende momenten van onbeschikbaarheid. Bijvoorbeeld een router valt na vier weken uit, dan na vijf weken, dan na drie weken. De MTBF wordt als volgt berekend: 4 + 5 + 3 = 12 / 3 = 4. De gemiddelde tijd tussen twee tijden van onbeschikbaarheid is 4 weken. Dat is extreem kort: vervangen dat apparaat!

4 weken = 672 uur, en stel dat de reparatie 2 uur kost dan is de berekening als volgt:

Availability = 672 / (672 + 2) * 100% = 99,70%

Als je een afspraak hebt met de leverancier van het apparaat dat de beschikbaarheid minstens 99,99% moet zijn, dan kan de leverancier voor de kosten opdraaien of hij levert een nieuw apparaat.

MTTR = mean time to restore. Dit is de gemiddelde tijd die nodig is om de onbeschikbaarheid ongedaan te maken. Als de router uitvalt, moet deze worden gerepareerd, onbeschikbaarheid betekent vaak dat er mensen niet kunnen werken. Dat is een flinke kostenpost, haast is altijd geboden. Hoe sneller de response, hoe lager de kosten. Als de router drie keer uitvalt, hoe lang duurt het dan gemiddeld om de router weer beschikbaar te maken? De gemiddelde tijd om een apparaat te herstellen (reparatie of vervanging) wordt uitgedrukt in de MTTR.

De MTTR bestaat uit de volgende vijf onderdelen:

1. Detectie van de uitval: hoe lang duurt het voordat de uitval wordt opgemerkt?
2. Notificatie van de uitval: meestal komt op de servicedesk een call binnen van een werknemer, deze wordt geregistreerd. Er wordt bijvoorbeeld en netwerkspecialist ingeschakeld.
3. Response-tijd voor herstel: er gaat wat tijd voorbij voordat de specialist ter plaatse is. Pas als de specialist aanwezig is, kan de reparatie beginnen.
4. De eigenlijke reparatie of restore: de duur van de reparatie of vervanging.
5. Opstarten van een systeem: het in de lucht brengen van het systeem.

In de volgende opdracht bereken je de beschikbaarheid.

Je hebt met leverancier IC-ICT afgesproken dat de servers die zij leveren een serviceniveau van 99,95% hebben. Zij hebben jou 2 servers geleverd, de mailserver MAIL01 en de databaseserver DB01. Beide systemen zijn 24/7 in de lucht. Er zijn meerdere incidenten geweest:

MAIL01

Op de servicedesk is op 9 maart om 11.00 uur 's ochtends gemeld dat de server sinds een half uur niet meer werkt. Onmiddellijk werd aan de leverancier doorgegeven dat het systeem haperde. Het duurde een uur voordat de monteur ter plekke was. Het systeem werd offline gehaald en de netwerkkaart vervangen. De reparatie was intensief (fout kon moeilijk gevonden worden) en duurde een uur. Het systeem werd weer online geplaatst en dit werd aan de servicedesk gemeld. Deze meldde aan iedereen dat het systeem weer werkte, wat nog een half uur in beslag nam.

Op 14 mei om 13.00 uur komt er een bericht op de servicedesk binnen dat de server lijkt te hangen. De monteur wordt gebeld die aan de systeembeheerder vraagt om het systeem te herstarten. De systeembeheerder doet dit en na een half uur werkt het systeem weer. De servicedesk meldt dit aan de organisatie en na een half uur kan iedereen weer werken.

Tenslotte hapert het systeem weer op 20 november om 14.00 uur. Het lijkt in de lucht te zijn, maar niemand kan er goed bij. Na een uur van klachten belt de servicedesk de monteur. Deze is na een half uur ter plekke en constateert dat de systeemschijf van de server geen vrije ruimte meer heeft. Hij belt met systeembeheer en zij komen overeen dat de monteur een aantal zeer grote logbestanden kan verwijderen, wat ongeveer 20% van de schijf opschoont. De gehele operatie kost drie uur. De server werkt daarna weer goed en dat wordt aan de servicedesk gemeld. Na een half uur is in de gehele organisatie bekend dat de server weer werkt.

De ICT-manager heeft zijn twijfels of de server het afgesproken service level van 99,95% wel heeft gehaald en vraagt jou de beschikbaarheid te berekenen.

Jij berekent de MTBF en de MTTR.

- Wat is de beschikbaarheid?
- Hoeveel is dat per jaar, per week en per werkdag?
- Wat adviseer jij vanuit security-oogpunt (beschikbaarheid)?

MTBF berekenen

Je kunt hier het aantal *uren* berekenen:
http://www.kalender-365.nl/bereken/periode-tussen-twee-datums.html

Wat is het aantal uren tussen 9 maart 2016 (11.00 uur) en 14 mei 2016 (13.00 uur)?

Het verschil blijkt 1583 uur te zijn. Hier tellen we 2 uur bij op (verschil tussen 11 en 13 uur), wordt 1585 uur.

Wat is het aantal uren tussen 14 mei 2016 (13.00 uur) en 20 november 2016 (17.00 uur)?

Het verschil blijkt 4561 uur te zijn. Hier tellen we 4 uur bij op (verschil tussen 13 en 17 uur), wordt 4565 uur.

Nu berekenen we het gemiddelde: (1585 + 4565) / 2 = 3075 uur

MTBF = 3075 uur

MTTR berekenen

Bij het eerste incident: Time to Repair = een half uur + een uur + een uur + een half uur = 3 uur

Bij het tweede incident: Time to Repair: half uur + half uur = 1 uur

Bij het derde incident: Time to Repair: een uur + half uur + 3 uur + half uur = 5 uur

MTTR = (3 + 1 + 5) / 3 = 3 uur

De beschikbaarheid is MTBF / (MTBF + MTTR) * 100% = 3075 / (3075+3) = 0,9990 * 100% = **99,90%**

De beschikbaarheid voldoet niet. Je kunt in de tabel aan het begin van dit practicum zien wat de downtime van het systeem per maand en per week is bij een beschikbaarheid van 99,9%.

Waar zou jij het proces verbeteren?

Bereken de beschikbaarheid van de DB01-server

Op 12 januari 2016 om 9.00 uur in de ochtend wordt een melding gemaakt dat de DB01-server niet bereikbaar is. Het duurt een uur (vanwege een vergadering) dat dit een aan monteur gemeld wordt. De monteur is met een half uur ter plekke en begint de reparatie. Het blijkt dat de monteur niet de juiste onderdelen (RAM-geheugenmodule is corrupt) bij zich heeft en laat deze leveren door een koerier. Dit duurt een uur. De verdere reparatie duurt nog eens anderhalf uur en dan meldt de monteur dat de server weer werkt. De servicedeskmedewerker meldt aan de organisatie dat de server weer online is, dit duurt 30 minuten.

Op 18 juni 2016 om 12.00 uur blijken de data op de DB01-server niet meer toegankelijk. Een half uur na de melding is de monteur ter plekke. De RAID-controller van de server heeft het begeven waardoor de schijven niet meer bereikbaar zijn. De vervanging en het herstarten van de RAID-controller duurt zo'n 2 uur. Na weer een half uur kan iedereen weer werken.

Op 14 december 2016 om 13.00 uur begint de DB01 spontaan te herstarten en blijft dit doen. De systeembeheerder had een driver geüpdatet van een moederbordonderdeel. Deze bleek voor de problemen te zorgen. Er werd snel een herinstallatie ingezet en een uur na de melding was iedereen weer normaal aan het werk.

Bereken de beschikbaarheid van dit systeem en rapporteer of het voldoet aan de afgesproken norm van 99,95%.

Welke maatregelen tref je om de bovenstaande problemen te voorkomen?

Practicum 2.1
De Grondwet

In Nederland kennen we de Grondwet. In de Grondwet staat precies beschreven wat Nederlanders wel en niet mogen doen, oftewel waar zij recht op hebben of wat verplicht is. De Grondwet bestaat uit een hele reeks artikelen waarvan je er straks een paar gaat bespreken. Met de Grondwet als basis worden in Nederland allerlei wetten geschreven. Onthoud dus goed dat wetten altijd gebaseerd zijn op de Grondwet. De Nederlandse Grondwet begint met de volgende tekst.

> De Grondwet is het belangrijkste staatsdocument van Nederland. Zij bevat de fundamentele regels voor onze staatsinrichting en legt tevens de grondrechten van de burgers vast. De Grondwet is de hoogste nationale wet voor de Nederlandse staat; andere wetten dienen haar bepalingen in acht te nemen.

Opdracht 1 De Grondwet

Werk voor dit practicum in groepen van twee. Bespreek de Grondwetsartikelen 1 tot en met 13. Bespreek en beschrijf wat de eerste dertien artikelen inhouden.

Geef voor alle Grondwetsartikelen een voorbeeld waarop jullie denken dat deze wet van toepassing is. Als voorbeeld zijn artikel 1 en 2 al ingevuld. Noteer jullie voorbeelden in een document.

Artikel 1. Gelijke behandeling en discriminatieverbod

Allen die zich in Nederland bevinden, worden in gelijke gevallen gelijk behandeld. Discriminatie wegens godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht of op welke grond dan ook, is niet toegestaan.

Vragen
Welk grondrecht wordt hier beschermd?
Voor wie geldt dit grondrecht?
Hebben jullie wel eens te maken gehad met dit artikel in je eigen leven?

Voorbeeld
1. Je mag iemand geen baan weigeren omdat hij of zij homofiel is.
2. Vrouwen moeten net zoveel verdienen als mannen in een gelijke baan.

Artikel 2. Nederlanderschap; vreemdeling; uitlevering; recht tot verlaten van land

1. De wet regelt wie Nederlander is.
2. De wet regelt de toelating en de uitzetting van vreemdelingen.
3. Uitlevering kan slechts geschieden krachtens verdrag. Verdere voorschriften omtrent uitlevering worden bij de wet gegeven.
4. Ieder heeft het recht het land te verlaten, behoudens in de gevallen, bij de wet bepaald.

Vragen
Welk grondrecht wordt hier beschermd?
Voor wie geldt dit grondrecht?
Hebben jullie wel eens te maken gehad met dit artikel in je eigen leven?

Voorbeeld
1. Je mag zonder toestemming altijd op vakantie (het land uit).
2. Asielzoekers mogen hier asiel aanvragen en moeten geholpen worden.

Artikel 3. Gelijke benoembaarheid

Alle Nederlanders zijn op gelijke voet in openbare dienst benoembaar.

Vragen
Welk grondrecht wordt hier beschermd?
Voor wie geldt dit grondrecht?
Hebben jullie wel eens te maken gehad met dit artikel in je eigen leven?

Voorbeeld
1.
2.

Artikel 4. Kiesrecht

Iedere Nederlander heeft gelijkelijk recht de leden van algemeen vertegenwoordigende organen te verkiezen alsmede tot lid van deze organen te worden verkozen, behoudens bij de wet gestelde beperkingen en uitzonderingen.

Vragen
Welk grondrecht wordt hier beschermd?
Voor wie geldt dit grondrecht?
Hebben jullie wel eens te maken gehad met dit artikel in je eigen leven?

Voorbeeld
1.
2.

Artikel 5. Petitierecht

Ieder heeft het recht verzoeken schriftelijk bij het bevoegd gezag in te dienen.

Vragen
Welk grondrecht wordt hier beschermd?
Voor wie geldt dit grondrecht?
Hebben jullie wel eens te maken gehad met dit artikel in je eigen leven?

Voorbeeld
1.
2.

Artikel 6. Vrijheid van godsdienst en levensovertuiging

1. Ieder heeft het recht zijn godsdienst of levensovertuiging, individueel of in gemeenschap met anderen, vrij te belijden, behoudens ieders verantwoordelijkheid volgens de wet.
2. De wet kan ter zake van de uitoefening van dit recht buiten gebouwen en besloten plaatsen regels stellen ter bescherming van de gezondheid, in het belang van het verkeer en ter bestrijding of voorkoming van wanordelijkheden.

Vragen
Welk grondrecht wordt hier beschermd?
Voor wie geldt dit grondrecht?
Hebben jullie wel eens te maken gehad met dit artikel in je eigen leven?

Voorbeeld
1.
2.

Artikel 7. Vrijheid van meningsuiting; censuurverbod

1. Niemand heeft voorafgaand verlof nodig om door de drukpers gedachten of gevoelens te openbaren, behoudens ieders verantwoordelijkheid volgens de wet.
2. De wet stelt regels omtrent radio en televisie. Er is geen voorafgaand toezicht op de inhoud van een radio- of televisieuitzending.
3. Voor het openbaren van gedachten of gevoelens door andere dan in de voorgaande genoemde middelen heeft niemand voorafgaand verlof nodig wegens de inhoud daarvan, behoudens ieders verantwoordelijkheid volgens de wet. De wet kan het geven van vertoningen toegankelijk voor personen jonger dan zestien jaar regelen ter bescherming van de goede zeden.
4. De voorgaande leden zijn niet van toepassing op het maken van handelsreclame.

Vragen
Welk grondrecht wordt hier beschermd?
Voor wie geldt dit grondrecht?
Hebben jullie wel eens te maken gehad met dit artikel in je eigen leven?

Voorbeeld **1.**
2.

Artikel 8. Vrijheid van vereniging

Het recht tot vereniging wordt erkend. Bij de wet kan dit recht worden beperkt in het belang van de openbare orde.

Vragen Welk grondrecht wordt hier beschermd?
Voor wie geldt dit grondrecht?
Hebben jullie wel eens te maken gehad met dit artikel in je eigen leven?

Voorbeeld **1.**
2.

Artikel 9. Vrijheid van vergadering en betoging

1. Het recht tot vergadering en betoging wordt erkend, behoudens ieders verantwoordelijkheid volgens de wet.
2. De wet kan regels stellen ter bescherming van de gezondheid, in het belang van het verkeer en ter bestrijding of voorkoming van wanordelijkheden.

Vragen Welk grondrecht wordt hier beschermd?
Voor wie geldt dit grondrecht?
Hebben jullie wel eens te maken gehad met dit artikel in je eigen leven?

Voorbeeld **1.**
2.

Artikel 10. Privacy

1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

Vragen Welk grondrecht wordt hier beschermd?
Voor wie geldt dit grondrecht?
Hebben jullie wel eens te maken gehad met dit artikel in je eigen leven?

Voorbeeld **1.**
2.

Artikel 11. Onaantastbaarheid lichaam

Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op onaantastbaarheid van zijn lichaam.

Vragen Welk grondrecht wordt hier beschermd?
Voor wie geldt dit grondrecht?
Hebben jullie wel eens te maken gehad met dit artikel in je eigen leven?

Voorbeeld **1.**
2.

12. Huisrecht

1. Het binnentreden in een woning zonder toestemming van de bewoner is alleen geoorloofd in de gevallen bij of krachtens de wet bepaald, door hen die daartoe bij of krachtens de wet zijn aangewezen.
2. Voor het binnentreden overeenkomstig het eerste lid zijn voorafgaande legitimatie en mededeling van het doel van het binnentreden vereist, behoudens bij de wet gestelde uitzonderingen.
3. Aan de bewoner wordt zo spoedig mogelijk een schriftelijk verslag van het binnentreden verstrekt. Indien het binnentreden in het belang van de nationale veiligheid of dat van de strafvordering heeft plaatsgevonden, kan volgens bij de wet te stellen regels de verstrekking van het verslag worden uitgesteld. In de bij de wet te bepalen gevallen kan de verstrekking achterwege worden gelaten, indien het belang van de nationale veiligheid zich tegen verstrekking blijvend verzet.

Vragen Welk grondrecht wordt hier beschermd?
Voor wie geldt dit grondrecht?
Hebben jullie wel eens te maken gehad met dit artikel in je eigen leven?

Voorbeeld **1.**
2.

13. Briefgeheim

1. Het briefgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, op last van de rechter.
2. Het telefoon- en telegraafgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.

Vragen Welk grondrecht wordt hier beschermd?
Voor wie geldt dit grondrecht?
Hebben jullie wel eens te maken gehad met dit artikel in je eigen leven?

Voorbeeld **1.**
2.

Opdracht 2 Grondwetswijziging

Hieronder zie je het stappenplan voor wijziging van de Grondwet.

Een Grondwetswijziging doorloopt 7 stappen:

1 De regering of een of meer leden van de Tweede Kamer dienen een voorstel tot Grondwetswijziging in.
2 De Tweede en Eerste Kamer nemen dit wetsvoorstel in 1e lezing aan met een gewone meerderheid. Dit heet ook wel de 'overwegingswet' of de 'verklaringswet'.
3 De Tweede Kamer wordt ontbonden en er worden verkiezingen gehouden. Hierdoor kunnen kiezers zich over de wijzigingen uitspreken.
4 Het in 1e lezing aangenomen voorstel wordt ingediend bij de nieuwe Tweede Kamer.
5 De Tweede en Eerste Kamer nemen het wetsvoorstel in 2e lezing aan met een 2/3 meerderheid.
6 Het het wetsvoorstel wordt ondertekend door de koning en een of meer ministers of staatssecretarissen.
7 De wijziging wordt gepubliceerd in het Staatsblad. De wijziging treedt daarna direct in werking.

Bezoek de website http://www.denederlandsegrondwet.nl, klik in het menu op het item "actueel".

Je ziet nu een lijst van Grondwetswijzigingen in hun verschillende fases.

In welke fase bevindt zich het Grondwetsartikel met betrekking tot het briefgeheim (artikel 13)?

Wat houdt dit voorstel in? Met andere woorden, beschrijf waarom de regering wil dat Grondwetsartikel 13 moet worden aangepast.

Kun je drie punten noemen waar de wijziging van dit Grondwetsartikel het werk van een security officer kan beïnvloeden?

De meldplicht datalekken

Bekijk de volgende twee video's met betrekking tot datalekken:
https://www.youtube.com/watch?v=fhcqMyIfEWg
https://www.youtube.com/watch?v=k4AOFLxvyYo

Lees de onderstaande pagina:
https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

Maak een PowerPoint-presentatie over het belang van de wet Datalekken. In de PowerPoint leg je uit:

- Wanneer de wet van toepassing is.
- Wanneer de wet ingaat.
- Wat een datalek is.
- Wat de boete is bij het niet melden.
- Hoe je een datalek kunt melden.

Practicum 2.2
WhatsApp

In jouw bedrijf wordt al minstens 2 jaar gebruik gemaakt van WhatsApp als communicatie-tool.

Het begon ooit met het uitwisselen van felicitaties en gelukwensen tussen personeel onderling. Al snel werd de tool ontdekt als middel om klanten op de hoogte te houden van de status van hun product. Vooral jonge klanten vinden het gebruik van WhatsApp een grote plus. Steeds meer basisschoolleerlingen hebben een mobiel en het bedrijf communiceert graag direct met de jonge klanten.

De procedure is als volgt:

Wij sturen de ouders een code. Zij sturen ons het telefoonnummer van hun kind. Wij zoeken vervolgens contact via WhatsApp met het kind en vragen om de code die we de ouders hebben toegestuurd. Alleen op deze wijze kunnen de scholieren vragen aan ons stellen over het platform.

Onze diensten bestaan uit het op een leuke manier leren rekenen en het stimuleren van de taalvaardigheid. De doelgroep bestaat uit basisscholieren van groep 3 tot groep 7.

Vraag 1

WhatsApp garandeert dat het de verstuurde berichten **nooit** opslaat. Alleen de zender en ontvanger kunnen het bericht lezen. Maar er is wel commotie ontstaan rond WhatsApp-versleuteling van berichten en het koppelen aan Facebook-accounts (WhatsApp is eigendom van Facebook).

Enkele verontruste ouders hebben contact gezocht met de servicedesk en met de directie van de scholen. De vraag is wat de wijzigingen in het WhatsApp-beleid eigenlijk zijn en welke gevolgen deze hebben. Jij gaat op onderzoek uit:

- Wat betekent het dat de WhatsApp-data versleuteld zijn?
- Op welke wijze zijn de data versleuteld?
- Wat betekent de koppeling aan de Facebook-gegevens voor de privacy?
- Vind je dat politie en justitie wel over de sleutels van encryptie mogen beschikken? Dan kunnen zij de WhatsApp-gegevens van verdachten lezen.

  Zo ja, waarom?

  Zo nee, waarom niet?
- Waar worden de berichten van WhatsApp bewaard? (Je kunt tenslotte de geschiedenis opvragen.)

Breng een advies uit over het gebruik van WhatsApp in jouw bedrijf. Vind je de WhatsApp-mogelijkheden voor kinderen een geschikte vorm van communiceren?

Licht je antwoord toe.

Referenties

http://www.nu.nl/apps/4312149/whatsapp-zet-deur-open-bedrijven.html
https://www.whatsapp.com/legal/#terms-of-service
https://ddma.nl/wp-content/uploads/2016/05/WhatsApp-Hoe-heurt-het-eigenlijk-versie-def-1.pdf
http://blog.iusmentis.com/2015/10/28/de-legaliteit-van-whatsapp-voor-je-klanten-service/
https://www.whatsapp.com/security/
https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

Vraag 2

Onlangs kwam in het nieuws dat artsen vaak via WhatsApp informatie uitwisselen over patiënten. Het bleek een goede en snelle manier van communiceren waarbij heel wat patiënten waren geholpen.
Vind je dat dit mag? Licht je antwoord toe.

Lees deze pagina goed door:
https://www.knmg.nl/actualiteit-opinie/nieuws/nieuwsbericht/knmg-artsenpanel-whatsapp-is-waardevol-maar-beveiliging-een-must.htm

Practicum 3-1
Zeroday-bescherming via een group policy

EMET in een group policy opnemen

Tijdens je technische lessen, Windows of netwerken, heb je te maken gehad met groepsbeleid. Het is een manier om via gebruikersgroepen op de Active Directory Server instellingen naar alle computers te sturen. In dit practicum stel je een policy samen die EMET voor alle gebruikers op dezelfde wijze instelt.

Om EMET te kunnen toepassen moet de tool op alle workstations zijn geïnstalleerd. In dit voorbeeld gebruiken we Windows 7 om de configuratie van EMET te tonen. Je hebt gpedit.msc nodig om de configuratie in te stellen Deze wordt niet standaard geleverd bij Windows 10 Home editie, die je wellicht hebt geïnstalleerd.

In Windows 10 Home: ga je naar de command prompt en typ je:

CD\ + enter
DIR GPEDIT.MSC /S + enter

Je ziet een versie van gpedit.msc op je harde schijf. Blader naar dit bestand met de Verkenner en kopieer het naar de map *c:\windows* en *c:\windows\sytem32*.

Je kunt nu wel gpedit.msc starten

Download de laatste versie van EMET van de Microsoft-site en installeer de tool op je computer.

Je kunt de vraag krijgen om .NET Framework te installeren. Klik ja.

Na de installatie voer je de volgende stappen uit:

Ga naar de map *c:\Program Files\EMET\Deployment\Group Policy Files*.

Kopieer het bestand EMET.admx naar *c:\Windows\PolicyDefinitions*.

Kopieer het bestand EMET.adml naar *c:\Windows\PolicyDefinitions\en-US*.

Open nu GPEDIT.MSC en blader naar: *Computer Configuration\Administrative Template\Windows Components\EMET GPO*

In het Nederlands is dit: *\computer configuratie\beheersjablonen\windowsonderdelen\EMET*

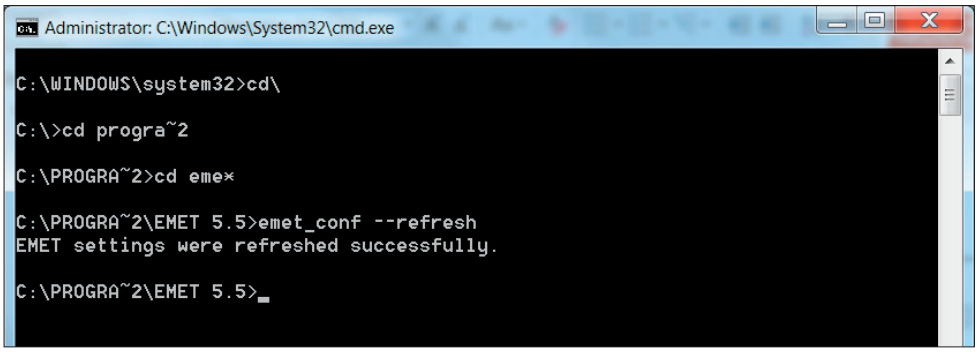
Nu kun je de EMET-instellingen aanpassen.

Stel in dat:

- Het EMET-icoon niet langer zichtbaar is na het opstarten.
- EMET Windows Internet Explorer beschermt.

– EMET alle aanbevolen programma's beschermt.
  Klik *OK*.

Ga als administrator naar een command prompt en geef de volgende commando's:



Als je nu je computer herstart zjn de EMET-instellingen van toepassing.

Indien je deze stappen uitvoert op een domain controller kun je de EMET-settings eenvoudig opnemen in het groepsbeleid. Je **moet** op alle computers het bovenstaande refresh-commando geven.

Practicum 3-2
Leegmaken gevensdragers

WIPE – hoe een schijf volledig leeg te maken

Plaats een (gebruikte) USB-stick in je computer. Zorg ervoor dat er **geen** belangrijke bestanden op staan.

A **Delete** alle bestanden op de USB-stick. Zijn de bestanden echt weg?

We gaan de USB stick 'low level' bekijken, wat betekent dat we naar de schijf gaan kijken zoals het OS de stick ziet.

Download de Engelse of Nederlandse HxD en plaats deze in je Tool-map. We gebruiken hier de Engelse versie. De tool werkt onder alle versies van Windows™.

https://mh-nexus.de/en/downloads.php?product=HxD

LET OP: Met deze tool kun je eenvoudig je hele systeem om zeep helpen!

Pak de tool uit en installeer deze op je harde schijf.

Start de tool als administrator.

Kies in het menu *Extra* > *Open disk*.

Selecteer de *Removable Disk* (je USB-stick).

Zorg ervoor dat *Read only* is aangevinkt en klik *OK*.

Check of de USB-stick echt leeg is.

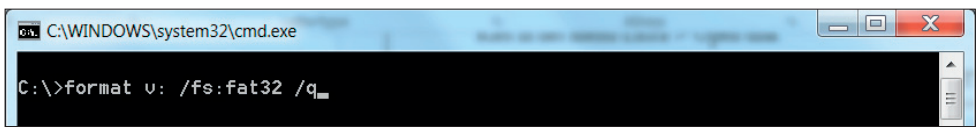
Blader door de sectoren (hoeveel zijn het er?) en controleer of de USB-stick leeg is.

Sluit de tool af.

B We gaan nu **formatteren**.

Ga naar een command prompt (typ *cmd*) en open deze als administrator en geef het commando dat hieronder staat.

V: staat voor de drive-letter van de USB-stick – dus **let op:** verander de V in de driveletter van jouw USB.



Check de drive-letter van je stick en formatteer je USB-stick.

/FS:FAT32 formatteer de schijf naar FAT32.
/Q voer een quick format uit.

Blader nogmaals met HxD door de sectoren (hoeveel zijn het er ?) en controleer of de USB-stick leeg is.

Start de tool als administrator.
Kies in het menu *Extra* > *Open disk*.
Selecteer de *Removable Disk* (je USB-stick).
Zorg ervoor dat er een vinkje staat bij *Readonly* en klik *OK*.
Check of de USB-stick echt leeg is.
Blader door de sectoren en controleer of ze leeg zijn.
Controleer sector 32 en sector 38 – zijn deze leeg?

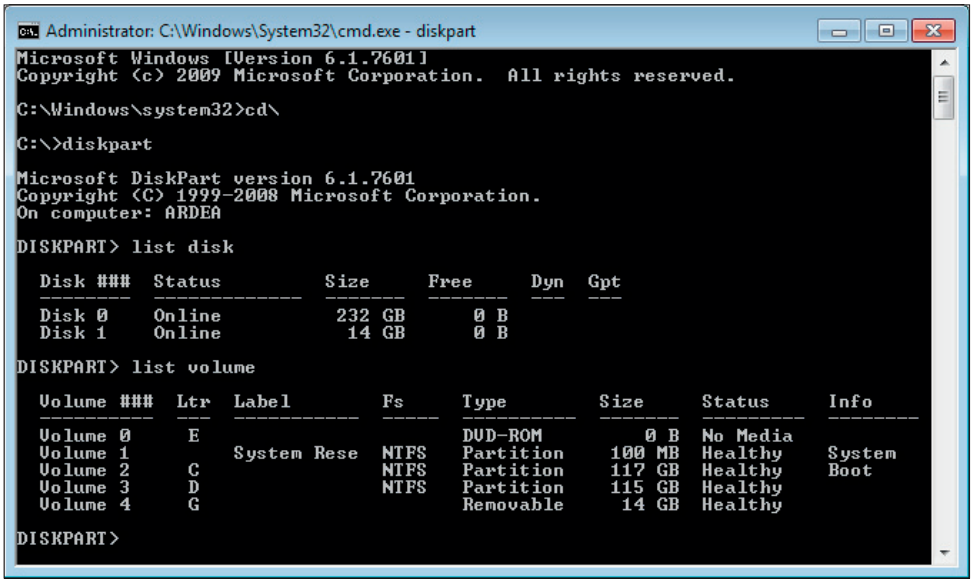
C We gaan de schijf nu **wipen**. We maken gebruik van een andere tool, namelijk **DiskPart**. Ook hier is van groot belang de onderstaande stappen **zorgvuldig** uit te voeren. DiskPart is een standaard-tool onder Windows™ waarmee schijfbewerkingen kunnen worden uitgevoerd.

Sluit de USB-stick aan op je computer (denk eraan: *echt alles gaat verloren!*).

Plaats een tekstbestandje op de USB-stick met je naam erin. Noem dit bestandje *test.txt*.

Ga naar een cmd-prompt en voer dit uit als *administrator.*
Voer het volgende uit en geef na alle commando's een Enter.

Typ cd\ je bent in *c:*\>.
Typ diskpart je bent nu in *diskpart:*\>; dit betekent dat al je commando's nu door DiskPart worden uitgevoerd.
Typ list disk je krijgt een overzicht van je schijven.
Typ list volume je krijgt een overzicht van je volumes.



We selecteren nu de USB. Je ziet dat dit in het 'disk'-lijstje Disk 1 is (14 GB). Om vergissingen te voorkomen heb je het 'volume'-lijstje opgevraagd, waar je naast de grootte ook de letter kunt zien en onder type 'removable' ziet staan.

LET OP! We selecteren nu het juiste volume waarmee we gaan werken.

Typ select volume 4 **Let op:** dit is bij jou wellicht een *ander getal*!
Typ list volume Je ziet dat er voor de USB-stick een *sterretje* is verschenen.

```
DISKPART> select volume 4

Volume 4 is the selected volume.

DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     E                       DVD-ROM         0 B  No Media
  Volume 1         System Rese  NTFS   Partition    100 MB  Healthy    System
  Volume 2     C                NTFS   Partition    117 GB  Healthy    Boot
  Volume 3     D                NTFS   Partition    115 GB  Healthy
* Volume 4     G                FAT32  Removable     14 GB  Healthy

DISKPART>
```

LET OP! Nu maken we de gehele USB leeg, alle informatie gaat verloren en er is geen mogelijkheid die terug te halen.

Typ clean all Alle informatie wordt nu van de stick verwijderd.

Afhankelijk van de grootte en de snelheid van de USB-stick kan dit enige tijd in beslag nemen (ongeveer 1 minuut per GB).

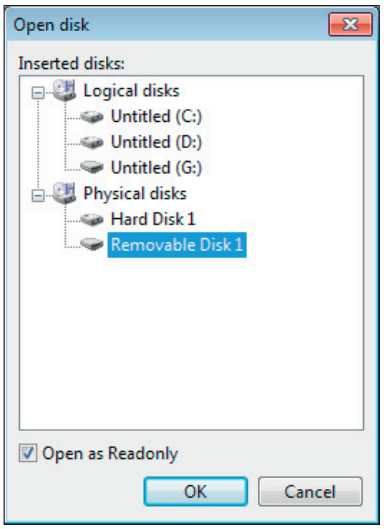
Na een tijdje verschijnt de volgende boodschap:

```
DISKPART> clean all

DiskPart succeeded in cleaning the disk.

DISKPART>
```

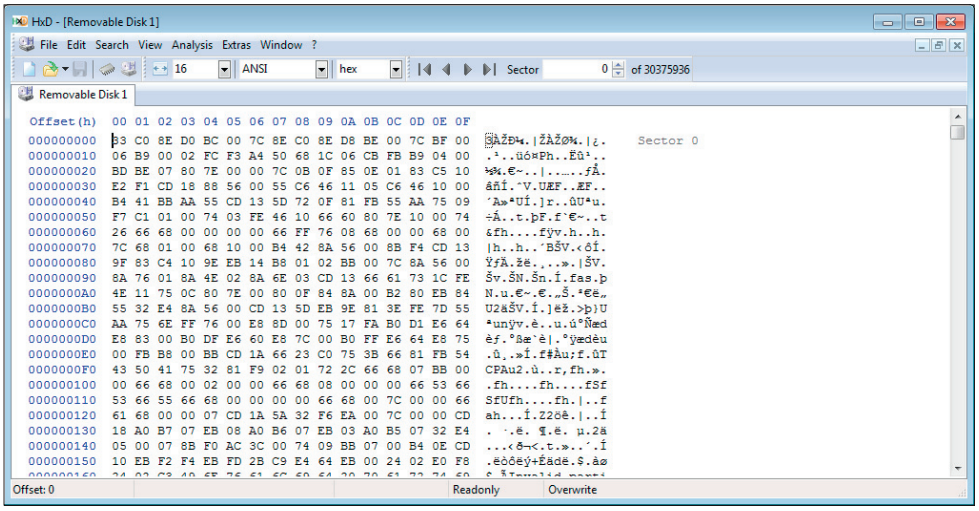
Ga naar de Verkenner en check je schijf. Je zult bemerken dat dit niet meer mogelijk is. De stick bevat geen informatie meer waardoor de schijf onleesbaar is geworden. Hoe leeg is de schijf nu eigenlijk?

We bekijken de USB-stick weer met HxD.

Start de tool als administrator.
Kies in het menu *Extra > Open disk*.
Selecteer de *Removable Disk* (je USB-stick).
Zorg ervoor dat er een vinke staat bij *Readonly* en klik *OK*.



Je krijgt ongeveer het volgende te zien:



Als je verder scrollt dan zie je dat **alle** sectoren (in dit voorbeeld meer dan 30 miljoen, oftewel een USB-stick van 16 GB) leeg zijn. Dit betekent dat op de eerste sector na de USB-stick volledig leeg is gemaakt.

Practicum 3-3
Update-checker

Flexera – personal software inspector

Een van de allerbelangrijkste beveiligingsmaatregelen is erop toezien dat van alle programma's en het besturingssysteem de laatste versie is geïnstalleerd. In ieder beleidsdocument ten behoeve van security neemt dit een belangrijke plaats in.

Microsoft voorziet in automatische updates via de update-service, maar die moet dan wel gestart zijn. Om in beeld te krijgen welke update-services op jouw systeem actief zijn doe je het volgende:

Open Powershell en geef het volgende commando:

```
Get-Service | where-object {$_.name -like '*update*'}
```

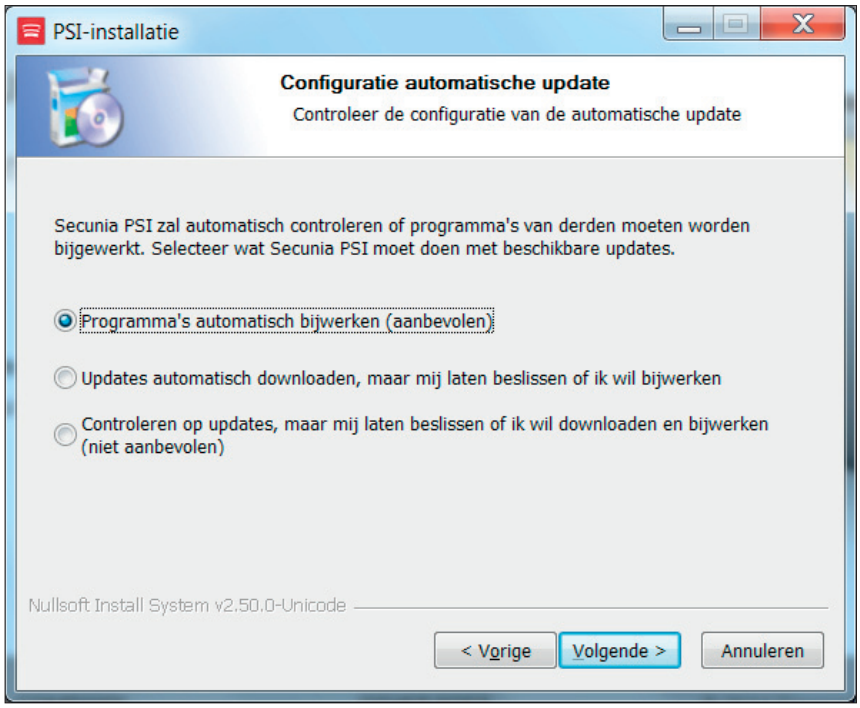
Je krijgt een lijst(je) te zien welke update-services actief zijn op jouw computer. Hieronder de lijst van een willekeurige computer van een docent.

```
Status   Name               DisplayName
------   ----               -----------
Stopped  AdobeFlashPlaye... Adobe Flash Player Update Service
Running  AviraUpdaterSer... Avira Updater Service
Stopped  dbupdate           Dropbox-update-service (dbupdate)
Stopped  dbupdatem          Dropbox-update-service (dbupdatem)
Stopped  gupdate            Google Update-service (gupdate)
Stopped  gupdatem           Google Update-service (gupdatem)
Stopped  scupdate           Scout Update-service (scupdate)
Stopped  scupdatem          Scout Update-service (scupdatem)
Running  Secunia Update ... Secunia Update Agent
Stopped  SkypeUpdate        Skype Updater
```

Vel van de services zijn gestopt, deze worden alleen gebruikt als er een update beschikbaar is. Dit spaart systeembronnen. Wist je dat je deze update-services had geïnstalleerd?

Om inzicht te krijgen welke programma's moeten worden geüpdatet, maken we gebruik van de gratis Personal Software Inspector van Flexera. Je kunt het programma via de volgende link downloaden:
http://mbosecurity.nl/2016/11/23/flexera-personal-software-inspector/

Na het downloaden het bestand PSISETUP.REN hernoemen we dit in PSISETUP.EXE.
Na het downloaden kun je de installatie starten, er is een scherm waar je een keuze dient te maken (wijzig daar niets).



Afhankelijk van het securitybeleid in je bedrijf kan je hier een keuze maken. Wij laten de standaard staan (zie hierboven).

Bij een eventuele vraag over Microsoft-update klik je op *nee*. Krijg je die vraag niet, doorklikken en de scan meteen uitvoeren. Je ziet meteen welke programma's op jouw computer een update nodig hebben.

Voordat je alle updates gaat uitvoeren, moet je je er wel van bewust zijn dat bij meer onbekende programma's juist via de updates malware kan binnenkomen. Dat is ook de reden waarom binnen bedrijven updates *niet* volledig automatisch worden uitgevoerd.

Zoek voordat je gaat updaten goed uit of er kwetsbaarheden in de update voor-

komen. Hierboven zie je in het screenshot een tool staan die Kain en Abel heet. Dit is een verouderde en notoire hackerstool. Dit is een voorbeeld van een tool die je niet zonder meer moet updaten.

Zoek op het internet naar kwetsbaarheden van gevonden programma's op jouw computer. Stel de onderstaande tabel op en vul de rijen met data over jouw programma's.

Tip: Zoek bijvoorbeeld naar: quicktime player vulnerability. Je kunt de naam van een programma combineren met termen als risk of threat.

Programma	**Wijze van update**	**Mogelijke kwetsbaarheden**	**Wel/niet automatisch updaten**
Quicktime player	Volledig automatisch	Ja, aangeraden wordt de QT player volledig te verwijderen!	Nee
OpenSSL 1.x	Verwijst naar een pagina. Dan downloaden en zelf installeren	Ja, op 10 november is er een security-update uitgebracht	Niet mogelijk

Maak je eigen tabel met (minimaal 10) programma's en de wijze van updaten. Als je geen 10 programma's hebt om bij te werken, bekijk dan de lijst van wel up-to-date programma's en kies een aantal voor verder onderzoek.

Je kunt na het practicum de PSI op je computer laten staan of deïnstalleren.

Practicum 4
Return on Security Investment uitrekenen

Binnen een bedrijf zal het management willen weten wat de kosten zijn van beveiligingsmaatregelen. Welke investering moet er gebeuren? Hoe lang duurt het voordat de maatregelen zichzelf hebben terugverdiend?

Uitgangspunt is dat je begrijpt wat met ALE wordt bedoeld. Dit is het verlies per jaar bij een bepaald incident. Kun jij je manager ervan overtuigen dat een investering in security zichzelf terugverdient? En zo ja, hoe bereken je dit?

Security op zich kun je verkopen of in de etalage zetten, het is een kostenpost waarvan niet zo snel duidelijk is hoe dit terugverdiend kan worden. De ROSI (Return on Security Investment) is een getal waarin wordt uitgedrukt hoe goede beveiliging winst kan opleveren.

De kosten voor de beveiligingsmaatregelen worden als volgt berekend:

De eenmalige kosten van de investering in maatregelen (K_{inv})
De *jaarlijkse* kosten van het beheer en onderhoud (K_{jaar})
ALE_{oud} = Annual Loss Expectancy vóór de maatregelen
ALE_{nieuw} = Annual Loss Expectancy ná de maatregelen

We gaan ervan uit dat een investering gedaan wordt voor een periode van *3 jaar*. Als de security-maatregelen goed hebben gewerkt, zijn de kosten na de maatregelen lager dan ervoor.

De formule: $ROSI = ((ALE_{oud} - ALE_{nieuw}) * J - (K_{inv} + K_{jaar} * J)) / (K_{inv} + K_{jaar} * J)$

In het kort: ROSI = (Voordelen minus Kosten) / Kosten

Casus 1 De malware-scanner

De directeur van jouw bedrijf heeft je gevraagd een malware-scanner aan te schaffen voor alle computers en servers.

Je hebt een goed product gevonden, waarvoor je jaarlijks een licentieverlenging koopt. De updates zijn verder gratis.

Na een gesprek met de incident-manager van jouw bedrijf blijkt dat de afgelopen jaren gemiddeld voor 16.000 euro schade is aangericht door malware in het netwerk.

Je schaft de malware-scanner-software aan voor 4000 euro. De scanners kosten verder voor beheer en licenties 1000 euro per jaar. De software wordt voor drie jaar aangeschaft. Uit onderzoek blijkt dat bij vergelijkbare bedrijven de kosten voor malware met 75% afnemen.

Vraag aan jou: is dit een goede deal?

De berekening met de formule:
ROSI= $((ALE_{oud} - ALE_{nieuw}) * J - (K_{inv} + K_{jaar} * J)) / (K_{inv} + K_{jaar} * J)$

ALE_{oud} = 16.000 euro, de jaarlijkse verwachte verlieskosten op basis van de afgelopen jaren
ALE_{nieuw} = 75% afname van 16.000 euro = 4.000 euro jaarlijkse verlieskosten, na gebruik van de scanner
J = 3, het aantal jaren dat de investering duurt
K_{inv} = 4.000 euro, dit zijn de eenmalige kosten
K_{jaar} = 1.000 euro per jaar terugkerende kosten

In de formule:

ROSI= ((16.000 - 4.000) * 3 - (4.000 + 1.000 * 3)) / (4.000 + 1.000 * 3) =

(12.000 * 3 - 7.000) / (7.000) = (36.000 - 7. 000) / 7.000 = 4,1
oftewel een winst van 410%

ROSI = (Voordelen - Kosten) / Kosten = (36.000 - 7.000) / 7.000 = 410%

Casus 2 De hackers

De kosten veroorzaakt door hackers en andere ellende vanaf het internet zijn 24.000 euro per jaar. Dit is de **ALE_{oud}**. Door de security manager wordt gevraagd of hij een aantal firewalls kan plaatsen (beveiligingsmaatregelen) voor een bedrag van 27.000 euro totaal. De firewalls werken voor een periode van 3 jaar. Het beheer van de apparaten kost 2.000 euro per jaar. Het blijkt dat door de maatregelen de kosten van de hackers hierna nog maar 8.000 euro waren. Dit is de **ALE_{nieuw}**.

De opbrengst is ALE_{oud} - ALE_{nieuw}= 24.000 - 8.000 = 16.000 per jaar

De berekening met de formule:
ROSI= $((ALE_{oud} - ALE_{nieuw}) * J - (K_{inv} + K_{jaar} * J)) / (K_{inv} + K_{jaar} * J)$

ALE_{oud} = 24.000 euro, de jaarlijkse verwachte verlieskosten op basis van de afgelopen jaren
ALE_{nieuw} = 8.000 euro = de jaarlijkse verlieskosten, na gebruik van de firewalls
J = 3, het aantal jaren dat de investering duurt
K_{inv} = 27.000 euro, dit zijn de eenmalige kosten
K_{jaar} = 2.000 euro per jaar terugkerende kosten

Bereken de ROSI.

Verdere toelichting
ROSI betekent Return on Security Investment. Als bedrijf wil je best investeren, maar natuurlijk ook je geld terugverdienen. In dit geval is het overduidelijk dat de maatregelen hebben geholpen, de kosten zijn met liefst 80% gedaald.

ROSI is in de bedrijfseconomie de rendementsberekening die de winst als percentage van het geïnvesteerde vermogen uitdrukt. Stel dat er een ROSI van 20% uitkomt. Dat betekent dat voor iedere geïnvesteerde euro er 1,20 euro wordt 'verdiend' (of bespaard). Wel is hierbij van belang over welke periode wordt gerekend. De periode van de verdienste en de investering moeten gelijk zijn. In ons geval dus drie jaar.

Casus 3 De software

Bereken de ROSI op basis van de onderstaande gegevens:

Een leverancier beweert dat zij de kosten via hun software kunnen terugbrengen naar ongeveer 10.000 euro per jaar. De huidige kosten van het pakket zijn 45.000 euro per jaar. Hiervoor willen zij een pakket leveren dat 65.000 euro eenmalig kost voor de duur van drie jaar. Ieder jaar moeten de licenties worden geüpdatet à 3.000 euro.

$$ROSI= ((ALE_{oud} - ALE_{nieuw}) * J - (K_{inv} + K_{jaar} * J)) / (K_{inv} + K_{jaar} * J)$$

Casus 4 Bewustzijnsprogramma

Er is een budget van 100.000 euro beschikbaar. Meedoen in een bewustzijnsprogramma levert een reductie van het aantal incidenten op van 10%, kosten per incident zijn gemiddeld 500 euro.

Het security-awareness-programma reduceert 10% van de incidenten gedurende de 3 jaar (daarna is het awareness-programma 'uitgewerkt'). Er zijn per jaar 1200 incidenten.

Bereken de ROSI.

Casus 5 Anti-virus-programmatuur

Er zijn nogal wat virusbesmettingen geweest en de vraag is of de aanschaf van een scan rendabel is. We berekenen de ROSI voor de periode van een 1 jaar en per werkplek.

De virusscan kost 200 euro per werkplek per jaar. De kosten voor het verhelpen van een virusbesmetting: 80 euro per werkplek per keer. Verwacht aantal besmettingen zonder anti-virus-programmatuur: 15 keer per jaar

Bereken de ROSI.

Casus 6 Aanschaf Storage Area Network

Het doel is het waarborgen dat de bedrijfsinformatie altijd beschikbaar is, zodat medewerkers alle informatie hebben om producten te verkopen.

De cijfers:
Directe investering: 320.000 euro
Duur van het project: 4 jaar
Beheerkosten per jaar: 30.000 euro
Kosten voor het niet-beschikbaar zijn van de gegevens is verloren omzet, omdat geen deals kunnen worden gesloten. Bij een storing in de serverruimte duurt het gemiddeld 3 uur voordat de servers en daarin opgeslagen informatie weer beschikbaar zijn. Gederfde omzet 50.000 euro per incident. Kans dat er een storing is, is naar schatting 5 keer per jaar. Naar verwachting zal het SAN het aantal incidenten reduceren tot 1 keer per 2 jaar.

Bereken via de formules de oude ALE
Bereken volgens de formules de nieuwe ALE
Bereken de ROSI

Practicum 5
Ransomware

De casus

Je werkt bij Mystics BV, een bedrijf dat scenario's voor games schrijft. Bij het bedrijf werken 15 mensen die allen gebruik maken van een HP-laptop waarop Windows 10 is geïnstalleerd. Het bedrijf heeft nog geen Active Directory, ook al zijn er vergevorderde plannen. De gebruikers werken 50% thuis en 50% op het werk. Op het werk is een netwerk aanwezig dat bestaat uit drie servers waar de werknemers hun bestanden opslaan. De servers zijn voorzien van Windows 2012 server-software. De servers zijn genaamd Mystico1, Mystico2, Mystico3. Mystico1 dient als file-server waar alle scenario's en ook alle persoonlijke bestanden worden opgeslagen. Mystico2 is de organisatorische server waar de directie en personeelszaken hun bestanden opslaan. Mystico3 dient als printserver en webserver. De printserver bedient de drie printers in de kantoorruimtes. Op Mystico3 draait ook de website. De webserver dient ook als webmail-host waar de werknemers hun mail kunnen verwerken. Meest gebruikte applicaties zijn Microsoft Office 10 en Acrobat Reader. Wat er verder op de laptops is geïnstalleerd is niet geheel duidelijk. Gebruikers kunnen als administrator inloggen en zelf applicaties installeren.

Het incident

Een van de medewerkers heeft ransomware opgelopen, de laptop is gegijzeld en alleen tegen betaling van € 150 kan de laptop ontgrendeld worden. De directeur is erg geschrokken van het voorval, omdat hij heeft begrepen dat ransomware zich snel kan verspreiden door een netwerk! Na wat speurwerk bleek de werknemer bewust de ransomware op de laptop te hebben geplaatst. Hij bleek een crimineel verleden te hebben van oplichting en kleine diefstal. Nadat hem was meegedeeld dat zijn contract niet werd verlengd, heeft hij willens en wetens het bedrijf willen schaden.

Om een indruk van de werking van ransomware te krijgen, bekijk je de volgende video: https://www.youtube.com/watch?v=nohlvsEK250
De directeur heeft het filmpje bekeken en wil dat er maatregelen getroffen worden om malware te voorkomen. Hij stelt, in samenwerking met een externe security officer, de volgende beleidsregels op.

1 Alle medewerkers beschikken over een OneDrive automatische backup-oplossing voor alle bestanden waar zij mee werken. OneDrive wordt standaard meegeleverd met Windows 10.

2 Er dient software te worden geïnstalleerd die alle software up-to-date houdt. Het verplichte pakket is Personal Software Inspector van Flexera.
3 Alle niet-noodzakelijke software dient te worden verwijderd van de laptops. Noodzakelijk voor gebruikers zijn Microsoft Office (is op de testcomputer niet geïnstalleerd vanwege licentieproblematiek), Chrome, Acrobat Reader, 7zip, Notepad++.
4 Er dient een goede antimalware- en virusoplossing te komen voor alle laptops. Verplicht pakket is Microsoft Defender.
5 Op alle computers dienen herstelpunten te worden aangemaakt en geactiveerd.
6 Op alle systemen moet de optie *Extensies voor bekende bestandstypen verbergen* worden gedeactiveerd.
7 Op alle systemen moeten alle bijlagen van mailbestanden automatisch worden gescand.
8 Op alle systemen moet Remote Desktop Control (RDP) worden uitgeschakeld.
9 Op alle computers wordt Chrome de standaard-browser.
10 De instellingen van de Chrome-browser worden op alle computers gereset.
11 Alle extensies binnen Chrome dienen te worden verwijderd.
12 Op alle systemen met Chrome wordt de Chrome Cleanup Tool uitgevoerd.
13 Alle medewerkers dienen een bewustzijnstraining te volgen.

Opdracht

Jij voert, in samenwerking met een collega, de implementatie van de beleids- en configuratieregels uit.

De regels zijn in groepen verdeeld:

- Regel 1 tot en met 4: software-installatie
- Regel 5 tot en met 9: configuratie Windows
- Regel 10 tot en met 12: browser-instellingen
- Regel 13: administratieve maatregelen (bewustzijnscursus en screening)

De testcomputer is een virtuele Windows-machine.

Je kunt inloggen als gebruiker Kees en met wachtwoord: Hallo1234\

Het beleid

1 Alle medewerkers beschikken over een OneDrive automatische backup-oplossing voor alle bestanden waar zij mee werken. OneDrive wordt standaard meegeleverd met Windows 10.
   - Controleer of OneDrive de mogelijkheid biedt van automatische backup van persoonlijke bestanden. Er moet minimaal iedere dag een automatische backup worden gemaakt. Wat zijn de mogelijkheden van een gratis account en wat van een betaalde oplossing?

2 Er dient software te worden geïnstalleerd die alle software up-to-date houdt. Het verplichte pakket is Personal Software Inspector van Flexera.
   - Installeer Flexera en test de werking. Wat doet de Personal Software Inspector? Is het mogelijk om via deze software alle applicaties up-to-date te houden? Noteer je bevindingen.

3 Alle niet-noodzakelijke software dient te worden verwijderd van de laptops. Noodzakelijk voor gebruikers zijn Microsoft Office (is op de testcomputer niet geïnstalleerd vanwege licentieproblematiek), Chrome, Acrobat Reader, 7zip, Notepad++.
- Check geïnstalleerde software op de computer. Noteer alle niet-standaardsoftware en geef advies wat met deze software te doen.

4 Er dient een goede antimalware- en virusoplossing te komen voor alle laptops. Verplicht pakket is Microsoft Defender.
- Installeer Windows Defender en stel een goed scanschema in. Noteer het schema in je rapport.

5 Op alle computers dienen herstelpunten te worden aangemaakt en geactiveerd.
- Noteer wat je voor herstelpunten hebt ingesteld. Licht kort toe waarom herstelpunten kunnen bijdragen aan het herstel bij actieve ransomware.

6 Op alle systemen moet de optie *Extensies voor bekende bestandstypen verbergen* worden gedeactiveerd.
- Beschrijf hoe dit hebt ingesteld en de geef de redenen.

7 Op alle systemen moeten alle bijlagen van mailbestanden automatisch worden gescand.
- Noteer hoe je dit instelt in Windows Defender.

8 Op alle systemen moet RDP worden uitgeschakeld.
- Noteer hoe je dit hebt uitgevoerd.

9 Op alle computers wordt Chrome de standaard-browser.
- Noteer hoe je dit hebt uitgevoerd.

10 De instellingen van de Chrome-browser wordt op alle computers gereset.
- Noteer hoe je dit hebt uitgevoerd.

11 Alle extensies binnen Chrome dienen te worden verwijderd.
- Noteer je bevindingen.

12 Op alle systemen met Chrome wordt de Chrome Cleanup Tool uitgevoerd.
- Noteer hoe je dit hebt uitgevoerd.

13 Alle medewerkers dienen een bewustzijnstraining te volgen.
- Maak een korte presentatie waarin je de belangrijkste onderdelen voor een bewustzijnscursus beschrijft. Wat vind jij belangrijk waar de medewerkers rekening mee moeten houden?

Rapportage

- Op basis van je notities stel je een rapport samen voor de directeur. Je geeft hierin puntsgewijs (per beleidsmaatregel) aan welke maatregelen je hebt getroffen.
- Je geeft aanbevelingen om het netwerk verder te versterken.
- Je onderzoekt of er mogelijk nieuwe software is die een besmetting met ransomware kan verhelpen.

Nader onderzoek

STIG – Chrome onder Windows 10

Om te controleren of alle aanbevelingen ten aanzien van browserbeveiliging voldoen, controleer je de STIG-lijst (Security Technical Implementation Guide) voor Chrome.
Bezoek de volgende pagina:
https://www.stigviewer.com/stig/google_chrome_v24_windows/
Hier vind je een aantal instellingen in de category HIGH specifiek voor Chrome. Hieronder zie je een zogenaamde finding. Je kunt in de pagina op het V-nummer klikken. Dan kom je op de pagina waar je ziet hoe je een bepaalde instelling kunt wijzigen.

Finding ID	Severity	Title	Description
V-35757	High	Use of cleartext passwords in the Password Manager must be disabled	Cleartext passwords would allow another individual to see password via shouldersurfing. "Controls whether the user may show passwords in clear text in the password manager. If you disable this ...

Als je op het V-nummer klikt zie je hoe je de setting kunt configureren. Bijvoorbeeld:

Details

Check Text (C-44102r1_chk)

Universal method (Requires Chrome Browser v15 or later):
1. In the omnibox (address bar) type chrome://policy
2. If PasswordManagerAllowShowPasswords is not displayed under the Policy Name cc
to false under the Policy Value column, then this is a finding.

Onderzoek de HIGH-categorie van de STIG-items en controleer in de Windows-10-omgeving hoe deze instellingen momenteel zijn geconfigureerd. Neem afwijkingen mee in je rapportage.

Je kunt de Google Chrome policy vinden met de Group Policy Editor:

- Open *gpedit.msc*.
- Blader naar *Computer Configuration* | *Beheer sjablonen* | *Classic Administrative Templates* | *Google Chrome*
- Ga naar de Stigviewer-pagina (link hierboven).
  Onderzoek hoe de HIGH category instellingen zijn geconfigureerd.

Tips

- Open Chrome en typ in de adresbalk: chrome://policy/
  Je krijgt zo de actieve instellingen te zien.
- Je kunt in de template kijken naar de instellingen **of** direct in het register kijken met *regedit.com* om de instellingen te controleren

Voorbeeld uitvoering

1. Start *gpedit.msc*.
2. Blader naar *Computer Configuration* | *Beheer sjablonen* | *Classic Administrative Templates* | *Google Chrome*
3. Ga naar de Stigviewer:
   https://www.stigviewer.com/stig/google_chrome_v23_windows/
4. Controleer de instellingen zoals hieronder beschreven

Hieronder staan de instellingen met de gewenste configuratie:
V-35757 Use of cleartext passwords in the Password Manager must be disabled

- Dubbelklik in het Google Chrome-sjabloon op:
  Password manager -
  "Enable Save Passwords" moet op *disabled* staan (dan kunnen wachtwoorden niet getoond worden).

Vul in de tabel hieronder in of de waardes conform het beleid zijn.

STIG	Waarde	Juist/onjuist
V-35757	Disabled	Juist (zie voorbeeld)
V-35622	Enabled	
V-35771	Disabled (via registry)	
V-35761	Enabled	
V-35760	Disabled	

Onderzoek Windows Defender

Tenslotte onderzoek je of Windows Defender de juiste keuze is als virus- en malware-blokker.
Neem je aanbevelingen mee in je rapportage.

Referenties:
https://www.av-test.org/en/antivirus/home-windows/
http://www.computeridee.nl/nieuws/windows-defender-slecht-uit-de-test/
http://www.pcworld.com/article/3025889/windows/tested-microsofts-windows-defender-antivirus-is-less-awful-than-it-used-to-be.html

Practicum 8
OpenSSL

In dit practicum maken we kennis met het gebruik van certificaten onder Windows. We maken een eigen certificaat en ondertekenen een pdf-bestand met dit certificaat.

Om een eigen certificaat te maken, maken we gebruik van OpenSSL.

1. We installeren OpenSSL.
2. We genereren een private sleutel.
3. We dienen een verzoek in om een certificaat te maken (getekend met je eigen sleutel).
4. We genereren een certificaat (met eigen verzoek en eigen sleutel) en converteren naar pfx.
5. We importeren het certificaat in Windows en ondertekenen een pdf-bestand met een digitaal ID (certificaat).
6. We importeren een certificaat in Acrobat Reader.
7. We tekenen een pdf-bestand.

1 Installatie OpenSSL

Donwload de tool hier:
http://mbosecurity.nl/2016/09/24/openssl-light-1-01-self-signed-certificaten-maken/

Unzip de inhoud naar *c:\openssl-win32*.

Na het uitpakken ziet de map er als volgt uit:

```
C:\>tree c:\openssl-win32
Map PATH-lijst voor volume OS
Het volumenummer is 72BE-4B6D
C:\OPENSSL-WIN32
└───bin
    └───PEM
        ├───certs
        ├───crl
        ├───demoCA
        │   ├───crlnumber
        │   ├───newcerts
        │   ├───private
        │   └───serial
        ├───demoSRP
        └───newcerts
```

Open na het uitpakken een cmd-prompt als administrator en geef het onderstaande commando:

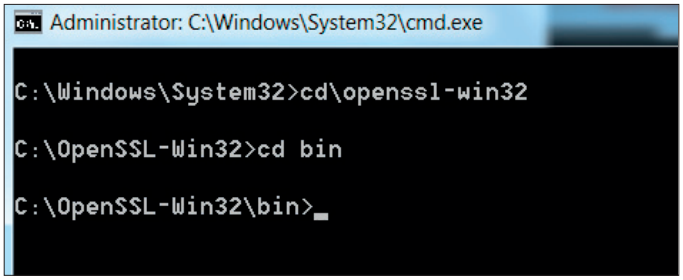
SETX OPENSSL_CONF c:\OpenSSL-Win32\bin\openssl.cfg en dan ENTER.

Sluit de command prompt niet af.

De installatie is nu gereed. We gaan nu een certificaat aanmaken via openssl

2 Maak een private sleutel

Ga naar de command prompt (als administrator) en geef de volgende commando's:
CD\OPENSSL-WIN32 en ENTER
CD BIN en ENTER

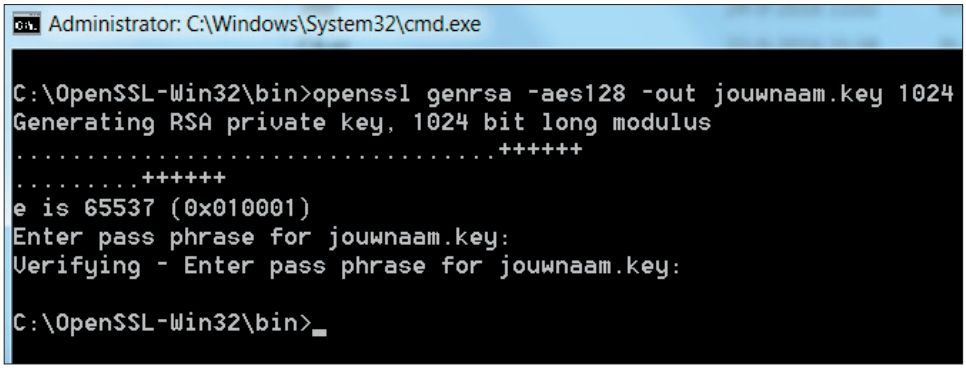


Met het onderstaande commando maak je een private sleutel. De sleutel is 1024 bits lang en wordt versleuteld met AES 128. Dat is ook meteen de reden dat je een passphrase (wachtwoord) moet opgeven, die wordt gebruikt voor de encryptie.

Verander jouwnaam in een naam naar jouw keuze.

Op de command prompt geef je het volgende commando. Als passphrase gebruik je hello.

openssl genrsa -aes128 -out jouwnaam.key 1024



Ga via de Verkenner naar de map *c:\openssl-win32\bin*.

Daar zie je jouw sleutel staan (jouwnaam.key).

Open dit bestand in Notepad of Notepad++ om het bekijken – **maar wijzig niets!**

3 Nu wordt een aanvraag (request) ingediend

Met het onderstaande commando dien je een verzoek in om het certificaat te laten tekenen. In dit geval tekenen we het certificaat zelf.

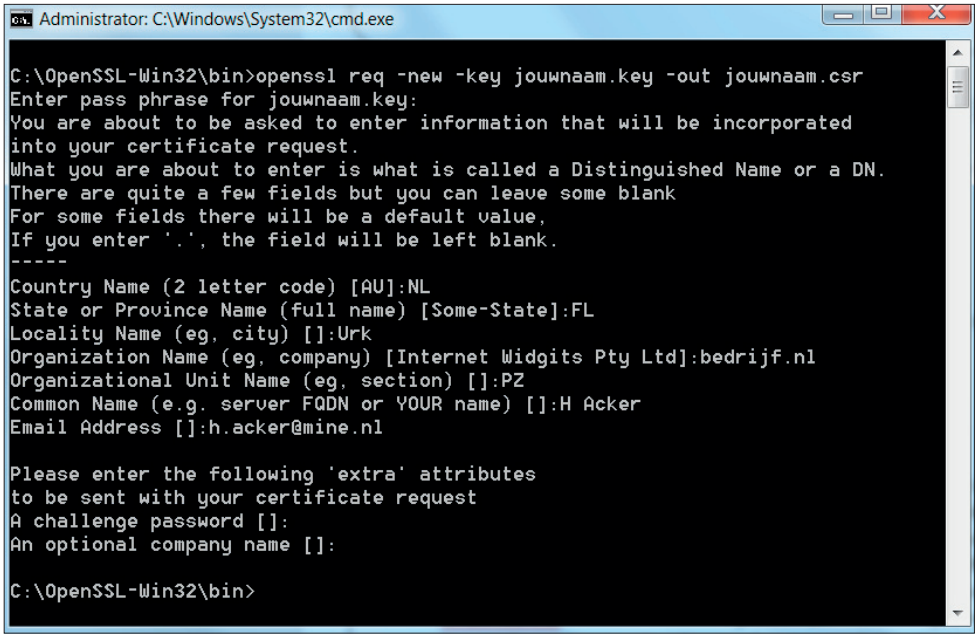
```
openssl req -new -key jouwnaam.key -out jouwnaam.csr
```

De passphrase is: hello

Je wordt gevraagd om wat extra informatie in te vullen:

Country Name	= NL	land van herkomst
State Or Province Name	= NH	provincie, hier Noord-Holland
Organization Name	= jouwbedrijf	jouw bedrijf voor het certificaat
Organizational Unit Name	= jouwafdeling	de afdeling waar je werkt
Common Name	= jouwnaam	jouw naam voor het certificaat
Email Address	= jouwemail	jouw e-mail

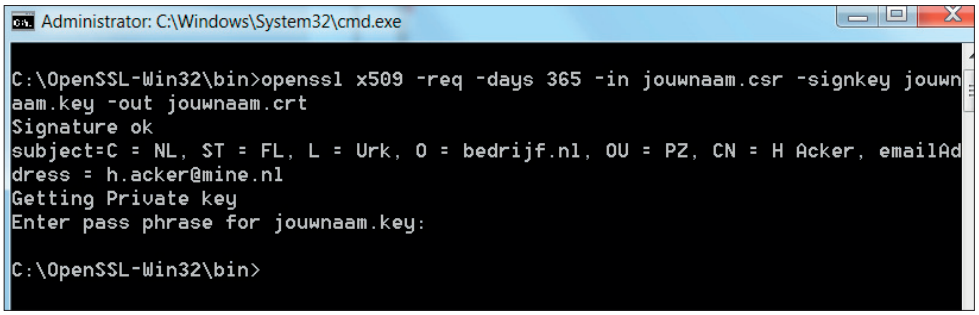
Nu worden er twee optionele waarden gevraagd, deze kun je overslaan (geef Enter).



4 Het self signed certificaat maken

Nu we de aanvraag hebben ingediend en alle gegevens hebben toegevoegd kunnen we het certificaat maken.

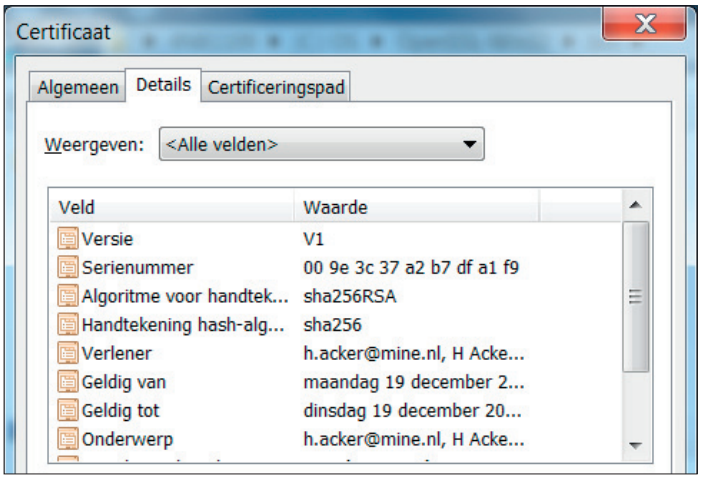
```
openssl x509 -req -days 365 -in jouwnaam.csr -signkey jouwnaam.key -out
jouwnaam.crt
```



In de map *c:\openssl-win32\bin* heb je nu drie bestanden gemaakt:

Jouwnaam.key als sleutel, *jouwnaam.crt* als aanvraag en *jouwnaam.crt* als certificaat.

Dubbelklik op *jouwnaam.crt*.



Om het certificaat te kunnen gebruiken in Acrobat Reader moet het eerst geconverteerd worden naar een pfx-versie. Je passphrase is weer hello. Geef het onderstaande commando in de prompt:

```
openssl pkcs12 -export -out certificate.pfx -inkey jouwnaam.key -in
jouwnaam.crt
```

Je hebt nu jouw certificaat geconverteerd naar *certificate.pfx*.

Dit certificaat heb je straks nodig

5 Importeren van het certificaat in Windows

Als je dat nog niet had gedaan, dubbelklik op het certificaat *jouwnaam.crt*.

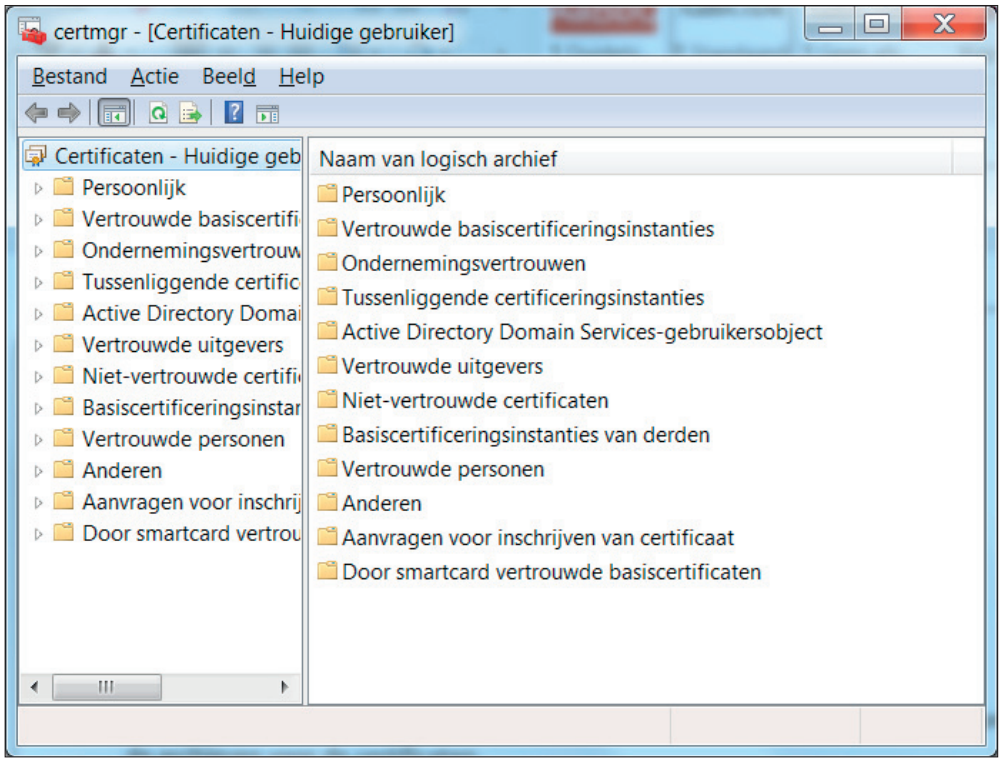
Klik op het tabblad *Algemeen* onderaan op *Certificaat installeren*.

Volg de wizard, wijzig niets en rond de wizard af.

Open nu de Certificaat Manager door *certmgr.msc* (open als administrator) uit te voeren.

Je hebt nu een overzicht van alle certificaten die bekend zijn bij jouw computer. De mappen die je ziet vormen de archieven voor de certificaten.

Ga naar de map *Tussenliggende certificaten*, daar vind je je eigen certificaat.



Dubbelklik op *Persoonlijk* en dan op *Certificaten*. Waarschijnlijk is deze map leeg. Mocht je een iPhone of iPad-device hebben aangesloten op deze computer met iTunes, dan heb je hier wel een Apple-certificaat staan.

Je hebt nu een certificaat toegevoegd aan je certificaatarchief.

Sluit Certificaat-beheer af

6 Importeren van een certificaat in Acrobat Reader

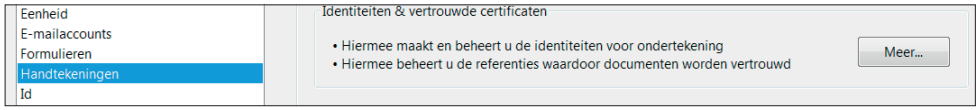
We gaan nu een certificaat in Acrobat Reader importeren. Met dit certificaat tekenen we later een pdf-bestand.

Mocht je Adobe Reader niet hebben, dan kun je hier de laatste versie downloaden (93 MB):
https://get.adobe.com/nl/reader/

De onderstaande plaatjes zijn gebaseerd op Acrobat Reader versie 2015. Eerdere versies hebben een heel andere werkwijze.

Open Acrobat Reader.

Klik op *Bewerken* | *Voorkeuren* | selecteer *Handtekeningen* in de lijst.



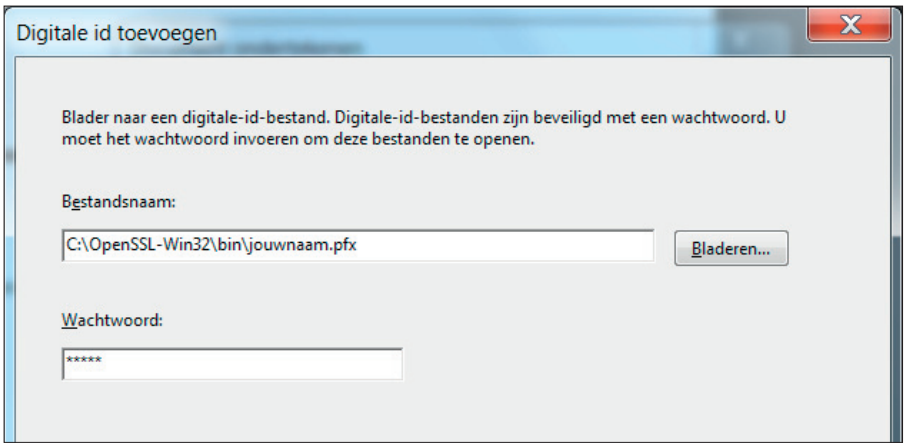
Klik op de knop *Meer* onder *Identiteiten en vertrouwde certificaten*.

Klik op het icoon +.

Selecteer *Een bestand* (dit is de standaard) en klik volgende:

Blader naar de map *c:\opensslwin32\bin* en selecteer het bestand *certificate.pfx*.

Vul bij *Wachtwoord* hello in.



Klik *Volgende* en sluit deze wizard af met een klik op *Voltooien*.

Je hebt nu een certificaat in Acrobat Reader geïmporteerd.

Je kunt dit scherm afsluiten, en sluit Acrobar Reader ook af.

7 Tekenen van een pdf-bestand met een digitale handtekening

Je ondertekent een pdf-bestand met je eigen certificaat. Hiervoor hebben we een pdf-bestand nodig. PDF betekent Portable Document Format en is het meest gebruikte documentformaat ter wereld.

Download *rsi.pdf*:

http://mbosecurity.nl/2016/09/24/openssl-win32-self-signed-certificaten-maken/

Onderin de post vind je het bestand.

Sla het bestand op in de map *Mijn documenten*.

Open het bestand *rsi.pdf* in Acrobat Reader door erop te dubbelklikken.

Blader naar de laatste pagina in het document.

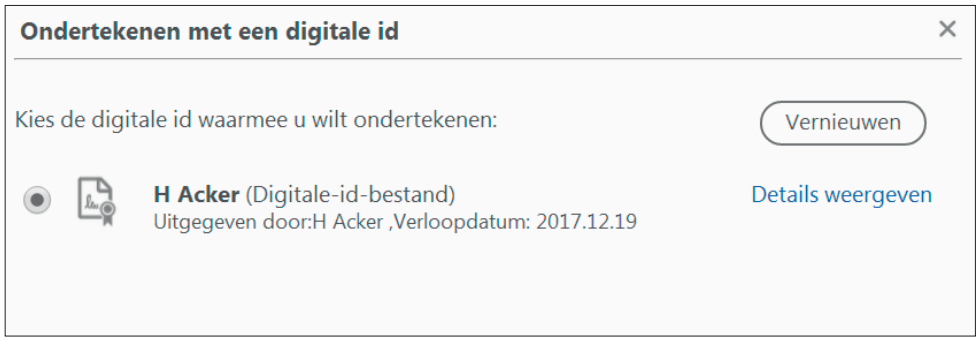
Klik in het menu op *Gereedschappen* en selecteer *Openen* onder het certificaten-icoon.

Klik op *Digitaal ondertekenen* en selecteer de plaats waar je de handtekening wilt zetten.

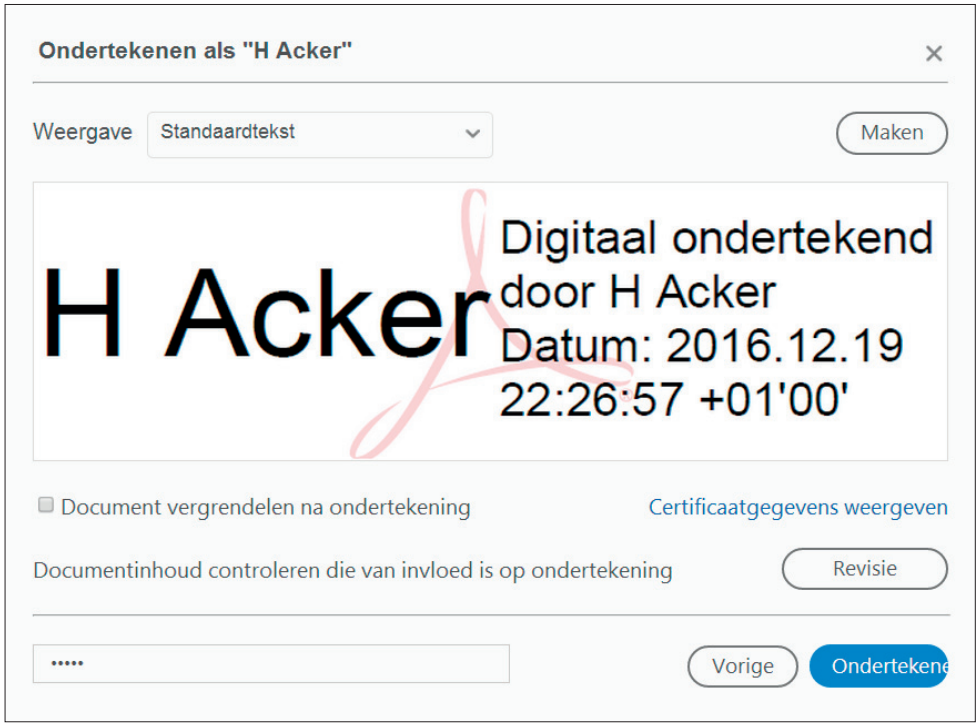
Nu kun je het bestand ondertekenen met je eigen certificaat.

Kies *Nieuwe handtekeningrechthoek slepen* en selecteer met je muis een vierkant in het document waar je je handtekening wilt plaatsen.

Het volgende scherm verschijnt:



Klik *Doorgaan* en het onderstaande scherm verschijnt.



Vul als passphrase in hello en klik *Ondertekenen.*

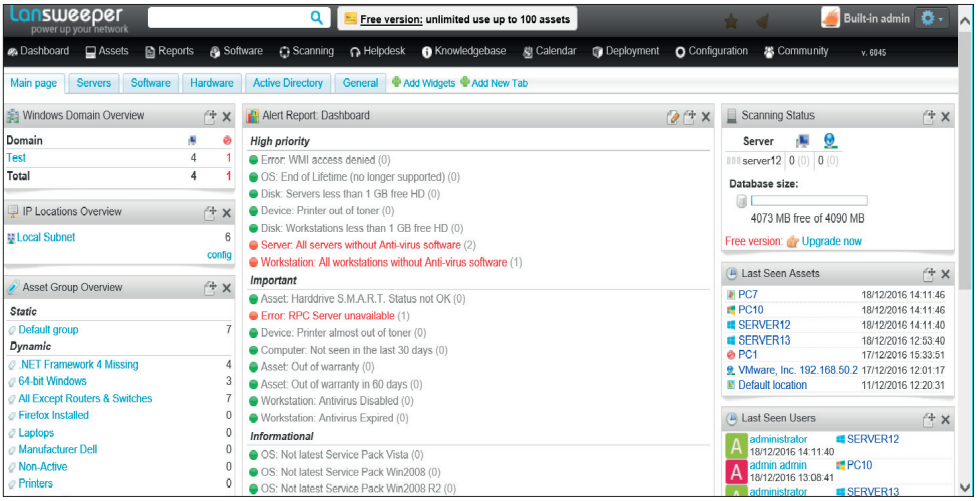
Sla nu *rsi.pdf* op als *rsi2.pdf.*

Je hebt nu een digitale handtekening toegevoegd aan je pdf-bestand.

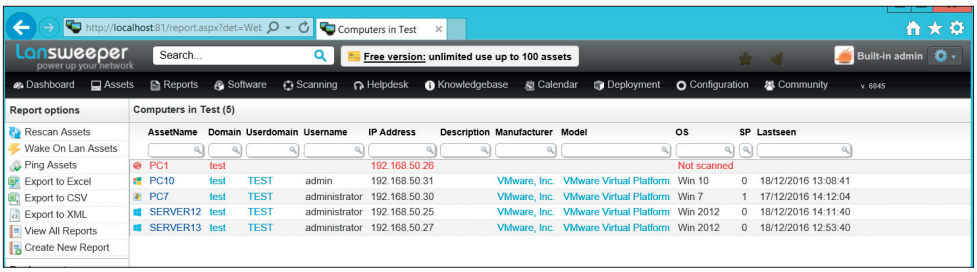
Practicum 9
De inventarisatie

Er zijn vele tools online te vinden waarmee een inventarisatie kan worden uitgevoerd. Wij kiezen ervoor om Lansweeper te gebruiken. De tool is gratis voor kleine netwerken en werkt via de browser. De tool kan hier gedownload worden: http://www.lansweeper.com/nl/

- Zorg ervoor dat alle 4 de systemen zijn opgestart voor je Lansweeper gebruikt.
- Het inventarisatieprogramma Lansweeper is geïnstalleerd op de domain controller.
- Je start het programma door te dubbelklikken op het desktop-icoon.
- Je logt in met Admin en als wachtwoord !Welkom1234//



Je krijgt bovenstaande interface te zien. Als je hier linksboven op *Dashboard* klikt kom je automatisch op de 'main page'. Je ziet linksboven *TEST* onder *Domain* staan. Als je op de naam *TEST* klikt zie je de assets in het domain.



Alle systemen die zich binnen het domain TEST bevinden komen in beeld.

Nu gaan we onderzoeken welke programma's geïnstalleerd zijn op de verschillende computers. Zo kunnen we uitvinden of er illegale dan wel ongewenste programma's in het domain zijn geïnstalleerd. Maak gebruik van het werkblad **Inventarisatie** om de gegevens in te vullen.

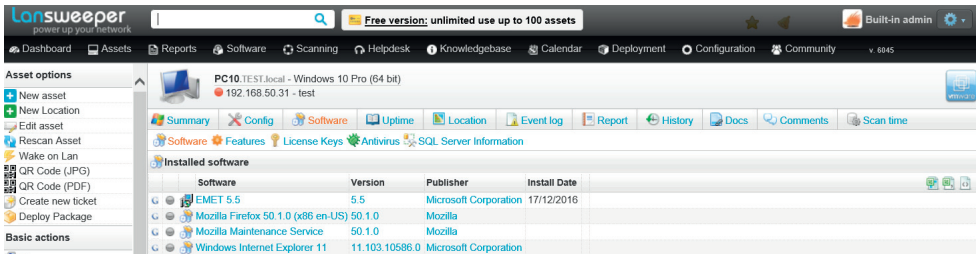
Om er zeker van te zijn dat je de meest up-to-date informatie over de computers hebt klik je in het menu op *Scanning*.

- Daar klik je op bovenste knop *Scan now*, deze scant alle aan het domain gekoppelde computers.
- Klik *Yes* en dan klik *OK*.
- Ga nu naar *Scanning queue* (links in het midden van het scherm).
- Heb geduld! Wacht 30 seconden en alle computers worden opnieuw gescand.
- Dit duurt van 1 minuut tot 3 minuten.
- Controleer het onderstaande beleid

Het beleid

De standaardinstallatie op de computers bestaat uit:

- Microsoft Essentials
- EMET 5.51
- Google als standaardbrowser
- 7zip als compressieprogramma
- OneDrive met automatische backup
- Notepad++ als tekstverwerker



- Gebruikers mogen geen eigen shares op de systemen hebben.
- Alle gebruikers moeten een home directory op server13 hebben.
- Er mag geen FTP-verbinding open staan op de domain systemen.
- Er mag geen remote connection actief zijn zonder NLA-beveiliging (test met admin-account).
- Op de client-systemen mogen geen lokale gebruikersaccounts aanwezig zijn.

Met deze opdracht heb je een inventarisatie uitgevoerd op een aantal domain-systemen door gebruik te maken van Lansweeper, een veelgebruikte tool.