Sector Rapport

Red Cell assessments

in opdracht van

MBO Digitaal

OPENBAAR

MBO-Digitaal-Sectorrapport-REPORT-v1.1.pdf
Ben Brücker, BSc., OSCP, GXPN, SEPP
Versie 1.1
13 December 2023

Over Secura

Sinds 2000 helpt Secura bedrijven, (zorg-)organisaties en (lokale) overheden bij het identificeren, verminderen en voorkomen van IT-beveiligingsrisico's. Dit doen we door het uitvoeren van audits, waaronder hoogwaardige beveiligingsonderzoeken- en beoordelingen, consultancy, penetratietests en certificering van producten en diensten.

Sinds 2021 is Secura onderdeel van Bureau Veritas (BV), wat betekent dat Bureau Veritas de meerderheid van aandelen in bezit heeft. Bureau Veritas is een beursgenoteerde onderneming (Euronext: BVI), gespecialiseerd in testen, inspecteren en certificeren. Bureau Veritas is opgericht in 1828, heeft meer dan 75.000 werknemers en is aanwezig in 140 landen. Secura vormt de hoeksteen binnen de cyberbeveiligingsstrategie van Bureau Veritas.

Op Europees niveau draagt Secura bij aan de ECSO (European Cyber Security Organization) om internationale samenwerking en standaardisatie te bevorderen (ook gekoppeld aan de EU Cyber Security Act). Op nationaal niveau participeert Secura in Cyberveilig Nederland. Secura is als een van de weinige bedrijven door de Nederlandse overheid geaccrediteerd voor het Baseline Security Product Assessment (BSPA) schema. Secura heeft in 2021 als eerste bedrijf in Nederland het keurmerk ontvangen voor 'Centrum voor Criminaliteitspreventie en Veiligheid (CCV) gecertificeerd pentest bedrijf'. Dit betekent dat onze pentesten worden uitgevoerd door gekwalificeerd personeel via een gestructureerde aanpak wat resulteert in een helder leesbaar rapport.

Secura hecht ook waarde aan het delen van kennis en ervaring door onze klanten te helpen met effectieve trainingen. Bovendien bieden wij een programma (SAFE®) aan dat is gericht op het overbruggen van de kloof tussen bewustwording (awareness) en gedrag. Daarnaast ontwikkelen wij krachtige tools zoals de Secure File Exchange (SFE): een gebruiksvriendelijk platform om gevoelige informatie (zoals onze rapportages) op de meest veilige manier te delen.

Secura B.V.

Vestdijk 59
5611 CA EINDHOVEN
The Netherlands

Herikerbergweg 15
1101 CN AMSTERDAM
The Netherlands

T +31 (0)40 23 77 990

E info@secura.com

W https://www.secura.com

INHOUDSOPGAVE

1. MANAGEMENTSAMENVATTING

In de periode van augustus tot en met oktober 2023 heeft Secura drie gelijktijdige Red Cell-assessments bij MBO-instellingen uitgevoerd op verzoek van MBO Digitaal. Bij Red Cell wordt de weerbaarheid van een organisatie tegen kwaadwillenden getest. Tijdens deze Red Cell-assessments nam Secura de rol van een aanvaller aan, waarbij cybercriminele organisaties werden gesimuleerd, met als doel toegang te krijgen tot gevoelige gegevens of systemen zoals Microsoft365-omgevingen, financiële en student-gegevens.

Red Cell is een digitale brandoefening in een verkort tijdsbestek in vergelijking met een volledige Red Teaming-assessment, waarbij verschillende realistische aanvalspaden worden gevolgd, in plaats van dekkend onderzoek naar (succesvolle) beveiligingsmaatregelen per systeem. Er wordt gezocht naar het pad van de minste weerstand richting de kroonjuwelen, net zoals een echte aanvaller zou doen. Dit biedt nieuwe inzichten in weerbaarheid tegen social engineering- en cyber-aanvallen. Vervolgens worden aanbevelingen gegeven voor aanvullende verdedigingsmaatregelen. Deze maatregelen zijn van toepassing op niveaus van mens, proces- en technologie.

1.1. Doel van het onderzoek

Het programma Cyberveiligheid heeft als doel om de cyberweerbaarheid van de mbo-sector te vergroten. Eén van de aandachtsgebieden van het programma is technische weerbaarheid. Red Teaming vormt daar een belangrijk onderdeel van. Vanuit het programma heeft MBO Digitaal voor drie scholen een Red Teaming oefening gefaciliteerd met drie doelen:

1. Verbeteren cyberweerbaarheid onderzochte instellingen Het eerste doel richt zich op het identificeren van kwetsbaarheden en mogelijke aanvalspaden die cybercriminelen kunnen bewandelen. De bevindingen van het onderzoek stellen de onderzochte instellingen in staat om hun cyberweerbaarheid aanzienlijk te verbeteren.
2. Verbeteren cyberweerbaarheid in de mbo-sector Door lering te trekken uit en het delen van de voornaamste bevindingen van de onderzoeken bij de drie scholen stelt de sector in staat om haar cyberweerbaarheid te verbeteren.
3. Ontwikkelen van een modelaanpak voor Red Teaming Door vanaf de zijlijn mee te kijken naar het verloop van het Red Teaming proces kan lering getrokken worden uit de zaken die (minder) goed verliepen. Deze kennis en ervaring stelt SURF en MBO Digitaal in staat om een geschikte modelaanpak voor Red Teaming te ontwikkelen en onder te brengen bij SURF als dienst.

1.1.1. Betrokkenheid van SURF bij deze assessments

Voor SURF vallen de testen binnen het thema ’Testen en Toetsen’ van het Security Expertise Centrum (SEC). Binnen het SEC begeleiden we onderwijs- en onderzoeksinstellingen bij het opzetten en uitvoeren van verschillende soorten cybersecuritytesten. Red- of purple-teaming is daar een onderdeel van, maar denk ook aan cybercrisioefening (N)OZON, pentesten, vulnerability scanning en hack-events zoals HALON. Als onderdeel van de dienstverlening neemt SURF plaats in white-teams bij grote en kleine tests; om kennis en ervaring te delen, en om de instellingen (capaci)tijd te besparen.

1.2. Samenvatting van de resultaten

Gedurende deze onderzoeken was Secura positief verrast over het niveau van volwassenheid van de organisaties op het gebied van beveiliging, detectie en mitigatie. Wel zijn er daarnaast een aantal belangrijke kwetsbaarheden waargenomen waarbij de mitigatie het risico voor de betrokken organisaties sterk zou verminderen. De volgende tabel geeft een overzicht van de assessments in cijfers:

Categorie	Observatie
Security Maturity	De waargenomen security maturity voor alle drie de doelorganisaties was hoger dan verwacht, vergeleken met soortgelijke organisaties. Positieve bevindingen waren vooral gerelateerd aan uitgebreide monitoring- en response-capaciteiten.
Toegang tot kroonjuwelen	Secura heeft in totaal 3 van in totaal 17 vlaggen gerelateerd aan kroonjuwelen weten te verkrijgen.
Active Directory overname	In 1 van de 3 assessments zijn de hoogste rechten binnen de Active Directory verkregen door Secura.
Aantal gekraakte wachtwoorden	11.680, waaronder studenten, docenten, beheerders en service accounts.
Geraden wachtwoorden	In totaal zijn de wachtwoorden van 70 accounts, verspreid over alle drie organisaties, gecompromitteerd door middel van het raden van zwakke wachtwoorden. Ook hier ging het om studenten, docenten en beheerders.
Phishing resultaten	Verdeeld over de organisaties hebben in totaal 48 van 145 gebruikers (33%) op phishing-links geklikt. Van deze 48 gebruikers hebben 28 hun inloggegevens afgestaan op de phishing-website.
Gerapporteerde Phishing Campagnes	Alle drie phishing campagnes zijn onderkend en passende maatregelen zijn genomen.
Detectie van technische aanvallen	Alle drie organisaties detecteerden op enig moment technische aanvallen tijdens de assessments. De assessments zijn vervolgens voortgezet onder het perspectief van een ‘assumed breach’.

Tabel 1.1: Resultaten van de assessments in cijfers

Naar aanleiding van de resultaten raadt Secura aan om de volgende zaken met prioriteit op te pakken binnen uw organisatie:

- Controleer de configuratie van Active Directory Certificaatsjablonen (ADCS). Deze worden in de praktijk veelvuldig gebruikt om hoge rechten in een Active Directory te verkrijgen. (Zie aanbeveling 6 op pagina 11)
- Om de risico’s van gestolen wachtwoorden verder te minimaliseren, is het van cruciaal belang om Multi-Factor Authenticatie (MFA) te activeren op alle applicaties en portalen. (Zie aanbeveling 1 op pagina 9)
- Train medewerkers regelmatig in het herkennen van social engineering-aanvallen om het bewust zijn op het gebied van IT-beveiliging te vergroten. Herhaal deze training regelmatig. Maak het ook makkelijk voor medewerkers om phishing-pogingen te melden door functionaliteit in de gebruikte e-mailclients in te schakelen. Beloon ten slotte medewerkers die regelmatig phishing-e-mails melden om hen te stimuleren hun mindset binnen uw bedrijf te delen. (Zie aanbeveling 11 op pagina 14)
- Omdat scholen open instellingen zijn en het is niet haalbaar om mensen te verhinderen binnen te komen. Hoewel het waar is dat het moeilijk is om iedereen te stoppen van het betreden van het gebouw, kan het beveiligingsbewustzijn van medewerkers voorkomen dat mensen toegang krijgen tot gevoelige locaties. (Zie aanbeveling 9 op pagina 13)
- Segmenteer het netwerk in gescheiden delen om de veiligheid te verhogen. Gebruik firewallregels om alleen toegang te verlenen aan systemen die deze specifieke netwerkdelen nodig hebben. (Zie aanbeveling 5 op pagina 10)

De volgende secties geven een overzicht van de belangrijkste gedeelde resultaten van deze assessments.

Technische bevindingen

RADEN VAN WACHTWOORDEN

- **Positief:** Hoewel er gaten zijn in de dekking van Multi-factor Authenticatie (MFA), was het positief om te zien dat MFA ook was ingeschakeld voor systemen op het interne netwerk, waardoor de impact van gestolen en gelekte wachtwoorden sterk werd beperkt.
- **Bevinding:** Zwakke wachtwoorden waren in alle organisaties toegestaan.
- **Bevinding:** Er was geen limiet aan het raden van wachtwoorden op de interne netwerken waardoor, in combinatie met het zwakke wachtwoordbeleid, in totaal 70 accounts zijn gecompromitteerd.
- **Bevinding:** Multi-Factor Authenticatie (MFA) wordt bijna overal afgedwongen, maar er zijn enkele gaten waar geraden of gelekte wachtwoorden kunnen worden uitgebuit.

BEPERKTE NETWERK-SEGMENTATIE

- **Bevinding:** Segmentatie tussen kantoorautomatisering en servers wordt niet overal afgedwongen. Dit stelt aanvallers in staat om servers en beheersystemen aan te vallen vanuit het perspectief van een Bring Your Own Device (BYOD) of een gecompromitteerde werkstation.
- **Bevinding:** Er waren beperkte of geen maatregelen om te voorkomen dat ongeoorloofde systemen verbinding maakten met het interne netwerk.

ACTIVE DIRECTORY MISCONFIGURATIES

- **Bevinding:** Er werden kwetsbaarheden ontdekt in de configuratie van de zogenaamde Active Directory Certificate Services (ADCS). Deze kwetsbaarheden worden vaak uitgebuit om privileges binnen het domein te verhogen.
- **Bevinding:** Inloggegevens worden soms opgenomen in zogenaamd “AD group policies”. Hierdoor kan elke domeingebruiker deze uitlezen.

Beveiligingsbewustzijn

PHISHING

- **Positief:** Multi-factor Authenticatie (MFA) was ingeschakeld op een groot percentage van de systemen, waardoor de impact van gestolen en gelekte wachtwoorden sterk werd beperk.
- **Positief :** Alle drie phishingaanvallen werden op een bepaald moment onderkend en de Blue Teams werden gealarmeerd.
- **Bevinding:** Phishing is nog steeds een van de meest voorkomende aanvallen waar soortgelijke organisaties mee te maken krijgen, en dit wordt weerspiegeld in de resultaten: Succesvolle phishingaanvallen werden uitgevoerd tegen alle drie ROCs. 19% van alle doelwitten voerde hun inloggegevens in op phishingpagina's.

FYSIEKE TOEGANG

- **Bevinding:** Social Engineers worden meestal niet uitgedaagd door medewerkers. Dit stelt de Social Engineers in staat om apparaten voor toegang op afstand aan de netwerken toe te voegen en vervolgaanvallen uit te voeren vanuit de interne netwerken.
- **Bevinding:** Alle organisaties zijn open en uitnodigend, zoals past bij ROCs, maar het nadeel is dat er weinig kans is om deze aanvallen te stoppen. Overweeg om gebruik te maken van gelaagde beveiliging waarbij bijvoorbeeld voor kantoren en andere belangrijke omgevingen additionele toegangsmiddelen verplicht zijn. Daarnaast was ook de gelaagde netwerktoegang en beveiliging niet altijd voldoende om aanvallers met fysieke toegang te stoppen.

Detectie bevindingen

DETECTIE

- **Positief:** Veel aanvallen op werkplekken en netwerken zijn gedetecteerd.
- **Bevinding:** Aanvallen waarbij wachtwoorden op het interne netwerk worden geraden werden niet altijd gedetecteerd.
- **Bevinding:** De vertraging tussen een kwaadaardige actie door een aanvaller en de detectie door een Security Operations Center (SOC) kan soms lang zijn, van uren tot een dag.
- **Bevinding:** Phishing wordt niet gemeld door een groot percentage van de gebruikers, waardoor een belangrijke informatiebron buiten de detecties voor Blue Teams blijft.

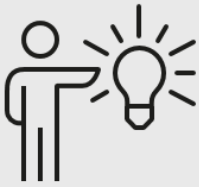
ATTRIBUTIE

- **Bevinding:** De correlatie van acties met een lopende aanval was meestal relatief snel vanwege de nauwe samenwerking tussen verdedigers. Maar deze informatie wordt nog niet gedeeld tussen organisaties.

MITIGATIE

- **Positief:** Apparaten voor Toegang op afstand zijn gedetecteerd en opgespoord na verdacht gedrag op het network.
- **Positief:** Geïmplementeerde Endpoint Detection and Response (EDR) software is zeer effectief in het stoppen van bepaalde categorieën aanvallen, en geeft verdedigers toegang tot extra detectie- en mitigatie-maatregelen.
- **Positief:** Het isoleren van systemen in het geval van verdacht gedrag is succesvol uitgevoerd.

Procesverbeteringen



TIMING

- **Positief:** Bij de meeste organisaties ging communicatie voorspoedig. Een open communicatie draagt bij aan een snelle doorlooptijd van het project.
- **Bevinding:** Kort na de zomervakantie is een minder geschikt moment voor het uitvoeren van dergelijke aanvallen. Gedurende deze weken is de beschikbaarheid van personeel niet optimaal.

VOORBEREIDING

- **Bevinding:** De voorbereiding van de opdrachten was nog niet optimaal vanwege een mismatch in verwachtingen en kennis tussen het Red Team en de deelnemende partijen. Hier is het aan te raden dat het Red Team een veel meer begeleidende rol aanneemt en de voorbereiding bij voorkeur ten minste 6 weken voor start onderzoek uitvoert.
- **Bevinding:** Er is een strakkere afstemming nodig waarbij voor begin van het onderzoek voor iedereen duidelijk is hoe er omgegaan moet worden bij detecties door de verdedigers.
- **Bevinding:** Hulp van de organisatie aan het Red Team, zogenaamde leg-ups moeten van tevoren helder zijn en in lijn liggen met het type onderzoek dat wordt uitgevoerd.

TYPE ONDERZOEK

- **Bevinding:** De onderzoeken zijn uitgevoerd volgens het Red Cell-methodologie waarbij er minder focus is op het omzeilen van de verdedigers en het correleren van aanvallen aan detecties. Dit bleek minder aan te sluiten bij de behoeften van de deelnemende ROCs. Een volledig Red Teaming-assessment geeft hiervoor meer mogelijkheden.

2. WAT IS RED TEAMING / RED CELL?

Red Teaming is een beveiligingsdiscipline die oorspronkelijk uit de militaire arena komt en waarbij cyberaanvallen over het gehele spectrum worden gesimuleerd. Hierdoor kunt u de effectiviteit van uw cyberverdediging tegen kwaadwillende actoren meten en kunnen uw verdedigers hun detectie- en reactiecapaciteiten oefenen in een gecontroleerde omgeving en deze vervolgens inspecteren en verfijnen. Ten slotte kan het Red Team ook tekortkomingen in uw algehele verdediging blootleggen aangezien het zich op de gehele organisatie richt en niet wordt beperkt door de restricties van een reguliere penetratietest.

De assessments voor de deelnemende MBO-instellingen zijn uitgevoerd volgens de **Red Cell**-methodologie. Hier wordt een beperkte Red Teaming assessment uitgevoerd in een korter tijdsbestek waardoor er minder focus is op 'stealth' en het ontwijken van het Blue Team. Hierdoor kan het Red Team sneller richting de doelen bewegen en binnen een kleiner budget ten kosten van een gedeelte van het realisme van het onderzoek.

Gedurende deze Red Cell-assessments zijn onder andere de volgende acties ondernomen samen met de MBO-instellingen om binnen de beschikbare onderzoekstijd te blijven:

- Allowlisting van phishing- en C2-domeinen.
- Het tegenhouden van blokkerende acties van de verdedigers na detectie.
- Waar nodig het aanleveren van test-accounts.

2.1. De Teams

Binnen Red Teaming / Red Cell wordt er verschil gemaakt in de volgende teams:

Red Team

Tijdens een Red Teaming assessment neemt het Red Team de rol aan van een vijandige aanvaller die de cyberbeveiliging van de organisatie uitdaagt. Op dit moment worden realistische aanvalsscenario's gesimuleerd. Dit betekent dat de verdedigers niet (volledig) weten wat het Red Team aan het doen is. Vaak zijn er maar weinig mensen op de hoogte van het feit dat er een RT-assessment wordt uitgevoerd, zodat de 'echtheid' van deze 'digitale brandoefening' optimaal is. Daarom is het nodig om ook aan de klantzijde teams aan te stellen.

Blue Team

Het Blue Team is verantwoordelijk voor het verdedigen van de netwerken, systemen en applicaties. Dit zijn uw belangrijkste middelen bij het detecteren, beantwoorden en beperken van cyberaanvallen. Dit team is meestal niet op de hoogte van deze simulatie om het realisme te verhogen en de respons te testen.

White Team

Het White Team fungeert als schakel tussen het Red Team en het Blue Team en is de directe opdrachtgever voor het Red Team. Het White Team bestaat uit medewerkers van uw organisatie en Secura, die kunnen escaleren en de-escaleren met het Blue Team en het Red Team. Dit team wordt op de hoogte gebracht van alle aanvallen door het Red Team en heeft het mandaat om aanvallen te starten, te stoppen en goed te keuren.

Purple Team

Het Blue Team wordt over het algemeen niet op de hoogte gebracht van deze simulatie om het realisme en de testrespons te vergroten. In sommige gevallen kan het Blue Team tijdens de Red Teaming oefening worden ingelicht, zodat er geen onnodige tijd wordt verspild aan zaken waar het White Team al van af weet. In een dergelijk geval wordt onderweg samen met het Blue Team actie ondernomen en wordt er dan van "Purple Teaming"gesproken.

3. ONDERLIGGENDE OORZAKEN EN AANBEVELINGEN

In dit hoofdstuk worden uitspraken gedaan over de onderliggende oorzaken van de meest significante gemeenschappelijke bevindingen. Daarnaast zullen er praktische, operationele aanbevelingen worden voorgesteld om de cyberweerbaarheid verbeteren.

3.1. Technische aanvallen

Als gevolg van technische kwetsbaarheden was Secura in staat om bij de meeste organisaties:

- Vrijwel onbeperkt wachtwoorden te raden.
- De hoogste privileges binnen het interne netwerk te verwerven vanuit een aanvankelijk niet-geauthenticeerd perspectief door het benutten van kwetsbaarheden in het wachtwoord- en lockout-beleid.
- De gebruikersnamen en wachtwoorden van een groot percentage van de domein gebruiker te compromitteren, inclusief studenten, leraren, beheerders en serviceaccounts. Dit is bereikt door het kraken van wachtwoordhashes die verkregen werden via domeinbeheerdersrechten.
- Toegang te verkrijgen tot netwerkbronnen die niet beschermd zijn door MFA.
- Toegang te verkrijgen tot een groot aantal systemen vanuit het perspectief van een BYOD-apparaat of gecompromitteerd werkstation. Dit werd veroorzaakt door te beperkte netwerksegmentatie.
- Gebruik te maken van kwetsbaarheden van de Active Directory Certificate Services.

De onderliggende redenen voor deze kwetsbaarheden zijn:

Onveilige beheer methodieken; De onveilige IT beheer methodieken die door de organisaties wordt gebruikt, veroorzaakten verschillende bevindingen. Zo zijn aanvallers in staat om zich door het netwerk te bewegen doordat accounts met hoge privileges worden gebruikt om administratieve taken uit te voeren die deze hoge privileges niet vereisen. Ook worden accounts met hoge privileges op dezelfde systemen gebruikt als veel lager geprivilegieerde accounts. Dit stelt een aanvaller in staat om mogelijk de privileges van lager geprivilegieerd account te escaleren naar het hoger geprivilegieerd account.

Onvoldoende sterk wachtwoordbeleid; De sterkte van de afgedwongen wachtwoord eisen was onvoldoende sterk. Ook is er geen goede account lockout policy ingesteld om aanvallen te stoppen die van zwakke wachtwoorden gebruikmaken.

Onvoldoende netwerksegmentatie en -filtering; Tijdens de toegangs-fase van deze assessments begon Secura hun aanval vanuit een regulier werkstation. Er werden slechts beperkte netwerksegmentaties waargenomen die er zijn om normale gebruikers te weerhouden van toegang tot gevoelige servers en applicaties. Bovendien had een groot aantal servers directe uitgaande internettoegang, wat het voor aanvallers eenvoudiger maakt om een commando- en controlekanaal naar een externe server op het internet op te zetten.

Onveilige Active Directory beveiligingsbeleid; Een aantal van de geïdentificeerde kwetsbaarheden is wijten aan misconfiguraties in de AD Certificate Services dienst. Omdat het hier niet direct gaat om een technische kwetsbaarheid, maar om een misconfiguratie is het aan te raden om additionele informatie over deze aanvallen te verspreiden naar de beheerders. Daarnaast is er geen eenduidig beleid over AD beveiligingsrichtlijnen, hierdoor zijn andere misconfiguraties aangetrokken zoals wachtwoorden die zijn opgenomen in group policies.

3.1.1. Technische Aanbevelingen

Secura heeft de volgende operationele aanbevelingen om de belangrijkste gedeelde kwetsbaarheden te verhelpen:

AANBEVELING 1	
Onderwerp	Technisch: Zwakke domeinwachtwoorden zijn toegestaan
Beschrijving	70 gebruikersaccounts zijn gecompromitteerd middels een passwordspray-aanval waarbij een lijst met veelvoorkomende wachtwoorden werd gebruikt. Daarnaast konden, na het overnemen van het Active Directory (AD) een groot percentage onderschepte wachtwoordhashes konden gekraakt worden binnen een korte tijd. Dit was mogelijk vanwege het gebruik van woordenboekwoorden die op voorspelbare wijze zijn getransformeerd om aan complexiteitseisen te voldoen (bijvoorbeeld door van de eerste letter een hoofdletter te maken, en een getal en uitroepteken aan het einde toe te voegen). Aanvallers kunnen hierdoor toegang krijgen tot domeinaccounts door het (automatisch) raden van wachtwoorden.
Aanbeveling	Verplicht bij voorkeur het gebruik van sterke wachtwoordloze authenticatie, zoals Windows Hello for Business. Dit elimineert de meeste wachtwoordgerelateerde risico's zoals password spraying, het kraken van hashes of het phishen van inloggegevens. Wanneer dit niet mogelijk is, dwing dan het gebruik van sterke wachtwoorden af. Secura raadt het volgende aan: • Vereis wachtwoorden van tenminste twaalf tekens, zonder daarbij complexiteitsregels af te dwingen zoals het gebruik van hoofdletters of cijfers. Moedig het gebruik van *wachtzinnen* aan. Dit houdt in dat gebruikers niet een enkel woord transformeren, maar drie of meer (fictieve) woorden en termen samenvoegen. • Controleer op het gebruik van wachtwoorden die in bekende datalekken zijn aangetroffen, bijvoorbeeld middels de Password Protection-dienst van Microsoft. Hiermee kunnen gebruikers worden beschermt die het slachtoffer zijn geworden van een datalek bij een derde partij. Bovendien is het ook een effectief middel om te voorkomen dat mensen veelgebruikte wachtwoorden kiezen, omdat dergelijke wachtwoorden waarschijnlijk ook in bekende datalekken aanwezig zijn. • Definieer een blocklist van specifieke wachtwoorden (of onderdelen van wachtwoorden) waarvan bekend is dat ze vaak gebruikt worden binnen de organisatie. Voorbeelden zijn de organisatienaam, steden van kantoorlocaties of een standaardwachtwoord dat vaak door beheerders wordt ingesteld. • Dwing gebruikers niet om periodiek hun wachtwoord te veranderen, omdat dit vaak resulteert in een keuze voor zwakkere wachtwoorden met opvolgende getallen erin. Forceer enkel wachtwoordwijzigingen wanneer er indicatoren zijn dat het gebruikerswachtwoord mogelijk is gelekt, of wanneer het wachtwoordbeleid is aangepast.

AANBEVELING 2	
Onderwerp	Technisch: Geen rate limiting op het raden van wachtwoorden
Beschrijving	Op het interne netwerk was er geen beperking aan het aantal foutieve wachtwoorden dat voor een account kan worden geraden. Hierdoor was het mogelijk om in korte tijd een grote hoeveelheid veelvoorkomende wachtwoorden te testen voor alle accounts.
Aanbeveling	Stel een maximum aantal wachtwoorden, bijvoorbeeld drie, in voordat er een (tijdelijke) lock-out plaatsvind op het betreffende account.

AANBEVELING 3	
Onderwerp	Technisch: Network Access Control ontbreekt
Beschrijving	Bij het aansluiten van een onbekend systeem op een Ethernet-aansluitpunt, krijgt deze direct toegang tot het netwerk. Wanneer we een eigen laptop aansluiten op een Ethernet-aansluitpunt, krijgt deze direct toegang tot het netwerk, zonder dat een netwerkbeheerder hiervoor maatregelen heeft genomen. Hierdoor kan een ongeautoriseerde persoon kan op eenvoudige wijze met een eigen systeem gebruikmaken van het netwerk.
Aanbeveling	Geef alleen bekende systemen toegang tot het netwerk. Een simpele maatregel is het Ethernet-adres van het systeem te controleren. Dit is echter eenvoudig te omzeilen door het ongeautoriseerde systeem een Ethernet-adres van een geautoriseerd systeem te laten aannemen. We raden daarom aan om 802.1X-authenticatie te gebruiken, waarbij een systeem credentials (in de vorm van een gebruikersnaam en wachtwoord, of een certificaat) moet overleggen alvorens toegang te krijgen. Ook deze beveiliging is te omzeilen, door het systeem van de aanvaller te plaatsen tussen de switch en een zichzelf automatisch authenticerend systeem. De drempel wordt hiermee echter wel significant verhoogd. Zorg ook voor monitoring, waardoor het aansluiten van een onbekend systeem direct wordt opgemerkt.

AANBEVELING 4	
Onderwerp	Technisch: Multifactorauthenticatie ontbreekt
Beschrijving	Er werd door een aantal toepassingen geen multifactorauthenticatie-mechanisme aangeboden. Een aanvaller die inloggegevens in handen krijgt, kan daarmee toegang verkrijgen tot de betreffende toepassingen.
Aanbeveling	Gebruik overal multifactorauthenticatie. Dit kan worden geïmplementeerd door bijvoorbeeld gebruik te maken van FIDO2 of U2F-tokens, authenticatie-apps, of clientcertificaten. Daarnaast kan multifactorauthenticatie worden gedelegeerd naar vertrouwde authenticatie verstrekkers. Zorg er ook voor dat in het beleid is opgenomen dat nieuwe toepassingen enkel met MFA mogen worden ontsloten.

AANBEVELING 5	
Onderwerp	Technisch: Netwerksegmentatie
Beschrijving	Een groot aantal server en clientsystemen bevinden zich op één en hetzelfde netwerk. Hierdoor kunnen systemen en services die normaal gesproken alleen door specifieke andere systemen gebruikt worden, onnodig vanuit het gehele netwerk worden aangevallen.
Aanbeveling	Segmenteer het netwerk zodanig dat systemen die voor een bepaalde toepassing gebruikt worden in een apart subnet worden geplaatst. Door middel van firewallregels kan vervolgens worden bewerkstelligd dat specifieke systemen alleen bereikbaar zijn vanaf systemen die hier een legitieme toepassing voor hebben.

AANBEVELING 6	
Onderwerp	Technisch: Te brede permissies op AD-certificaattemplateconfiguratie (ADCS)
Beschrijving	Active Directory maakt gebruik van certificaatdiensten die gebruikt kunnen worden voor client-authenticatie. Door een misconfiguratie in deze service had een aanvaller schrijfrechten op ten minste één certificaattemplate. Hiermee kon een aanvaller het template kwetsbaar maken voor escalatie van privileges met behulp van de certificaat-service, en daarmee de hoogste privileges binnen het domain verkrijgen. Een gebruiker met beperkte privileges kan het certificaattemplate dusdanig aanpassen om zichzelf aan te melden bij het template, en een verzoek indienen met een arbitraire Storage Area Network (SAN). Met dit certificaat kan een een gebruiker zich authenticeren als een willekeurige gebruiker binnen het domein, inclusief domeinbeheerders. Dit geeft een aanvaller de mogelijkheid om privileges te escaleren binnen het netwerk, en de hoogste rechten binnen het domein te verkrijgen. Een aanvaller met toegang tot deze privileges kan ransomware plaatsen op alle domein-assets, inclusief alle domain-joined interne servers en laptops van medewerkers van de betreffende organisatie.
Aanbeveling	Review alle permissies van alle certificaat-templates, en verwijder onnodige schrijfrechten voor gebruikers die dit niet nodig hebben. Evalueer of de certificaattemplates nog nodig zijn, en verwijder de certificaattemplates die niet worden gebruikt. Ga tevens na welke certificaten reeds uitgegeven zijn en trek de geldigheid in van eventuele onterecht uitgegeven certificaten.

AANBEVELING 7	
Onderwerp	Technisch: Gegevens opgeslagen in GPO
Beschrijving	Er werd vastgesteld dat lokale beheerdersgegevens waren opgeslagen in een Group Policy Object. Het sprayen van deze inloggegevens kan resulteren in lokale beheerderstoegang op interne systemen.
Aanbeveling	Neem geen inloggegevens op in GPOs.

Om de onderliggende oorzaken die tijdens deze assessments zijn geïdentificeerd te verhelpen, heeft Secura naast operationele aanbevelingen ook de volgende strategische aanbevelingen om de beveiligingshouding van de organisaties te verbeteren.

Onveilig beheer methodieken; Een significant deel van het risico waaraan de organisatie is blootgesteld, komt voort uit onveilige beheer methododieken. Een directe winst kan worden behaald door ervoor te zorgen dat alle systemen een uniek sterk wachtwoord hebben voor ingebouwde beheerdersaccounts. De beheerlast van het bijhouden van al deze wachtwoorden kan worden verlicht door het implementeren van een wachtwoordkluis of een geautomatiseerde oplossing zoals Microsoft LAPS.[1]

Om het moeilijker te maken voor aanvallers om hun privileges te escaleren, kan een administratief niveau-model worden geïmplementeerd. In zo'n model worden verschillende vertrouwelijkheidsniveaus gedefinieerd. Elk niveau heeft bijbehorende beheerdersaccounts en er zijn technische controles die voorkomen dat accounts van gevoeligere niveaus toegang krijgen tot systemen in minder gevoelige niveaus. Dit moet ervoor zorgen dat als een aanvaller erin slaagt een beheerdersaccount in één niveau te compromitteren, zij dat account niet kunnen misbruiken om toegang te krijgen tot een gevoeliger niveau, waardoor hun privileges toenemen. Bijvoorbeeld, accounts met domeinbeheerdersprivileges (niveau 0) zouden nooit in staat moeten zijn om in te loggen op serversystemen (niveau 1) of werkstations van medewerkers (niveau 2).

[1] https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-guide-how-to-configure-microsoft-local/ba-p/2806185

Een andere manier om het aantal bevoorrechte accounts dat gemakkelijk kan worden misbruikt door aanvallers te verminderen, is het implementeren van een Privileged Identity Management-oplossing. Deze softwarepakketten integreren met andere producten en kunnen worden gebruikt om tijdelijk toestemmingen of beheerdersaccounts voor applicaties en servers op verzoek te verlenen. Een goed geïmplementeerde PIM-oplossing kan ook helpen problemen te mitigeren die ontstaan door een gebrek aan beveiligingsbewustzijn. Let op dat het implementeren van een PIM vaak een lang en moeilijk project is.

Onvoldoende netwerksegmentatie en -filtering; Segmenteer het netwerk in kleinere, beter beheersbare groepen systemen door soortgelijke netwerkbronnen te combineren in enkele segmenten. Dit kan worden uitgevoerd door een combinatie van firewalls, Virtual LANs (VLANs) en Software Defined Networking. Het wordt aanbevolen om het principe van het minste privilege te volgen en complexiteit door oversegmentatie te beperken. Zorg ervoor dat na segmentatie strikte filtering aanwezig is om onnodig verkeer tussen de segmenten te voorkomen. Zodra de filtering is ingezet, moet deze worden getest door meerdere connectiviteitstests uit te voeren vanuit de verschillende segmenten.

Daarnaast moeten netwerktoegangscontroleoplossingen worden geïmplementeerd om ervoor te zorgen dat alleen geautoriseerde apparaten op het netwerk zijn toegestaan.

3.2. Beveiligingsbewustzijn

Als gevolg van beperkt beveiligingsbewustzijn van medewerkers was Secura in staat om bij de meeste organisaties:

- Toegang te verkrijgen tot verschillende locaties in de fysieke gebouwen van de MBO-instellingen. Dit maakte op zijn beurt persistente toegang tot het interne netwerk mogelijk door middel van het plaatsen van apparaten voor toegang op afstand. Dit werd versterkt door de afwezigheid van sterke Network Access Control-oplossingen.
- Inloggegevens te verkrijgen van zowel medewerkers als studenten vanuit een extern aanvallersperspectief met behulp van een phishingaanval.

De onderliggende reden voor deze kwetsbaarheden is:

Onvoldoende beveiligingsbewustzijn; Bij verschillende gelegenheden tijdens de assessments werd een gebrek aan beveiligingsbewustzijn misbruikt. Voorbeelden hiervan zijn medewerkers die hun inloggegevens invoerden bij een phishingaanval, het opslaan van niet-versleutelde inloggegevens in verschillende bestanden en een onveilige methodologie voor systeembeheer. Een voorbeeld van zo'n onveilig systeembeheer is het gebruik van domeinbeheerdersaccounts om in te loggen op systemen waar deze privileges niet nodig zijn. Het gebrek aan beveiligingsbewustzijn heeft aanzienlijk bijgedragen aan een aantal kwetsbaarheden tijdens deze assessments.

3.2.1. Aanbevelingen met betrekking tot beveiligingsbewustzijn

Secura heeft de volgende operationele aanbevelingen om de belangrijkste gedeelde kwetsbaarheden te verhelpen:

AANBEVELING 8	
Onderwerp	Fysieke toegang: Beveiligingsbewustzijn
Beschrijving	De social engineers worden tijdens de aanval niet aangesproken door medewerkers op hun aanwezigheid of gedrag. Hierdoor kan een social engineer: • Toegang krijgen tot gevoelige locaties op het terrein. • Toegang krijgen tot vertrouwelijke bedrijfsinformatie. • Toegang krijgen tot het interne netwerk. • Apparatuur voor toegang op afstand achterlaten in het netwerk. • Goederen stelen die vervolg aanvallen mogelijk maken zoals toegangspassen of laptops. Er werd geen alarm geslagen binnen de MBO-instellingen.
Aanbeveling	Waarschuw de organisatie regelmatig om alert te zijn op indringers. Train medewerkers regelmatig in het herkennen van social engineering-aanvallen om het veiligheidsbewustzijn te vergroten en train ze om een persoon in het gebouw te benaderen die ze niet kennen. Herhaal deze training regelmatig.

AANBEVELING 9	
Onderwerp	Fysieke toegang: Onbevoegde toegang
Beschrijving	De Social Engineers hadden ongeautoriseerde toegang tot fysieke locaties van de organisaties. Deze toegang werd op de volgende manieren verkregen: • De Social Engineer gebruikte een voorwendsel om medewerkers te overtuigen toegang te verlenen tot bepaalde locaties. • In het kader van het karakter van MBO-instellingen is er geen strikte toegangscontrole tot de gebouwen. Er werden geen waarschuwingen gegeven en de Social Engineer werd niet gestopt. Deze toegang is het startpunt voor Social Engineering vervolgaanvallen die kunnen leiden tot toegang tot gevoelige locaties of toegang tot de interne netwerken.
Aanbeveling	Omdat scholen open instellingen zijn en het is niet haalbaar om mensen te verhinderen binnen te komen. Hoewel het waar is dat het moeilijk is om iedereen te stoppen van het betreden van het gebouw, kan het beveiligingsbewustzijn van medewerkers voorkomen dat mensen toegang krijgen tot gevoelige locaties waar interactie met een medewerker vereist is. Bijvoorbeeld toegang krijgen tot een patchkamer was alleen mogelijk na het vragen aan een medewerker die de identiteit van de social engineers niet verifieerde. Bovendien, wanneer mensen toegang hebben tot het interne netwerk, zouden ze alleen toegang moeten hebben tot een openbaar segment waar alleen toegang tot een beperkte set systemen mogelijk zou moeten zijn.

AANBEVELING 10	
Onderwerp	Fysieke toegang: Netwerk toegang
Beschrijving	Onbevoegde personen hebben toegang tot de netwerken van de MBO-instellingen zonder te worden uitgedaagd. Hierdoor konden ze de netwerken van de organisaties verkennen.
Aanbeveling	Waarschuw medewerkers regelmatig om alert te zijn op indringers. Train werknemers regelmatig in het herkennen van social engineering-aanvallen om het beveiligingsbewustzijn te vergroten. Herhaal deze training regelmatig. Zorg ervoor dat openbare ruimtes geen verbindingen bieden met het interne netwerk. Creëer een netwerk speciaal voor gasten. Controleer het netwerkverkeer op scans en onbekende MAC-adressen.

AANBEVELING 11	
Onderwerp	Phishing: Medewerkers openen phishing-e-mails en klikken op kwaadaardige links.
Beschrijving	Social engineers gebruiken een phishing-e-mail om mensen te beïnvloeden om acties te ondernemen die niet in hun belang zijn. Hieronder valt: • Mensen naar een nep website lokken die ze verleid om hun inloggegevens in te voeren. • Mensen een document laten openen dat kwaadaardige code bevat. • Mensen naar een website lokken die een drive-by-download verstuurt. • Mensen overtuigen om in opdracht van de Social Engineer processen uit te voeren, bijvoorbeeld geld overmaken. • Informatie verzamelen over het doelbedrijf of het type computersystemen dat binnen het doelbedrijf wordt gebruikt. De mogelijkheid om medewerkers op links te laten klikken, is meestal de eerste stap om geldige accounts te compromitteren. Afhankelijk van de staat van beveiliging van het apparaat en het netwerk kan een social engineer toegang krijgen tot vertrouwelijke bedrijfsgegevens. Daarnaast laten timestamps in de verzamelde gegevens laten zien dat werknemers probeerden phishing-e-mails te openen of inloggegevens op een phishing-website in te dienen, nadat een bedrijfsbrede waarschuwing was verzonden. Wanneer maatregelen om werknemers te informeren niet effectief zijn, kan dit mogelijk de duur van de social engineering-aanval verlengen.
Aanbeveling	Train medewerkers regelmatig in het herkennen van social engineering-aanvallen om het bewustzijn op het gebied van IT-beveiliging te vergroten. Herhaal deze training regelmatig. Maak het ook makkelijk voor medewerkers om phishing-pogingen te melden door functionaliteit in de gebruikte e-mailclients in te schakelen. Beloon ten slotte medewerkers die regelmatig phishing-e-mails melden om hen te stimuleren hun mindset binnen uw bedrijf te delen. Help medewerkers bovendien bij het detecteren van phishing-e-mails door bijvoorbeeld e-mails van externe adressen of links die naar buiten de organisatie leiden te markeren. Overweeg het gebruik van oplossingen zoals internetfilters die de toegang tot niet-vertrouwde externe domeinen verbieden om de impact te beperken van werknemers die op kwaadaardige links klikken. Zet ook een centraal meldpunt op voor het melden van social engineering-aanvallen. Informeer de medewerkers regelmatig over het centrale meldpunt en hoe deze te gebruiken in het kader van een security awareness training. Zorg ervoor dat dit centrale meldpunt een beleid hanteert om ervoor te zorgen dat de effecten van de social engineering-aanval beperkt blijven. Configureer bijvoorbeeld een tijdelijke zwarte lijst op netwerk- en/of DNS-niveau om te voorkomen dat meer werknemers de phishingwebsite bezoeken.

Om de onderliggende oorzaak die tijdens deze assessments is geïdentificeerd te verhelpen, heeft Secura naast operationele aanbevelingen ook de volgende strategische aanbevelingen om de beveiligingshouding van de organisaties te verbeteren.

Onvoldoende beveiligingsbewustzijn; Een aantal technische beveiligingsmaatregelen kan omzeild worden door (mogelijk onwetende) medewerkers die onveilige keuzes maken. Deze assessments hebben aangetoond dat de beheerders en medewerkers mogelijk onvoldoende bewust zijn van de gevolgen van hun keuzes met betrekking tot de beveiliging van de organisaties. Als er trainingsplannen voor beveiligingsbewustzijn bestaan, moeten deze worden herzien en aangevuld met specifieke informatie over fysieke toegang en spearphishing. Als er geen plan bestaat, moet een programma voor beveiligingsbewustzijn worden gecreëerd om het beveiligingsbewustzijn van medewerkers te verhogen. Het is raadzaam om een beveiligingspartner te contacteren om te helpen bij het ontwikkelen, uitvoeren en valideren van de effectiviteit van dit nieuwe en/of verbeterde programma.

3.3. Detecties en mitigaties

Als gevolg van beperkingen in detecties en mitigaties was Secura in staat om bij de meeste organisaties:

- Wachtwoordraad-aanvallen uit te voeren zonder beperkingen. Specifiek, uitgebreide en herhaalde wachtwoord-spray-aanvallen die meerdere uren of dagen aanhouden.
- Enkele belangrijke aanvallen uit te voeren die niet zijn opgevallen in verband met beperkingen in de dekking van het SOC.

3.3.1. Aanbevelingen met betrekking tot detecties en mitigaties

Hoewel bepaalde problemen met betrekking tot detecties en mitigatiemaatregelen zijn besproken met de deelnemende MBO-instellingen, zijn er geen sterke algemene tekortkomingen in beveiliging ontdekt. Ook, omdat de focus van deze Red Cell-assessments minder op stealth lag, kunnen momenteel geen algemene aanbevelingen worden uitgegeven.

Het is echter aanbevolen om een validatie uit te voeren om te controleren dat de technieken die uitvoerig zijn gebruikt in de Red Cell-assessment, daadwerkelijk op een correcte wijze worden gedetecteerd en gemitigeerd. Hiervoor kan gebruik worden gemaakt van het MITRE ATT&CK Framwework. MITRE ATT&CK staat voor ”MITRE Adversarial Tactics, Techniques, and Common Knowledge”. Het is een wereldwijd erkend kennisraamwerk dat gebruikt wordt in de cybersecurity-industrie om cyberdreigingen te classificeren en te begrijpen. Dit raamwerk is ontwikkeld door MITRE, een Amerikaanse non-profitorganisatie, en biedt een uitgebreide lijst van tactieken, technieken en procedures (TTP’s) die cyberaanvallers gebruiken. De TTP’s zijn georganiseerd volgens verschillende fasen van een cyberaanval, zoals initial access, execution, persistence, enzovoort. Elk onderdeel binnen het raamwerk bevat gedetailleerde informatie over hoe aanvallers bepaalde technieken kunnen gebruiken en wat de mogelijke indicatoren van een aanval zijn. Dit stelt verdedigers in staat om beter te begrijpen hoe aanvallen werken en hoe ze zich kunnen voorbereiden op en reageren op dreigingen.

Bij het inregelen van detecties en mitigaties is het essentieel om prioriteit te geven aan de TTP’s die het meest relevant zijn voor de specifieke omgeving en dreigingslandschap van de organisatie. De tabel met MITRE ATT&CK TTP’s kan als leidraad dienen om te bepalen welke technieken het meest waarschijnlijk gebruikt zullen worden door aanvallers die zich richten op de sector of technologieën van de organisatie. Door zich te richten op de TTP’s met de hoogste prioriteit, kunnen organisaties hun middelen effectiever inzetten en een sterker verdedigingsmechanisme ontwikkelen. Dit houdt in dat zij detectiecapaciteiten moeten ontwikkelen voor de meest waarschijnlijke aanvalstechnieken en passende mitigatiestrategieën moeten implementeren om potentiële schade te minimaliseren. Het prioriteren van TTP’s helpt ook bij het focussen op de meest kritieke gebieden en vermindert de kans dat belangrijke dreigingen over het hoofd worden gezien.

Gedurende deze onderzoeken zijn door het Red Team voornamelijk de volgende TTP’s gebruikt:

- T1110: Brute Force
- T1078: Valid Accounts
- T1566: Phishing
- T1200: Hardware Additions
- T1649: Steal or Forge Authentication Certificates
- T1552: Unsecured Credentials
- T1087: Account Discovery
- T1083: File and Directory Discovery
- T1069: Permission Groups Discovery
- T1135: Network Share Discovery
- T1615: Group Policy Discovery
- T1046: Network Service Discovery
- T1210: Exploitation of Remote Services
- T1039: Data from Network Shared Drive
- T1005: Data from Local System
- T1003: OS Credential Dumping

3.4. Procesverbeteringen

Uit de uitgevoerde Red Cell-assessments zijn waardevolle inzichten voortgekomen die kunnen bijdragen aan een efficiëntere aanpak van toekomstige onderzoeken. Deze bevindingen zijn belangrijk voor het maximaliseren van de effectiviteit van dergelijke onderzoeken. De verbeteringen richten zich op diverse aspecten van het Red Cell proces.

Ten eerste, is gebleken dat een langere voorbereidingstijd cruciaal is voor het succes van het onderzoek. Vooral wanneer de organisatie niet eerder een Red Teaming-assessment heeft laten uitvoeren. Een minimale voorbereidingstijd van zes weken wordt aanbevolen. Deze extra tijd stelt teams in staat om grondiger te plannen, specifieke doelen te stellen en de benodigde middelen te organiseren. Dit zorgt voor een meer gestructureerde aanpak.

Daarnaast is een strakkere afstemming nodig over hoe om te gaan met detecties door verdedigende teams. Dit omvat duidelijke afspraken over de reacties op en de afhandeling van gedetecteerde activiteiten. Ook de verwachtingen rondom de inzet van 'leg-ups', ofwel assistentie voor het Red Team, moeten duidelijker worden vastgesteld. Deze verbeteringen zullen helpen om de interactie tussen het Red Team en de verdedigers te optimaliseren, waardoor de leerervaring voor beide partijen wordt verrijkt.

Tot slot blijkt dat voor sommige meer volwassen organisaties een volledig Red Teaming onderzoek waardevoller kan zijn dan een beperkter Red Cell onderzoek. Dit is vooral het geval op het gebied van detecties en mitigaties, waar een volledige aanval meer inzicht kan bieden in de daadwerkelijke beveiligingsstatus van de organisatie. Deze aanpak kan leiden tot relevantere resultaten en een dieper inzicht in potentiële kwetsbaarheden en de effectiviteit van bestaande verdedigingsmechanismen.

A. GEBRUIKTE AFKORTINGEN

In ons vakgebied wordt vaak gebruikgemaakt van afkortingen. Niet altijd is meteen duidelijk waar een bepaalde afkorting voor staat. Vandaar dat we in deze appendix proberen om een overzicht te geven van de in dit rapport gebruikte afkortingen[1].

AD	Active Directory
ADCS	AD Certificate Services
BSPA	Baseline Security Product Assessment
C2	Command & Control
CCV	Centrum voor Criminaliteitspreventie en Veiligheid
DNS	Domain Name System
FIDO2	Fast IDentity Online 2
GPO	Group Policy Object
IT	Information Technology
LAN	Local Area Network
LAPS	Local Administrator Password Solution
MAC	Message Authentication Code
MFA	Multi-Factor Authentication
NAC	Network Access Control
PIM	Privileged Identity Management
SAN	Storage Area Network
SFE	Secure File Exchange
SOC	Security Operations Center
TTP	Tactics, Techniques & Procedures
U2F	Universal 2nd Factor
VLAN	Virtual LAN

[1] In veel gevallen zal hier een Engelse “verklarende beschrijving” zijn opgenomen.