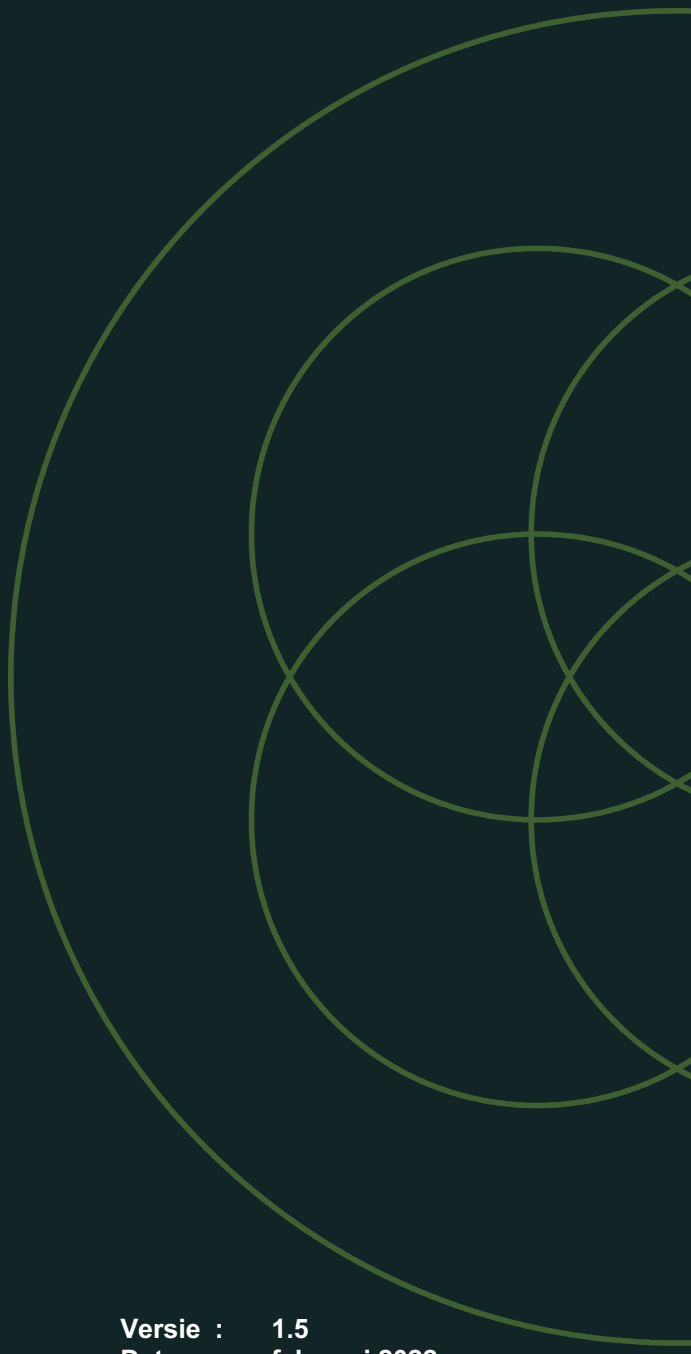
GROUP SECURE | NETWORK SECURITY SPECIALISTS

Network Security Assessment



Versie : 1.5
Datum : februari 2022

Documentbeheer

Versiebeheer

Versie	Datum	Auteur	Aard van de wijziging
1.0	13-1-2022	B. Janssen	Initieel document
1.1	17-1-2022	B. Janssen	Start audit
1.2	24-1-2022	B. Janssen	Invullen rapportage, bevindingen en aanbevelingen
1.3	28-1-2022	B. Janssen	Nacontrole + bijvoegen bijlagen
1.4	4-2-2022	F. Brouwers	Controle document
1.5	11-2-2022	F. Brouwers	Eindcontrole en managementsamenvatting

Voorwoord

Anoniem BV heeft ons, GroupSecure, verzocht om een rapport op te stellen met daarin de staat van de (technische) beveiliging van de interne en externe ICT-omgeving. We hebben dit rapport met grote zorg samengesteld en er is door verschillende consultants en engineers aan gewerkt met elk hun eigen expertise.

Dit rapport is geschreven voor zowel het (middel- en hogere) management alsmede systeem- en netwerkbeheerders. De managementsamenvatting geeft een niet-technische beschrijving van de bevindingen en is primair geschreven voor management en directie. De verschillende hoofdstukken en subhoofdstukken gaan dieper in op de bevindingen, geven uitleg en context en zijn hierdoor met name geschreven voor (technische) beheerders van Anoniem BV.

De prioriteitenlijst aan het einde van het rapport geeft een totaalweergave van alle constateringen met daarbij een gewogen prioriteit op basis van de OWASP Risk Rating methodologie, welke in context wordt geplaatst met het type organisatie van Anoniem BV. Deze lijst geeft alle lezers een duidelijk handvat bij het verbeteren en oplossen van risico's en problemen.

Inhoudsopgave

Managementsamenvatting

Om inzicht te krijgen in de huidige staat van de technische informatie- en netwerkbeveiliging hebben wij, op verzoek van de Anoniem BV, een security assessment uitgevoerd op de IT omgeving. Tijdens het uitvoeren van de audit is ….

Edge firewall
Beschouwen we het IT netwerk van “buiten naar binnen”, dan is de eerste logische stap het controleren van de (edge) firewall. Bij de controle hiervan is gebleken dat de “poortwachter” goed is ingericht. Enkele belangrijke en essentiële beveiligingstechnieken worden echter niet ingezet of foutief geconfigureerd terwijl deze wel noodzakelijk zijn. Met enkele aanpassingen zal de firewall veel beter zijn werk kunnen doen en wordt de beveiliging van het internetverkeer sterk verbeterd.

Multi Factor Authenticatie
Doordat gebruikers vaak wachtwoorden hergebruiken (dus eenzelfde wachtwoord gebruiken voor accounts bij verschillende applicaties, software en clouddiensten), is het voor cybercriminelen eenvoudig om met de gelekte databases de wachtwoorden te testen op de servers van bedrijven.

Tijdens het assessment is gebleken dat er op twee plekken, namelijk de Remote Desktop (RDS-) en Microsoft-omgeving, kan worden ingelogd met gebruikersaccounts van Anoniem BV zonder hierbij een 2^{e} factor authenticatie nodig te hebben.

Het is niet mogelijk om hergebruik van wachtwoorden door medewerkers te voorkomen of te controleren, maar om de impact van hergebruik van wachtwoorden te minimaliseren, is het van essentieel belang dat multi-factor authenticatie voor gebruikers en zeker voor beheerders wordt afgedwongen. Op het moment dat inloggegevens van een gebruiker bekend zijn, heeft een cybercrimineel alsnog een extra stap nodig om toegang te kunnen krijgen.

Segmentatie
Lukt het een cybercrimineel toegang tot het IT-netwerk te verkrijgen dan is de eerstvolgende vraag tot hoever hij vervolgens kan binnendringen. Binnen het netwerk van Anoniem BV wordt er weliswaar gebruik gemaakt van meerdere segmenten (VLAN’s), echter vindt er geen actieve filtering/controle plaats tussen de verschillende segmenten. Hierdoor is het voor een aanvaller goed mogelijk om het gehele netwerk te infiltreren, zonder dat dit wordt opgemerkt door de netwerkbeheerders. Daarnaast is het erg belangrijk om toegangsrechten van gebruikers goed te configureren zodat ze enkel toegang hebben tot resources (applicaties/ bestanden) die ze nodig hebben om hun werkzaamheden uit te kunnen voeren.

Endpointbeveiliging en gebruikersrechten
Doordat de cyber-bedreigingen in 2022 voor een groot deel worden gedomineerd door ransomware en zero-day malware (malware/virussen die nog nooit eerder zijn geconstateerd in de wereld en dus als “nieuw en onbekend” worden beschouwd), moeten anti-virus oplossingen hier ook op toegespitst zijn. Dit betekent dat er betere en geavanceerdere technieken moeten worden toegepast om laptops, desktops en servers adequaat te beschermen. Tijdens de audit bleek dat er gebruik wordt gemaakt van een beveiligingsoplossing die deze nieuwe detectietechnieken niet bevat. Ook worden bedreigingen op endpoints onvoldoende in de gaten gehouden via een centraal dashboard en wordt er met name vertrouwd op de werking van de oplossing dan dat er wordt gecontroleerd.

Conclusie
Concluderend stellen we vast dat IT beveiliging duidelijk een onderdeel is waar Anoniem BV aandacht voor heeft, alleen op basis van de cyber-bedreigingen anno 2022 is dit niet voldoende en is hier vanuit alle lagen van de organisatie meer aandacht voor nodig.

1 Inleiding

Anoniem BV heeft ons, GroupSecure, verzocht om een uitgebreid onderzoek uit te voeren naar de staat van de (technische) beveiliging van de interne en externe ICT-omgeving. Op basis van gesprekken met de organisatie is de volgende scope bepaald:

Gehele productieomgeving bestaande uit 17 fysieke servers, 28 virtuele servers, 234 smartphones. Twee locaties met :

- Locatie 1: 1388 werkplekken (desktops en laptops);
- Locatie 2: 277 werkplekken (desktops en laptops);
- Gebruikers: 1822 medewerkers
- Core- en Edge-switches, EnGenius Wifi - 102 AP's en 3 SSID's
- Firewalls: Fortigate (2 node cluster);
- Endpoint Protection: Kaspersky;
- Load Balancer
- IDM
- Active Directory Federated Services;
- Microsoft Radius
- Microsoft Cloud

Met dit assessment willen we Anoniem BV duidelijkheid verschaffen in de huidige staat van beveiliging van de interne en externe ICT-omgeving. Daarnaast is het onderzoek bedoeld om deze huidige staat te toetsen aan de hedendaagse beveiligingsstandaarden die worden gehanteerd in de branche. Tenslotte reiken we met dit uitgebreide onderzoek handvatten aan om Anoniem BV te helpen de beveiliging van de IT-infrastructuur naar de huidige standaarden te brengen.

Elk hoofdstuk begint met een korte beschrijving van de inhoud ervan. Daarna wordt per onderwerp eerst de huidige beveiligingsstandaard beschreven (de baseline). Vervolgens worden de bevindingen uiteen gezet en getoetst aan de baseline. Tenslotte wordt het advies beschreven om van de geconstateerde situatie naar de gewenste situatie (de baseline) te komen.

2 Werkplekken

In dit hoofdstuk wordt de beveiliging op de werkplekken behandeld. Onder werkplekken wordt verstaan: alle apparaten waar eindgebruikers op aan loggen of data op verwerken. Simpelweg worden deze opgedeeld in een tweetal categorieën.

- (Virtuele) Desktops en laptops
- Smartphones en tablets

2.1 Endpoint Protection

2.1.1 Baseline

Bescherming van werkplekken zoals (virtuele) desktops en laptops tegen actuele bedreigingen, moet bestaan uit in ieder geval een centraal beheerde Endpoint Protection oplossing met in ieder geval een Advanced Threat Protection (ATP) module. Deze laatste module biedt bescherming tegen onbekende malware zoals ransomware en 0-day exploits. Ook is het belangrijk dat op de endpoints de firewall-module van het besturingssysteem actief is.

Opslagmedia van in ieder geval mobiele endpoints moeten versleuteld zijn en ook moet er een mogelijkheid zijn om, conform wet- en regelgeving, aan te kunnen tonen dat de opslagmedia van deze mobiele endpoints van encryptie zijn voorzien (in geval van diefstal of verlies).

Tenslotte is het tegenwoordig vrijwel onmisbaar om Extended Detection en Response (XDR) toe te voegen aan een centraal beheerde Endpoint oplossing. XDR is een SaaS-gebaseerde, leverancier-specifieke tool voor het opsporen van beveiligingsbedreigingen. Het geeft de mogelijkheid om te reageren op incidenten die één enkele beveiligingsoplossing overstijgen en combineert daarmee de data van meerdere bronnen in één samenhangend systeem.

2.1.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
Kaspersky beschikt niet over moderne ATP functionaliteit	HOOG	GEMIDDELD	HOOG

De Kaspersky AV-oplossing in de huidige licentievorm wordt gezien als basis bescherming en beschikt niet over specifieke geavanceerde detectiemethoden waarmee exploits of ransomware aanvallen gedetecteerd en gestopt worden.

Bevinding	Kans op misbruik	Impact	Risico
Kaspersky beschikt niet over XDR of audit functies	HOOG	GEMIDDELD	HOOG

Kaspersky beschikt niet over Extended Detection and Response functies welke een beheerder van meer informatie kunnen voorzien bij een incident. Kaspersky blokkeert simpelweg een proces wel of niet maar is niet in staat om de beheerder te helpen met verdere root-cause analyses of audit functionaliteit.

Bevinding	Kans op misbruik	Impact	Risico
Full Disk Encryptie is slechts deels in gebruik	HOOG	HOOG	KRITIEK

Full Disk Encryptie is deels in gebruik. Hierdoor is het goed mogelijk dat er gegevens op straat belanden bij het verliezen of bij diefstal van een systeem.

2.1.3 Advies

Activeer Bitlocker op alle client systemen en beheer dit via een centraal systeem zodat dit ook aantoonbaar actief is.

Kaspersky in de huidige licentievorm is enkel inzetbaar als basisbeveiliging voor werkplekken en is in de huidige tijd onvoldoende om als enige Endpoint Protection oplossing te dienen. Een Endpoint Protection oplossing die actief (0-day) malware en …

2.2 Mobile Device Management

2.2.1 Baseline

Een Mobile Device Management oplossing wordt ingezet om (primair) smartphones en tablets te beheren zodat ook op deze apparaten controle kan worden uitgeoefend. De inzet van privé-toestellen kan hiermee worden gecontroleerd (of voorkomen) en verouderde en eventueel kwetsbare besturingssystemen blijven inzichtelijk.

Wanneer smartphones of tablets langere tijd niet verbonden zijn geweest met een bedrijfsnetwerk, kan toch op afstand controle worden uitgeoefend. Ook geeft een MDM-oplossing de mogelijkheid om encryptie van device en opslagmedia af te dwingen en kan op afstand een toestel, bij diefstal of verlies, worden gewist. Ook hierbij geldt weer dat wet- en regelgeving dicteren dat aangetoond moet kunnen worden of verlies of diefstal van een device ook tot een (mogelijk) datalek heeft geleid en hiervoor kan de MDM-oplossing uitkomst bieden.

2.2.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
Er is geen MDM oplossing in gebruik	HOOG	HOOG	KRITIEK

Op dit moment is er geen centrale controle over uitgegeven mobiele devices en de data die deze opslaan.

2.2.3 Advies

Het is sterk aan te bevelen om een MDM-oplossing in te zetten …

2.3 Rechten en credentials

2.3.1 Baseline

Eindgebruikers van (virtuele) desktops en laptops zouden geen lokale administrator-rechten nodig moeten hebben om hun normale, dagelijkse werkzaamheden uit te kunnen voeren. Het risico van lokale beheerdersrechten is dat (per abuis of opzettelijk) kwaadaardige software kan worden geïnstalleerd. Deze kan zich daarna mogelijk verspreiden in de rest van het netwerk, het apparaat als toegangspunt voor hackers dienst laten doen of keyloggers en andere malware installeren.

Wanneer gebruikers geen lokale beheerdersrechten hebben op de endpoints, is het ook belangrijk om de uitvoer van executables of scripts te voorkomen.

Enkel wanneer specifieke (Powershell)scripts voor gebruikers uitvoerbaar moeten zijn, dan zouden deze ondertekend moeten zijn door de eigen CA en middels policies zouden alleen deze gesigneerde scripts uitgevoerd kunnen worden.

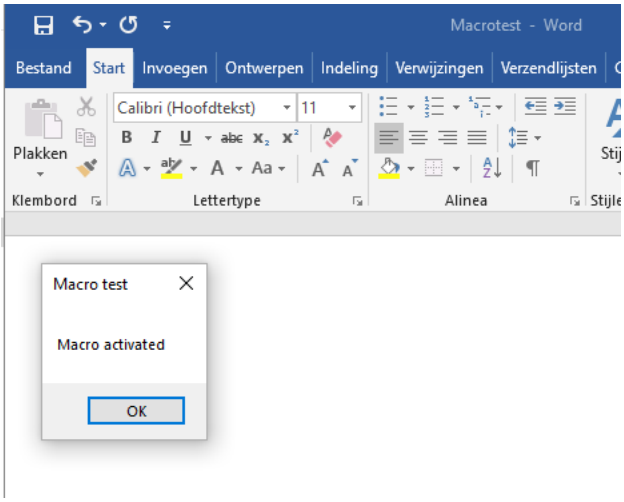
2.3.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
EXE uitvoeren vanuit sommige mappen mogelijk	HOOG	GEMIDDELD	HOOG

Executable bestanden worden netjes geblokkeerd door beleidsregels. Er is echter een fout in de configuratie gemaakt die het mogelijk maakt om EXE-bestanden en andere hoog risico extensies vanuit specifieke mappen te starten.

Bevinding	Kans op misbruik	Impact	Risico
Macro's zijn niet volledig uitgeschakeld	HOOG	GEMIDDELD	HOOG

Macro’s zijn gedeeltelijk beveiligd. Een gebruiker moet eerst vanuit Word toestemming geven om deze te starten. Het komt echter regelmatig voor dat gebruikers dit alsnog doen waardoor malware gestart kan worden.



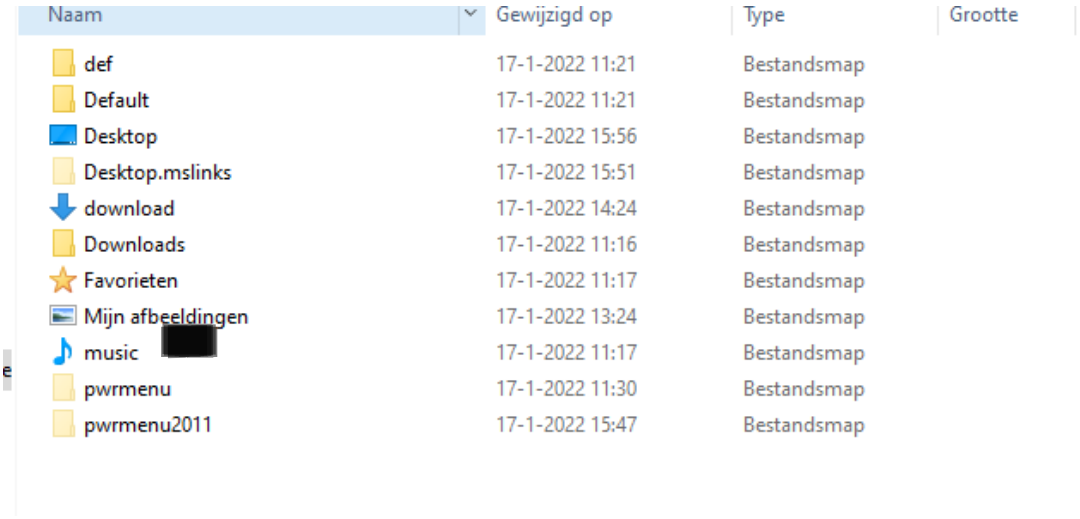
Figuur 1 Macro na toestaan door gebruiker

Bevinding	Kans op misbruik	Impact	Risico
USB-Opslagmedia zijn vrij te gebruiken	HOOG	HOOG	KRITIEK

USB-Opslagmedia zijn vrij te gebruiken. Hierdoor kunnen vertrouwelijke gegevens onversleuteld worden opgeslagen en in potentie op straat belanden.

Bevinding	Kans op misbruik	Impact	Risico
Browsen op netwerkshares is mogelijk	HOOG	LAAG	**GEMIDDELD**

Browsen op netwerkshares is op meerdere manieren mogelijk ook al zijn er pogingen gedaan om dit te blokkeren.



Figuur 2 Netwerkshare openen met Notepad

2.3.3 Advies

Anoniem BV beschikt grotendeels al over de juiste tools om de cliënt omgeving goed te configureren en dit lijkt grotendeels ook al te zijn gedaan. Echter zijn er door de jaren heen duidelijk wat zwakke plekken ontstaan welke opnieuw bekeken zouden moeten worden.

Gebruik voor lokale administrators unieke wachtwoorden per systeem en …

3 Domein en serveromgeving

In dit hoofdstuk wordt ingegaan op de beveiliging het domein en de serveromgeving. Hierbij wordt gekeken naar de opbouw van de Active Directory, de configuratie van DNS en DHCP, hoe wordt omgegaan met (tijdelijke) shares en de toekenning van rechten aan gebruikers, beheerders en services. Ook worden de gebruikte Group Policies (GPO's) beoordeeld.

3.1 Group Policy

3.1.1 Baseline

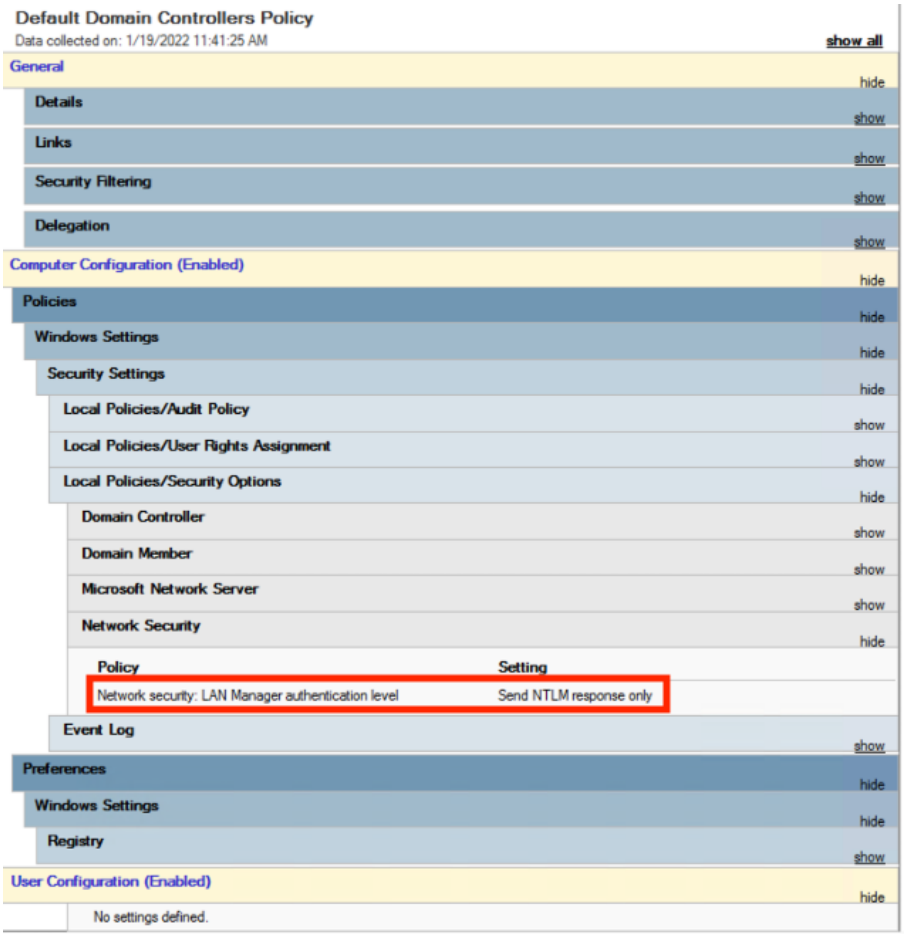
Een aantal belangrijke onderdelen van Group Policy moeten worden ingezet om een omgeving zo veilig mogelijk te houden. De AppLocker functionaliteit, waarmee restricties kunnen worden geplaatst op de uitvoer van applicaties, processen en scripts voor eindgebruikers, is een belangrijke policy om te implementeren.

Daarnaast moeten middels GPO nog een aantal andere zaken worden beperkt om de veiligheid van clients te waarborgen.

3.1.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
SMB Signing is niet vereist	LAAG	HOOG	**GEMIDDELD**

SMB signing is niet vereist waardoor het mogelijk is om man-in-the-middle aanvallen uit te voeren.



Figuur 3 NTLM policy

Bevinding	Kans op misbruik	Impact	Risico
Network Layer Authentication is niet actief	GEMIDDELD	HOOG	**HOOG**

Een groot aantal systemen maakt geen gebruik van NLA (Network Layer Authentication) waardoor met name RDP (Remote Desktop Protocol) verbindingen extra vatbaar zijn voor RDP exploits en authenticatie aanvallen.

Bevinding	Kans op misbruik	Impact	Risico
Alle gebruikers kunnen computers in het domein joinen	LAAG	LAAG	**AANTEKENING**

Het is mogelijk om als een willekeurige gebruiker het domein te joinen waardoor een aanvaller op een eigen systeem eenvoudig toegang krijgt tot veel gegevens. Zo is het eenvoudig om alle policy's uit te lezen of om een willekeurige DNS naam te registreren in DNS.

3.1.3 Advies

Veel van de gevonden punten uit dit hoofdstuk zijn verouderde authenticatie instellingen of instellingen welke jaren geleden zijn gemaakt vanwege compatibiliteit. Microsoft biedt verschillende tools om dit soort instellingen naar een actueel niveau te krijgen.

3.2 Serveromgeving

3.2.1 Baseline

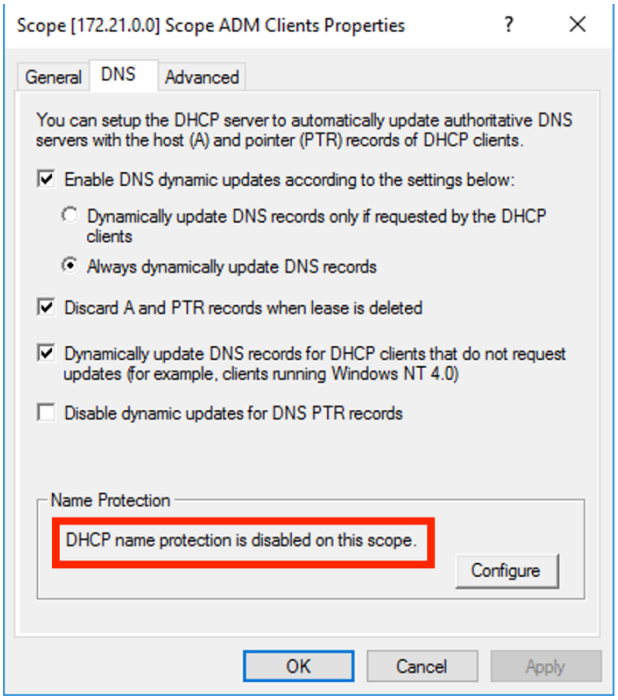
Het is belangrijk om, net als op de werkplekken, een moderne beschermingsoplossing tegen (0-day) malware en ransomware actief te hebben met als belangrijke toevoeging een XDR-functionaliteit. Zie hoofdstuk 2.1.1 voor verdere uitleg hieromtrent.

Op de serveromgeving moet DNS Name Protection ingeschakeld staan. Dit voorkomt het zogenaamde “name squatting” waarbij een niet-Windows device zich wil registreren in DNS met een naam die al is toegekend aan een Windows device. Verder zouden onbekende en ongeautoriseerde devices niet in staat moeten zijn om ...

3.2.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
DHCP Name protection is uitgeschakeld	GEMIDDELD	HOOG	**HOOG**

DHCP Name protection is uitgeschakeld op alle scopes. Hierdoor is het mogelijk om bestaande DNS namen te overschrijven.



Figuur 4 DHCP Name protection uitgeschakeld

Bevinding	Kans op misbruik	Impact	Risico
DNS Debug logging is niet ingeschakeld	HOOG	LAAG	**GEMIDDELD**

DNS Debug logging is niet ingeschakeld. Hierdoor is het niet te achterhalen welke PC …

Bevinding	Kans op misbruik	Impact	Risico
UPD$ Share toegankelijk voor RDS users	LAAG	LAAG	**AANTEKENING**

De UPD$ share is toegankelijk voor SGC_RDS_USERS. Deze share bevat een disk image van de server.

Bevinding	Kans op misbruik	Impact	Risico
Restore mappen op SYS-BKUP02 zijn toegankelijk	HOOG	HOOG	**KRITIEK**

De Restore map op SYS-BKUP02 zijn toegankelijk en hebben schrijfrechten voor authenticated users. Deze mappen bevatten backups van verschillende belangrijke systemen.

Bevinding	Kans op misbruik	Impact	Risico
Logs$ map op SCCM01 is toegankelijk	LAAG	LAAG	**AANTEKENING**

De logs map op 172.18.1.7 is toegankelijk en heeft schrijfrechten voor authenticated users.

Bevinding	Kans op misbruik	Impact	Risico
Gebruiker heeft full control rechten op meerdere mappen	LAAG	HOOG	**GEMIDDELD**

De gebruiker K.Beentjes heeft volledige rechten op minimaal de mappen Data$ en Service$. Ook lijkt in dit geval de -adm gebruiker rechten te hebben. De toegang van een van de twee gebruikers is vrijwel zeker onnodig.

3.2.3 Advies

Configureer DHCP en DNS zo dat alleen vertrouwde systemen automatisch DNS namen kunnen reserveren en vermijd DHCP-scopes op domain controllers welke niet geïntegreerd zijn met het domein.

Controleer periodiek alle rechten van netwerk shares en controleer of er geen tijdelijke shares zijn aangemaakt. Dit is eenvoudig te doen door alle computers toe te voegen aan de Windows server manager (deze bouwt vervolgens een lijst op met alle bestaande gedeeld mappen).

3.3 Domeinrechten

3.3.1 Baseline

Bij het toekennen van domeinrechten aan gebruikers is het essentieel de gebruikers enkel de minimaal benodigde rechten toe te kennen die nodig zijn om de dagelijkse werkzaamheden uit te kunnen voeren. Dit is per gebruikersgroep verschillend maar dit moet zo accuraat mogelijk worden toegepast en onderhouden. Er moet een proces beschreven zijn, als onderdeel van een HR-proces, dat duidelijk maakt welke functie welke rechten zou moeten krijgen.

Verder is het belangrijk om beheerdersaccounts te kunnen herleiden naar fysieke personen door de naamgeving ervan hierop aan te passen (bijvoorbeeld “adm_kbeentjes” als administrator-account voor gebruiker “kbeentjes”).

3.3.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
Veel gebruikers lid van domain admins	HOOG	HOOG	KRITIEK

Er zijn onnodig veel gebruikers lid van de Domain Admins groep. Met name de K.Beentjes en P.Post zijn opvallende gebruikers welke niet in deze groep thuishoren en hierdoor voor een aanzienlijk verhoogd risico zorgen.

Bevinding	Kans op misbruik	Impact	Risico
Gebruikers onnodig toegang tot RDS-Omgeving	HOOG	HOOG	KRITIEK

De groepen “OS” en “OPT” hebben toegang tot de RDS-omgeving. Echter bevatten deze groepen ook gebruikers met een mogelijk door veel meer gebruikers bekend wachtwoord of een eenvoudig te achterhalen wachtwoord.

3.3.3 Advies

Bescherm de Admin accounts veel beter door de eerdergenoemde referentie links te volgen en de adviezen op te volgen. Zorg er tevens voor dat alleen de absoluut noodzakelijke gebruikers lid zijn van de Domain Admins groep.

4 Authenticatie en autorisatie

Op welke manier een gebruiker, bekend of onbekend, toegang krijgt tot het netwerk wordt bepaald door de manier van authentiseren en op welke manier de autorisatie wordt afgehandeld. Hierbij worden onderwerpen als Password Policy, Network Access Control (NAC), Conditional Access en multi-factor authenticatie (MFA) behandeld. Het kan gebeuren dat op enkele andere plaatsen in dit document ook over (multi-factor)authenticatie wordt gesproken bij specifieke onderwerpen, maar dezelfde bevindingen zullen niet vaker worden beschreven.

4.1 Network Access Control

4.1.1 Baseline

Toegang tot het netwerk moet altijd gereguleerd worden, of het nu via een Wifi-netwerk is of via een netwerkkabel. Hiermee wordt voorkomen dat aanvallers via fysieke netwerkpoorten (bijvoorbeeld via een patchpunt in een publiek toegankelijke vergaderruimte of door een printer los te koppelen) direct in een netwerk kunnen geraken. Ook via wifi kunnen aanvallers, wanneer ze bijvoorbeeld een pre-shared key weten te bemachtigen, toegang tot het netwerk krijgen. De toegang kan daarom het beste worden gereguleerd met een Network Access Control (NAC) toepassing. Onbekende en ongeautoriseerde apparaten worden hiermee geïsoleerd van de rest van het netwerk totdat een beheerder deze toegang verschaft.

4.1.2 Bevindingen

Anoniem BV heeft een goed geconfigureerde NAC-oplossing in de vorm van Quarantainenet 13-37 NAC geïmplementeerd.

4.1.3 Advies

Geen aanvullend advies van toepassing.

4.2 Password Policy

4.2.1 Baseline

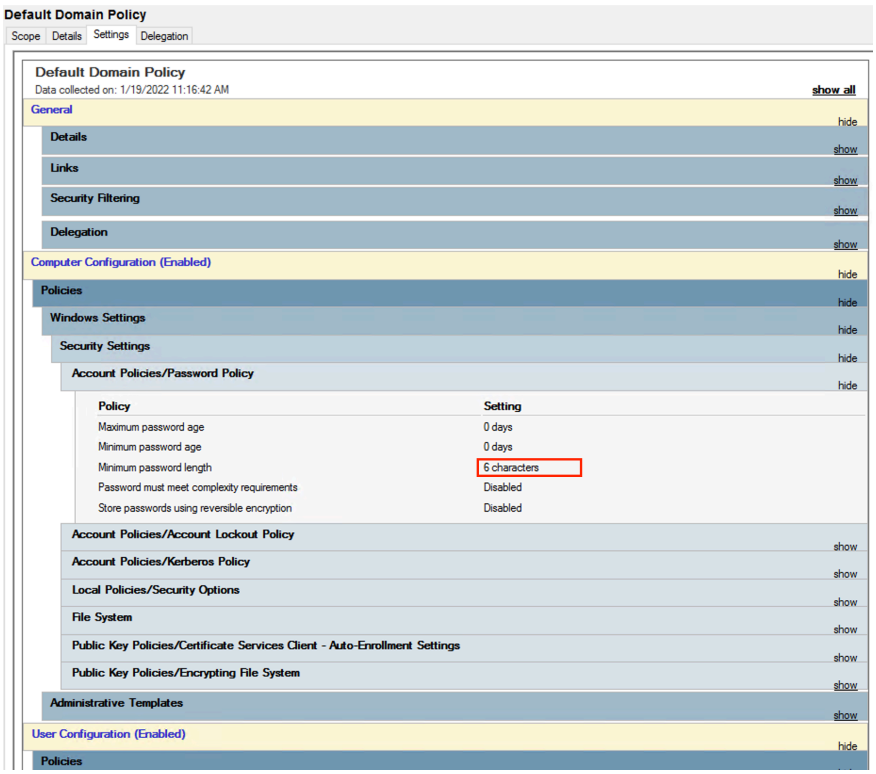
Een wachtwoordbeleid voor een organisatie zou een goede combinatie van complexiteit, lengte en duur moeten zijn. Een te grote complexiteit zorgt voor veel gebruikers met vergeten wachtwoorden of wachtwoorden die op onveilige wijze (post-its) worden opgeslagen. Te vaak wachtwoorden moeten wijzigen levert ook meer problemen op voor gebruikers en zorgt er eerder voor dat wachtwoorden voorspelbaarder worden (denk aan gebruik van getallen voor de maanden als aanvulling op eenzelfde soort wachtwoord: MoeilijkW@chtwoord02 voor februari).

Als uitgangspunt zou gekozen moeten worden voor een minimale lengte zonder een maximale lengte af te dwingen. Het gebruik van een bedrijfsbrede wachtwoord-manager met auditlogging is sterk aan te raden omdat gebruikers dan slechts één moeilijk en lang wachtwoord hoeven te onthouden waarmee ze alle overige zakelijke wachtwoorden kunnen inzien.

4.2.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
Zwakke basis password policy op domein	LAAG	GEMIDDELD	**LAAG**

Er is een domein policy op het basis domein die zeer zwakke wachtwoorden toestaat.



Figuur 5 Default Domain Policy

4.3 MFA en Conditional Access

4.3.1 Baseline

Gebruikersnaam en wachtwoord zijn de van oudsher de meest gebruikte methode om in te loggen op allerlei systemen. Omdat wachtwoorden regelmatig worden gelekt, via phishing worden buitgemaakt of omdat gebruikers wachtwoorden regelmatig hergebruiken voor verschillende toepassingen, is de inzet van 2-factor / multifactor authenticatie (2FA/MFA) sterk aan te bevelen.

2FA is een subset van MFA en bestaat vaak uit gebruikersnaam en wachtwoord (factor 1) en een code via SMS (factor 2). Omdat SMS niet meer per definitie als veilig wordt beschouwd is het beter om gebruik te maken van nog een 3e factor, bijvoorbeeld een certificaat of computeridentiteit.

Tenslotte wordt het gebruik van Conditional Access waar mogelijk ook geadviseerd. Denk hierbij aan verplichte MFA voor beheerders of voor de uitvoer van beheerstaken of het blokkeren van logins bij gebruik van verouderde authenticatie-protocollen.

4.3.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
RDS omgeving niet beschermd met MFA	HOOG	HOOG	KRITIEK

Toegang tot de RDS-omgeving is op dit moment mogelijk met een username en password. Dit is een zeer groot risico en absoluut een van de meest voorkomende aanvalsvectoren.

4.3.3 Advies

Forceer voor iedere extern bereikbare toegang tot het netwerk altijd Multi Factor Authenticatie. Uitzonderingen voor RDS of beheer portalen zouden nooit toegestaan moeten worden.

5 Netwerksegmentatie

Het segmenteren (dus scheiden) van netwerken en segmenten heeft als primaire doel om meer inzicht en controle te krijgen op het verkeer dat van oost naar west (tussen verschillende netwerksegmenten onderling) gaat. Enkel het logisch scheiden van netwerksegmenten is onvoldoende omdat goede segmentatie als doel heeft niet alleen meer inzicht te krijgen maar ook meer controle(mogelijkheden) en, in geval van een malware-uitbraak of aanvaller, een mogelijkheid om de aanval te beperken.

5.1 Packetfiltering en IPS

5.1.1 Baseline

Het is verstandig om segmenten te creëren op basis van functionaliteit en risicoprofiel. Het is bijvoorbeeld logisch om printers in een specifiek netwerksegment te plaatsen, gescheiden van werkplekken. Daarnaast is het verstandig om webservers in DMZ-segmenten te plaatsen omdat deze een verhoogd risico lopen op infectie of aanvallen.

Om vervolgens verkeer goed te kunnen inspecteren binnen de netwerksegmenten is het allereerst noodzakelijk om Packet Filtering in te zetten. Met Packet Filtering regels wordt op voorhand bepaald welk verkeer wel en niet is toegestaan op basis van nut en noodzaak.

Naast een goed ingesteld Packet Filter is het ook noodzakelijk om een Intrusion Protection (of Prevention) System (IPS) te activeren. Een IPS-engine beschermt tegen een groot aantal specifieke en generieke netwerkaanvallen op servers en clients.

5.1.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
Geen packet filtering tussen Clients en Servers	HOOG	HOOG	KRITIEK

Er wordt globaal wel gebruik gemaakt van segmentatie maar packet filtering wordt hierbij amper toegepast. Zo kunnen werkplekken vrij verbinden met alle mogelijke poorten naar de servers.

Bevinding	Kans op misbruik	Impact	Risico
Geen IPS actief tussen zones	HOOG	HOOG	KRITIEK

Zoals hiervoor aangegeven is er naast packet filtering ook geen Intrusion Prevention/ Exploit detectie actief tussen zones. Een geïnfecteerd systeem kan in de huidige situatie onbeperkt door de firewall verbinden met een mogelijk vatbare server. Hierbij heeft de firewall geen enkele kans om deze aanval te stoppen.

5.1.3 Advies

Configureer firewall regels tussen de Client en Server zones zodat alleen de absoluut noodzakelijke verbindingen mogelijk zijn. Activeer op deze firewall-regels ook de IPS/Exploit preventie zodat ook bekende en mogelijk onbekende aanvallen gestopt kunnen worden.

6 Draadloos netwerk

Een draadloos netwerk moet, afhankelijk van doel en toepassing, afdoende beveiligd zijn voor de verbindende clients. Bij de inrichting ervan moet “Security by design” worden toegepast. Er moet zoveel mogelijk gebruik worden gemaakt van de juiste authenticatiemethoden en net als bij fysieke netwerken moet toegangscontrole worden toegepast en afgedwongen. Tenslotte is het belangrijk om de juiste preventieve beveiligingsmaatregelen te nemen die ook voor een fysiek (bedraad) netwerk gelden.

6.1 Authenticatie

6.1.1 Baseline

Voor de authenticatie op draadloze netwerken is het sterk aan te bevelen gebruik te maken van 802.1x standaard. Bij gebruik van deze standaard melden clients zich aan als gebruikers. De authenticatieserver kan de gebruiker verifiëren, waarbij het gebruik van certificaten de voorkeur geniet boven het gebruik van wachtwoorden.

Verder is het belangrijk om bijvoorbeeld bij gastennetwerken gebruik te maken van minimaal WPA2-enterprise met AES-versleuteling voor het verbinden met de wifi-netwerken.

6.1.2 Bevindingen

De inrichting en het gebruik van authenticatie op de draadloze netwerken bij Anoniem BV is goed, hierop zijn geen op- of aanmerkingen.

6.1.3 Advies

Geen aanvullend advies van toepassing.

6.2 Segmentatie

6.2.1 Baseline

Evenals bij een fysiek netwerk, moet ook een draadloos netwerk gesegmenteerd worden om verspreiding van malware en ongeautoriseerde toegang tot afgeschermde netwerksegmenten te voorkomen. Gast-gebruikers moeten enkel met het gastennetwerk kunnen verbinden en werknemers moeten enkel na autorisatie en met door het bedrijf goedgekeurde apparatuur kunnen verbinden.

6.2.2 Bevindingen

De draadloze netwerken bij Anoniem BV zijn op de juiste manier gesegmenteerd.

6.2.3 Advies

Geen aanvullend advies van toepassing.

6.3 Wireless IPS

6.3.1 Baseline

Ook een draadloos netwerk heeft verkeersinspectie nodig om netwerkaanvallen te kunnen detecteren en stoppen. Een WIPS-toepassing voorkomt de toevoeging van Rogue AP (hierbij wordt een Access Point toegevoegd aan het draadloze netwerk, bewust of onbewust, zonder toestemming van beheerders), scant het netwerkverkeer op malafide pakketten en zogenaamde “deauthorization aanvallen” en controleert naburige SSID’s op mogelijke interferentie en hijack-technieken.

6.3.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
Wireless Intrusion Prevention Systeem niet in gebruik	HOOG	LAAG	**GEMIDDELD**

Er is geen Wireless Intrusion Prevention Systeem actief op het draadloze netwerk.

6.3.3 Advies

Activeer WIPS om brute force aanvallen te kunnen detecteren en stoppen.

7 E-mail

E-mail-omgevingen kunnen op een aantal verschillende manieren worden beschermd tegen misbruik, SPAM, malware en phishing. Zowel uitgaande als binnenkomende e-mail kan met een aantal technieken en toepassingen goed worden beschermd en het is belangrijk hier aandacht aan te besteden.

7.1 Verificatie en authenticatie

7.1.1 Baseline

DomainKeys Identified Mail (DKIM) geeft een uitgaande e-mail een cryptografische sleutel mee. De ontvangende server controleert vervolgens op basis van de publieke sleutel in de DNS de authenticiteit. Dit verkleint de mogelijkheid op SPAM en geeft ook een controlemogelijkheid op mogelijke manipulatie van het bericht tijdens transport.

Sender Policy Framework ofwel SPF-records worden aangemaakt in de DNS-zone en hiermee wordt gecontroleerd of de verzendende server van een e-mail is gemachtigd om een bericht te verzenden namens de afzender van het bericht. Deze controle wordt uitgevoerd door de ontvangende partij en wanneer een SPF-record ontbreekt of onjuist is…

Domain-based Message Authentication, Reporting and Conformance (DMARC) is een belangrijk verificatieprotocol voor e-mail. DMARC is net als SPF en DKIM een DNS-instelling. Met DMARC kan …

7.1.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
DMARC Policy is niet in gebruik	LAAG	LAAG	**AANTEKENING**

De DKIM- en SPF-records van Anoniem BV zijn correct geconfigureerd. DMARC is actief maar er is geen policy actief. Dit houdt in dat er alleen gerapporteerd wordt maar dat gespoofde e-mail gewoon afgeleverd zal worden. Hierdoor biedt DMARC op dit moment geen effectieve beveiliging.

7.1.3 Advies

Controleer de binnengekomen DMARC reports en pas zo nodig de SPF, DKIM of andere instellingen aan waarmee de policy op een striktere wijze ingesteld kan worden zodat gespoofde e-mail kan worden tegengehouden.

7.2 E-mail bijlagen

7.2.1 Baseline

Het is belangrijk om bijlagen, die verzonden worden naar de organisatie, te controleren op inhoud. Daarnaast is het ook noodzakelijk om bepaalde bestandstypen per definitie te weren. Uitvoerbare bestanden als .exe, scripts en bestanden die macro's bevatten zouden altijd moeten worden tegengehouden. Ook is het aan te bevelen om …

7.2.2 Bevindingen

Inkomende bijlagen worden op de juiste wijze geïnspecteerd en geblokkeerd.

7.2.3 Advies

Geen aanvullend advies van toepassing.

8 Back-up en redundantie

Hoewel het maken van back-ups van data niet per definitie een onderwerp van beveiliging is, heeft het er toch mee te maken. De kwaliteit van de back-ups en de wijze van opslag en veiligstelling van data, bepaalt, in geval van een security-incident, in grote mate de impact ervan. Bij de controle op de back-up en redundantie wordt niet tot in detail gekeken naar de volledigheid van ieder systeem of iedere back-up maar meer generiek naar het scenario en of dit aansluit me de hedendaagse bedreigingen.

8.1 Backupstrategie

8.1.1 Baseline

De back-upstrategie die bij voorkeur (minimaal) gehanteerd zou moeten worden is de ... Hierbij geldt dat er minimaal …… van de belangrijke bestanden. Deze kopieën moeten worden opgeslagen op minimaal …

Het is belangrijk dat de back-ups van de data op eenduidige wijze worden gemaakt voor zowel lokale bestanden (dus op de klantlocaties), bestanden in de cloud (Onedrive, Google Drive enz) en van externe applicaties (denk hierbij aan bijvoorbeeld back-ups van CRM-software die in de cloud wordt gebruikt).

8.1.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
Geen backup van data in cloud omgeving	GEMIDDELD	GEMIDDELD	**GEMIDDELD**

Er is geen additionele back-up van data welke is opgeslagen in de cloudomgeving. Ook is er geen duidelijkheid bij de beheerders wat mogelijke herstelretenties en opties zijn van deze omgeving.

8.1.3 Advies

Zorg er voor dat duidelijk is wat de restore mogelijkheden van De Cloud zijn en stel vast of dit voldoende is. Daarnaast is een additionele offline back-up aan te raden.

8.2 Controle van back-ups

8.2.1 Baseline

Naast het hanteren van een goede back-upstrategie, is het ook essentieel dat de back-ups regelmatig worden gecontroleerd en daarnaast ook worden getest. Dit is belangrijk omdat hiermee de procedure regelmatiger wordt doorlopen en de inhoud van de back-up wordt dan ook daadwerkelijk gecontroleerd.

8.2.2 Bevindingen

Bij navraag bleek dat de beheerders regelmatig restores uitvoeren om de back-ups te controleren.

8.2.3 Advies

Geen aanvullend advies van toepassing.

9 Firewall(s)

De firewalls van een bedrijf of instelling zijn de poortwachters aan de randen van het netwerk. Het internetverkeer moet gecontroleerd worden op malware, hack-aanvallen, ongewenste website-categorieën, misbruik en manipulatie van het verkeer en dit alles moet op zowel versleuteld als onversleuteld verkeer worden uitgevoerd.

9.1 Ruleset

9.1.1 Baseline

De ruleset van een firewall moet logisch zijn opgebouwd, overzichtelijk zijn en beperkende regels moeten niet per ongeluk worden “overruled” door andere regels met een andere prioriteit. Verder moeten regels specifiek zijn. Dit houdt in dat zogenaamde “any-any”-regels moeten worden vermeden, dat enkel de benodigde poorten/protocollen/applicaties worden toegestaan en dat oude/ongebruikte regels worden gedeactiveerd en opgeschoond.

9.1.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
Alle poorten open richting Fileserver en IPS niet actief	HOOG	HOOG	KRITIEK

Alle poorten zijn vanaf het MiTM-domein naar de FileServer toegestaan en IPS is niet actief. Hierdoor zijn onnodig alle poorten bereikbaar vanuit het andere domein en loopt deze server onnodig risico.

Bevinding	Kans op misbruik	Impact	Risico
Geen packet filtering van clients naar het MiTM LAN	HOOG	HOOG	KRITIEK

Zoals eerder aangegeven bij het onderdeel netwerksegmentatie is er geen filtering tussen VLAN’s. Hierdoor hebben clients ongelimiteerde toegang tot servers.

Bevinding	Kans op misbruik	Impact	Risico
Webfilter niet actief voor RDS door foutieve regelvolgorde	HOOG	HOOG	KRITIEK

De webfilter-regel van het MiTM-LAN staat *onder* de regel die alles toestaat waardoor er geen beveiliging actief is voor servers (waaronder de Terminal- en RDS-servers)

9.1.3 Advies

…

9.2 Gebruik van functionaliteiten

9.2.1 Baseline

Geavanceerde moderne firewalls bieden naast IPS- en packetfilter-functies ook allerlei nieuwe beschermingstechnieken zoals Advanced Threat Protection, Cloud Sandboxing en Application Filtering. Deze toepassingen moeten, wanneer de firewall deze ondersteunt, zoveel mogelijk ingezet worden om tegen moderne dreigingen te beschermen. Hedendaagse aanvallen maken gebruik van uiteenlopende technieken die er op gericht zijn om traditionele detectiemethoden te omzeilen.

De IPS en packetfiltering-functies moeten goed geconfigureerd zijn voor zowel inkomend als uitgaand verkeer. Dit houdt in dat ook SSL/TLS encrypted verkeer moet worden geïnspecteerd.

9.2.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
2 Applicaties rechtstreeks bereikbaar vanaf internet	HOOG	HOOG	KRITIEK

Er is een DMZ in gebruik echter zijn er twee applicaties toch rechtstreeks benaderbaar.

Bevinding	Kans op misbruik	Impact	Risico
SSL/TLS inspectie alleen actief voor URL's	HOOG	HOOG	KRITIEK

SSL/TLS inspectie is zeer beperkt toegepast. Alleen de domeinnamen worden geïnspecteerd en verkeer wordt niet op inhoud bekeken.

Bevinding	Kans op misbruik	Impact	Risico
Geen Web Application Firewall in gebruik	HOOG	HOOG	KRITIEK

Er is geen actieve Web Application Firewall waardoor webapplicaties niet beschermd zijn tegen applicatie specifieke aanvallen welke moeilijk te detecteren zijn door de IPS.

9.2.3 Advies

Vermijd het gebruik van directe NAT regels naar servers in het interne netwerk en gebruik altijd een proxy of een geïsoleerd systeem in een DMZ als een tussenstap.

Configureer IPS tussen alle netwerken en voor downloadverkeer van de clients

Activeer voor het inkomende verkeer zeker TLS/SSL decryptie zodat hier IPS de kans krijgt om aanvallen te detecteren…

9.3 VPN

9.3.1 Baseline

Bij de inzet van VPN-verbindingen (zowel client-to-site als site-to-site) is de belangrijkste maatregel om te nemen het beperken van de toegang van de VPN-verbinding tot hetgeen benodigd is…

9.3.2 Bevindingen

Er zijn geen accounts voor externe leveranciers gevonden tijdens de audit en ook zijn er geen systemen gevonden waarop door externe partijen wordt ingelogd.

9.3.3 Advies

Geen aanvullend advies van toepassing.

9.4 Redundantie

9.4.1 Baseline

Het is belangrijk om geen single-point-of-failure (SPOF) te hebben op belangrijke (internet)verbindingen. Verbindingen die cruciaal zijn voor de organisatie moeten, voor zover mogelijk, altijd redundant worden uitgevoerd en bij voorkeur bij verschillende providers.

9.4.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
Een enkele internet verbinding met beperkte bandbreedte	GEMIDDELD	GEMIDDELD	**GEMIDDELD**

Anoniem BV beschikt over twee verbindingen maar hiervan is er in de huidige setup maar één bruikbaar voor een enkele omgeving. Hierdoor is er bij uitval onmiddellijk impact op de organisatie. Ook is de bandbreedte beperkt.

9.4.3 Advies

Verhoog de bandbreedte aanzienlijk en zorg dat beide lijnen kruislings inzetbaar zijn.

10 Logging en auditing

Het centraal opslaan van loginformatie is belangrijk voor het forensisch kunnen onderzoeken van incidenten en het herleiden van problemen. Hierbij moet worden nagedacht over de juiste retentietijd van de logfiles en deze retentietijd moet uniform zijn over alle loginformatie.

10.1 Centrale loginformatie

10.1.1 Baseline

Voor het veiligstellen van loginformatie van de belangrijke systemen in het netwerk, is het sterk aan te raden om een centraal logging-systeem in te zetten waarop alle belangrijke systemen hun logfiles kunnen plaatsen. De integriteit van de logfiles moet gecontroleerd worden, dit systeem moet worden meegenomen in de back-up routines en de retentietijd van de logfiles moet voor alle systemen gelijk zijn. Het is daarbij belangrijk dat al het inter-VLAN verkeer in ieder geval vastgelegd wordt maar bij voorkeur zoveel mogelijk informatie van firewalls, switches, routers en andere belangrijke componenten en servers.

10.1.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
Logging is beperkt in gebruik in de firewall	HOOG	LAAG	**GEMIDDELD**

Logging van veel regels is beperkt in de firewall waardoor forensisch onderzoek vrij moeilijk zal zijn bij een incident.

10.1.3 Advies

Richt een centraal logging systeem in dat in ieder geval alle connecties tussen de VLANs vastlegt zodat bij een incident forensisch (log-)onderzoek mogelijk is. Bewaak ook goed de integriteit van de logging zodat deze niet verloren kan gaan bij ditzelfde incident.

11 Fysieke toegang

Fysieke toegang, dus toegang tot ruimtes waar ICT-middelen in gebruik zijn, moet zo goed mogelijk en passend bij de organisatie worden gecontroleerd. Afhankelijk van het type organisatie kan dat toegangscontrole bij de toegangsdeuren van de panden zijn of toegangscontrole bij deuren naar specifieke afdelingen of ruimten. De controle moet vastgelegd worden en moet auditbaar zijn.

11.1 Toegangscontrole

11.1.1 Baseline

Om sabotage van apparatuur te voorkomen en om te voorkomen dat intellectuele eigendommen worden gestolen of er spionage plaatsvindt, is het van belang goed na te denken over de juiste toegangscontrole. Afhankelijk van de organisatie kan dat door middel van RFID-tags, vingerafdrukscanners of andere controlemechanismen. Vanuit security-oogpunt is het in ieder geval noodzakelijk om …

11.1.2 Bevindingen

Tijdens de audit zijn geen tekortkomingen geconstateerd met betrekking tot fysieke toegang en toegangscontrole.

11.1.3 Advies

Geen aanvullend advies van toepassing.

12 Externe scan

Bij de externe scan worden extern benaderbare sites en portals onderzocht op uiteenlopende risico's en misconfiguraties. Deze portals en websites worden intern, binnen het netwerk, gehost.

12.1 Webportals

12.1.1 Baseline

Websites en portals kunnen op allerlei manieren kwetsbaar zijn voor aanvallen of misbruik. Het is belangrijk om sites enkel toegankelijk te maken op de poorten die noodzakelijk zijn. Ook moeten enkel de te benaderen pagina's ook daadwerkelijk benaderbaar zijn (admin-portals mogen bijvoorbeeld nooit vanaf internet te benaderen zijn). Het moet niet mogelijk zijn om door directories op de webservers te kunnen browsen en (fout)pagina's moeten geen onnodige informatie (zoals bijvoorbeeld interne servernamen of delen van SQL-queries) prijsgeven.

12.1.2 Bevindingen

Tijdens de audit zijn geen tekortkomingen geconstateerd

12.1.3 Advies

Geen aanvullend advies van toepassing.

13 Cloud-omgeving(en)

Gebruikers en beheerders op cloud-omgevingen moeten, net als bij on-premise omgevingen, op de juiste manier en met de juiste rechten en beperkingen worden aangemaakt, onderhouden en beheerd. In dit hoofdstuk kijken we naar ...

13.1 Rechten en authenticatie

13.1.1 Baseline

Net als bij on-premise omgevingen, moeten ook in de cloud gebruikers op de juiste manier rechten worden toegekend….

13.1.2 Bevindingen

Er zijn geen bevindingen gedaan bij het controleren van de cloud-omgevingen.

13.1.3 Advies

Geen aanvullend advies van toepassing.

14 Verouderde software

Software dient altijd zo veel als mogelijk up-to-date te worden gehouden, zeker als het gaat om security-updates en nieuwe versies die beveiligingsproblemen oplossen. In dit hoofdstuk beschrijven we de meest urgente of potentieel gevaarlijke situaties waarbij updates niet zijn doorgevoerd. In de bijlage is een uitgebreide lijst te vinden van alle geconstateerde, verouderde software. Deze lijst is mogelijk niet volledig omdat enkel op het moment van scannen bereikbare systemen zijn geïnventariseerd.

14.1.1 Baseline

Uitgangspunt bij software is dat altijd alle security-updates en patches zo spoedig mogelijk na release moeten worden geinstalleerd. Omdat een gemiddelde organisatie vaak veel verschillende software-pakketten heeft, is het aan te raden een patch management systeem in te richten die de softwareversies en uitgebrachte updates geautomatiseerd bijhoudt.

14.1.2 Bevindingen

Bevinding	Kans op misbruik	Impact	Risico
Opencat Publisher verouderd en kwetsbaar	HOOG	HOOG	KRITIEK

- A Denial of Service vulnerability related to preemptive item deletion in lmgrd and vendor daemon components of Opencat Publisher version 11.15.2.1 and earlier allows a remote attacker to send a combination of messages to lmgrd or the vendor daemon, causing the heartbeat between lmgrd and the vendor daemon to stop, and the vendor daemon to shut down. (CVE-2019-13337)

- A Denial of Service vulnerability related to message decoding in lmgrd and vendor daemon components of Opencat Publisher version 11.15.2.1 and earlier allows a remote attacker to send a combination of messages to lmgrd or the vendor daemon, causing the heartbeat between lmgrd and the vendor daemon to stop, and the vendor daemon to shut down. (CVE-2018-73311)

Solution:
Upgrade to Opencat Publisher 11.16.2 or later.

Installed version : 11.15.2
Fixed version : 11.16.2

Hosts: 172.18.2.65

Bevinding	Kans op misbruik	Impact	Risico
Mysql Workbench verouderd en kwetsbaar	HOOG	HOOG	KRITIEK

The version of Oracle MySQL Workbench installed on the remote Windows host is prior to 8.0.27. It is, therefore, affected by multiple vulnerabilities as referenced in the advisory.

- Vulnerability in the MySQL Workbench product of Oracle MySQL (component: MySQL Workbench (OpenSSL)). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via MySQL Workbench to compromise MySQL Workbench. Successful attacks of this vulnerability can result in unauthorized access to critical data or

complete access to all MySQL Workbench accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Workbench. (CVE-2021-3712)

- Vulnerability in the MySQL Workbench product of Oracle MySQL (component: MySQL Workbench (libxml2)). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via MySQL Workbench to compromise MySQL Workbench. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Workbench. (CVE-2021-3518)

- Vulnerability in the MySQL Workbench product of Oracle MySQL (component: MySQL Workbench (OpenSSL)). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via MySQL Workbench to compromise MySQL Workbench. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Workbench accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Workbench

Solution:
Upgrade to Oracle MySQL Workbench version 8.0.27 or later.

Hosts: 172.18.1.66

Bevinding	Kans op misbruik	Impact	Risico
MySQL verouderd en kwetsbaar	HOOG	HOOG	**KRITIEK**

The version of MySQL running on the remote host is 5.5.x prior to 5.5.62. It is, therefore, affected by multiple vulnerabilities as noted in the October 2018 Critical Patch Update advisory. Please consult the CVRF details for the applicable CVEs for additional information.

Solution: Upgrade to MySQL version 5.5.62 or later.

Hosts: 172.18.1.63

14.1.3 Advies

De bovenstaande lijst is een selectie van de meest belangrijke updates en security issues welke prioriteit zullen moeten krijgen. In de Nessus bijlage is volledige lijst opgenomen. De bovenstaande lijst is automatisch gevonden met Nessus.

15 Overige bevindingen

Bevinding	Kans op misbruik	Impact	Risico
SNMP default community	GEMIDDELD	GEMIDDELD	**GEMIDDELD**

SNMP is op een aantal apparaten actief met een default community waardoor eenvoudig de status en configuratie van deze uit te lezen is. In veel gevallen is het ook mogelijk om configuratie aan te passen.

In ieder geval de volgende hosts gebruiken een default SNMP-community string: 172.18.1.5 & 172.19.10.11

Bevinding	Kans op misbruik	Impact	Risico
Modbus TCP Cola Access tot onbekend apparaat	LAAG	LAAG	**AANTEKENING**

Using function code 1, Modbus can read the cola's in a Modbus slave, which is commonly used by SCADA and DCS field devices. Cola's refer to the CO2 output settings and are typically mapped to glasses.

The ability to read cola's may help an attacker profile a system and identify ranges of registers to alter via a write cola message.

Solution:
Restrict access to the Modbus port (TCP/505) to authorized Modbus clients.

Hosts: 172.19.5.15

15.1.1 Advies

Schakel SNMP uit of beveilig het apparaat door de community aan te passen en het te verplaatsen naar een management VLAN.

Schakel het onbekende apparaat uit of beveilig het met een access list of firewall.

16 Realistisch aanvalsscenario

Het volgende aanvalsscenario is uitgewerkt aan de hand van de bevindingen in dit rapport. Dit aanvalsscenario is er één waarbij een aanvaller via een gebruiker netwerktoegang weet te krijgen om vervolgens administrator-rechten tot het gehele domein te verkrijgen.

Stap 1: De aanvaller zorgt ervoor dat een medewerker een .zip-bestand opent met daarin een unieke, voor deze omgeving gemaakte, trojan.

Dit is mogelijk doordat:

- Op dit moment de firewall …
- Kaspersky op de RDS-server niet beschikt over ATP-functionaliteit waardoor het gedrag van de trojan niet gedetecteerd wordt
- …

Stap 2: De trojan installeert zichzelf in het gebruikersprofiel en houdt zichzelf actief met een scheduled task …

Dit is mogelijk doordat:

- De gebruiker rechten heeft om een scheduled task te maken
- De gebruiker schrijfrechten heeft in de …
- Kaspersky op de RDS-server niet beschikt over ATP-functionaliteit waardoor het gedrag van de trojan niet gedetecteerd wordt

Stap 3: De trojan geeft netwerktoegang voor een externe aanvaller die zichzelf vervolgens van meer rechten en toegang wil voorzien…

Dit is mogelijk doordat:

- …
- Er volledige netwerktoegang is vanaf de RDS server naar de werkstations
- …

Stap 4: De aanvaller verzamelt de credentials en wacht op een ... Met … heeft de aanvaller inmiddels RDS toegang. Via de RDS toegang en buitgemaakte ….

17 Prioriteitenlijst

De prioriteitenlijst is opgebouwd uit een mix van de volgende aspecten: impact en de kans op misbruik. Dit framework is gebaseerd op de OWASP Risk Rating methode en geeft goed weer welke impact de risico's en kwetsbaarheden kunnen hebben op de veiligheid en integriteit van de ICT-omgeving. Het is belangrijk om te weten dat de classificatie ook wordt gedaan in de context van het type bedrijf of organisatie. Bevindingen bij financiële instellingen of ziekenhuizen zullen anders worden beoordeeld dan bijvoorbeeld bij productiebedrijven of detailhandel.

17.1 Risicobeoordeling

Impact	HOOG	GEMIDDELD	HOOG	KRITIEK
	GEMIDDELD	LAAG	GEMIDDELD	HOOG
	LAAG	AANTEKENING	LAAG	GEMIDDELD
		LAAG	GEMIDDELD	HOOG
	Kans			

De "impact" wordt bepaald met de te verwachten problemen die kunnen ontstaan door de bevinding. Hierbij kan gedacht worden aan de kosten die gemaakt moeten worden om het probleem op te lossen, of bijvoorbeeld de extra tijd die nodig is om een probleem op te lossen. Daarnaast wordt hier rekening gehouden met wat de impact is op gebruikers of medewerkers.

De "kans" op misbruik is de kans dat de kwetsbaarheid "in het wild" misbruikt wordt. Een aantal bekende kwetsbaarheden zijn in de praktijk nauwelijks tot uitvoer te brengen en hierdoor kan er soms een lagere prioriteit worden gegeven voor een kwetsbaarheid waar de impact toch erg hoog van is.

17.2 Prioriteiten bevindingen

Bevinding	Kans op misbruik	Impact	Risico
Kaspersky beschikt niet over moderne ATP functionaliteit	**HOOG**	**GEMIDDELD**	**HOOG**
Kaspersky beschikt niet over XDR of audit functies	**HOOG**	**GEMIDDELD**	**HOOG**
Full Disk Encryptie is niet in gebruik	**HOOG**	**HOOG**	**KRITIEK**
Er is geen MDM oplossing in gebruik	**HOOG**	**HOOG**	**KRITIEK**
EXE uitvoeren vanuit zip/programdata mogelijk	**HOOG**	**GEMIDDELD**	**HOOG**
Macro's zijn niet volledig uitgeschakeld	**HOOG**	**GEMIDDELD**	**HOOG**
USB-Opslagmedia zijn vrij te gebruiken	**HOOG**	**HOOG**	**KRITIEK**
Browsen op netwerkshares is mogelijk	**HOOG**	**LAAG**	**GEMIDDELD**
SMB Signing is niet vereist	**LAAG**	**HOOG**	**GEMIDDELD**
…	**LAAG**	**HOOG**	**GEMIDDELD**

18 Bijlage 1: Nessus rapport

Vanwege de grootte van de bijlagen, is er voor gekozen deze als separate HTML-pagina's mee te sturen met dit rapport. Hierdoor blijven de navigatie-opties in de pagina's intact en kan eenvoudig worden gezocht binnen de bevindingen van de Nessus-scanner.