Adviesrapport SAM-Oplossing

Onderzoek continue netwerk monitoring MKB bedrijven

Auteur: Ruben Weijer
Bedrijf: Cyber Security Centrum Noord-Nederland
Datum: 4-7-2022
Versie: V1.3

Inhoud

1 Inleiding

Vergroot een netwerk detectiesysteem (IDS) de digitale weerbaarheid van MKB-bedrijven? Is het ook haalbaar om Security Operations Center (SOC) dienstverlening aan te bieden aan kleine MKB-bedrijven in combinatie met deze IDS? Dit adviesrapport is opgesteld om een duidelijk beeld te geven van de mogelijkheden van een netwerk detectiesysteem. Ook zal er ingegaan worden op welke manier, en waar deze het best kan worden ingezet. Binnen dit adviesrapport zal specifiek gekeken worden naar de mogelijkheden van de SAM-oplossing die SecureMe2 heeft ontwikkeld. In het volgende hoofdstuk (1.1) zal verdere uitleg gegeven worden over deze oplossing. Binnen dit rapport zal ook het onderzoek worden meegenomen dat is gedaan om dit advies vorm te geven. Om de hier boven genoemde vragen te beantwoorden is onderzoek noodzakelijk. Dit is gedaan door een case study uit te voeren. Tijdens deze case study zijn IT-professionals geïnterviewd om een beeld te krijgen hoe zij naar deze oplossing kijken. Ook zijn er online onderzoeken doorgenomen om een baseline te creëren over hoe weerbaar het MKB momenteel is en wat er gedaan kan worden om dit zo te houden en te verbeteren. Ook zijn er experimenten uitgevoerd om zo inzicht te krijgen in wat de SAM-oplossing kan detecteren en in welke mate dit als behulpzaam wordt gezien door de MKB-er en IT-dienstverlener.

Dit onderzoek is uitgevoerd in opdracht van de Stichting Cyber Security Centrum Noord Nederland. Hierna te noemen de Stichting. De stichting wil graag het MKB digitaal weerbaarder maken tegen digitale dreigingen zoals cybercrime. Dit doen zij door met verschillende organisaties samen te werken. Voorbeelden zijn: Hanzehogeschool Groningen, bedrijvenverenigingen, gemeente- en provincie Groningen. Deze samenwerkingen houden in dat kennis en middelen bij elkaar komen om de weerbaarheid van het MKB in Noord Nederland te vergroten.

Cybercrime wordt een steeds groter probleem bij MKB-bedrijven omdat zij vaak achterlopen op het gebied van digitale veiligheid. (KPN, 2020) Dit is zeer zorgelijk omdat bijna 99.9% van de Nederlandse bedrijven, MKB-bedrijven zijn. (CBS, 2021) Mocht een grote groep van deze bedrijven ernstig geraakt worden door cybercrime dan zou dit een gedeelte van de samenleving kunnen ontwrichten. Het is van groot belang dat het MKB zijn verantwoordelijkheid neemt, maar de overheid moet hier ook een faciliterende rol in spelen. Dit omdat het hier gaat om een gezamenlijke verantwoordelijkheid. (Doorne, 2021) Het is van belang dat we een goede mix van organisatorische en technische middelen inzetten om de weerbaarheid van het MKB te vergroten. (Raoul Notté, 2016/2017)

1.1 SAM-oplossing

De SAM-oplossing is een IDS systeem dat is ontwikkeld door SecureMe2. Dit is een kastje dat je aan het begin van je netwerk hangt. Het kastje verzamelt al het netwerkverkeer. De metadata van het verzamelde verkeer wordt verstuurd naar de Cloud omgeving van SecureMe2. Hier wordt het verkeer geanalyseerd door verschillende, door SecureMe2 ontwikkelde, algoritmes. Mochten deze algoritmes aan de hand van de metadata verdachte activiteit detecteren wordt er een melding verstuurd naar het dashboard. Bij een melding met een hoge prioriteit wordt er een mailtje verstuurd naar de ondernemer en/of de IT-dienstverlener. Tevens heeft de SAM ook een Application Programming Interface (API). Via deze API kunnen de meldingen die naar voren komen makkelijk worden geïntegreerd in een bestaande Security information and event management (SIEM) oplossing. Hierdoor kunnen onderlinge relaties makkelijk worden onderzocht. Deze methode is niet onderzocht omdat dit niet binnen de scope van de opdracht viel.

2 Onderzoek

In dit hoofdstuk zal worden ingegaan op de methode waarmee het onderzoek is uitgevoerd en welke resultaten hieruit naar voren zijn gekomen.

2.1 Onderzoeksmethode

De onderzoeksmethode die is gebruikt tijdens dit onderzoek is een case study. Om de onderzoeksresultaten te verkrijgen zijn meerdere vormen van dataverzamelingsmethoden gebruikt. Er zijn interviews gehouden met IT-security professionals en MKB-ondernemers. Tevens is er onderzoek gedaan naar bronnen die online beschikbaar waren. Zoals onderzoeken naar de weerbaarheid van MKB-bedrijven en welke oplossingen hier worden gegeven om deze weerbaarheid te vergroten. Ook is er tijdens dit onderzoek gebruik gemaakt van experimenten. Dit door de SAM-oplossing bij meerdere MKB-bedrijven ongeveer 4 weken in het netwerk te hangen en te onderzoeken welke meldingen er naar voren kwamen.

2.2 Interviews IT-security professionals

Als vooronderzoek zijn er interviews gehouden met verschillende personen. Hieronder volgt een korte samenvatting van elk gesprek en de lessen die daaruit kunnen worden meegenomen om het vervolgonderzoek aan te vullen. De vragenlijst die als leidraad heeft gediend tijdens deze interviews is te vinden in bijlage B1.

2.2.1 Interview Aad van Boven (SecureMe2)

Aad van Boven is CEO bij SecureMe2. Hij heeft veel ervaring op securitygebied. In het gesprek kwam vooral de technische werking van de SAM naar voren. Door de technische werking van de SAM te begrijpen is het makkelijker om advies te geven over de SAM-oplossing. Ook geeft Aad aan dat het niet haalbaar is om de SAM zonder dienstverlening aan te bieden aan MKB-ondernemers. SecureMe2 heeft meerdere IT-dienstverleners als partners die wel SOC-dienstverlening aanbieden aan hun klanten. Dit is haalbaar omdat de IT-dienstverlener precies weet wat er voor de klant belangrijk is en welke systemen er in het netwerk hangen. Door deze kennis kunnen zij adequaat handelen op meldingen die op het SOC binnenkomen.

Aad geeft aan dat de SAM-oplossing een andere aanpak heeft dan bijvoorbeeld een next-gen firewall waar ook IDS in gebouwd zit. Bij de SAM-oplossing wordt de meta data naar de Cloud van SecureMe2 gestuurd en geanalyseerd. In tegenstelling tot de lokale IDS die in de firewall zit. Hier wordt de dreigingsinformatie naar de firewall zelf toegestuurd. Binnen de Cloud van SecureMe2 is vele malen meer rekenkracht en opslag beschikbaar dan een lokale firewall. Hierdoor kunnen complexe analyses worden uitgevoerd. Ook kan er aan de hand van gebeurtenissen bij andere klanten nog betere meldingen worden verstuurd. Door al deze data te analyseren kunnen ook historische gebeurtenissen zoals het uit buiten van zero days, met terug werkende kracht worden gedetecteerd. Hier kan dan ook weer een melding over worden verstuurd richting de klant. Dit is niet mogelijk bij een lokaal IDS systeem omdat deze niet met terugwerkende kracht de data kan analyseren en ook niet de data van alle andere firewalls beschikbaar heeft. Hierdoor heeft SecureMe2 een uniek product ontwikkeld die erg goed dreigingen accuraat kan detecteren.

2.2.2 Interview Stefan Zevenberg (Surity)

Stefan Zevenberg heeft al meer dan 20 jaar ervaring op het gebied van Cyber Security. Hij was onder meer eigenaar en directeur van een IT-dienstverlener genaamd NewComm IT. Deze was voornamelijk gericht op de Cyber Security kant van IT-dienstverlening. Momenteel werkt hij als business consultant bij Surity. In het gesprek met Stefan kwamen de volgende onderwerpen aan bod:

- Zijn MKB-bedrijven digitaal weerbaar?
- Bij welke MKB-bedrijven is de SAM-oplossing van toegevoegde waarde?
- Wat moet er met een melding worden gedaan?
- Hoe ziet de ideale situatie eruit?
- Hoe staat een pentest in deze discussie?

Over het algemeen zijn MKB-bedrijven zich nog niet genoeg bewust van de risico's die digitalisering van bedrijfsprocessen met zich meebrengen. Dit komt mede omdat zij de noodzaak, om de risico's in kaart te brengen, nog niet in zien. Bedrijven die medewerkers in dienst hebben met verstand van risicobeheersing, zijn eigenlijk de enige soort bedrijven waar de SAM-oplossing optimaal kan functioneren. Stefan geeft aan dat zonder beleid en bijbehorende processen, de technische SAM-oplossing geen kans van slagen heeft. Dit mede doordat de ondernemer geen goede inschatting kan maken van de door de SAM verstuurde meldingen. Een melding moet ook niet gelijk naar de IT-dienstverlener worden gestuurd omdat diegene er meestal ook geen verstand van heeft. Op de helpdesk werken meestal alleen maar techneuten en geen personen die een goede risico inschattingen kunnen maken. De ideale situatie zal ongeveer gelijk staan aan het volgende: een IT-dienstverlener die deze SAM dienst aanbiedt, samen met een consultant die gespecialiseerd is in het inschatten van risico's. De ondernemer en deze consultant moeten eerst samen een beleid opstellen. Hieruit zullen processen en procedures komen. Hierna kan de SAM-oplossing worden ingericht om het beleid, de processen en de procedures te controleren. Mocht er dan een melding naar voren komen, dan zal de consultant aan de hand van deze melding het beleid aanpassen. Hoeft het beleid niet aangepast te worden? Dan zal er een proces of procedure in werking treden. Is er nog geen proces of procedure? Dan wordt er een gemaakt aan de hand van het beleid wat is opgesteld. Zonder beleid en proces is de technische oplossing nutteloos en biedt deze slechts voor een geringe periode enigszins bescherming. Op het onderdeel pentesten is ook ingegaan. Pentesten zijn op zichzelf staand een te grote hype. Het MKB krijgt hierdoor het idee dat na een pentest alles veilig is en enige tijd veilig blijft. Dit is helaas niet het geval, mede omdat er zo snel en zo veel kwetsbaarheden in software worden gevonden. Hierom is een pentest ook alleen maar een controlemiddel dat na het opstellen van beleid en processen moet worden gebruikt om deze periodiek te controleren.

2.2.3 Interview Martijn Mandos (Wortell)

Martijn Mandos is adviseur cyber security bij Wortell. Martijn geeft in het gesprek aan dat de melding die uit de SAM naar voren komt bij iemand terecht moet komen die verstand van de IT-omgeving heeft. Het huidige dashboard is te technisch en geeft weinig tot geen aanbevelingen. Als dit ook voor kleine ondernemers ingezet wordt, zonder IT-medewerker, is het van belang dat er een duidelijk advies bij elke melding komt te staan. Een ondernemer zonder IT-kennis weet niet wat de concrete impact is van een melding. Mocht er voor gekozen worden de meldingen direct door te zetten naar de IT-dienstverlener, dan is het van belang dat zij werknemers in dienst hebben die meldingen correct kunnen interpreteren. Wel zou de SAM er voor kunnen zorgen dat de ondernemer meer inzicht krijgt in zijn of haar IT-omgeving. Hierdoor zal het bewustzijn vergroot worden, dat ook zijn/haar onderneming aangevallen wordt en dat er misschien extra middelen ingezet moeten worden om dit risico te beperken.

2.2.4 Interview Jan Martijn Broekhof (Gardian360)

Jan Martijn is managing director bij Gardian360. Hij heeft al veel ervaring op het gebied van IT-dienstverlening doordat hij bijna 20 jaar een eigen IT-bedrijf heeft gehad. Nu is Jan Martijn gefocust op het aanbieden van securitydienstverlening. In het gesprek met Jan Martijn kwam naar voren dat het momenteel nog niet uit kan om een SOC dienst aan te bieden aan kleine MKB-organisaties. Hier heb je sowieso 4 tot 5 personeelsleden voor nodig die ook nog eens 24/7 de systemen in de gaten moeten houden. Ook geeft hij aan dat je om een SOC dienst aan te bieden niet alleen maar een IDS oplossing nodig hebt, maar nog veel meer middelen zoals: firewall logging, vulnerability scanners en MS365 monitoring. Elke klant heeft ook weer specifieke use cases. Dit kunnen bijvoorbeeld use cases zijn als: bedrijf x vindt het prima als iemand eerst vanuit Amsterdam inlogt op een systeem en 3 uur later vanuit Moskou. Bedrijf y kan dit juist niet acceptabel vinden en wil hier graag een melding over ontvangen. Hierdoor is het lastig om een standaard oplossing aan te bieden. Door het gebrek aan standaardisatie zal de SOC dienstverlening nog duurder worden. Het is volgens Jan Martijn verstandig om eerst de focus te houden op de basisbeveiligingsmaatregelen. Dit houdt bijvoorbeeld in dat je eerst antivirus, antispam en een updatebeleid op orde hebt. Hierna kan er voor inzicht gezorgd worden door netwerkmonitoring en vulnerability scanning. Voor veel klanten zal dit al het volwassenheidsniveau zijn wat zij nodig hebben. Om deze basis in te richten adviseert Jan Martijn ESET antivirus of Sentenel One omdat deze twee tools redelijk betaalbaar zijn voor het MKB en ook centraal te beheren zijn. Dit maakt het beheren en reageren op meldingen makkelijker. Hierdoor verschuif je de risicobeheersing voor een gedeelte naar de end point en accepteer je tot zekere hoogte dat er verdachte activiteit in het netwerk plaats kan vinden. Maar dit zal er dan niet toe leiden dat er malware wordt geïnstalleerd op end points.

Mocht de Stichting wel een faciliterende rol gaan spelen om samen met IT-dienstverleners SOC dienstverlening collectief aan te bieden aan kleinere MKB-bedrijven, dan zou het zeker een goed idee zijn om inloop avonden te organiseren voor de ondernemers. Tijdens een inloop avond kunnen dan anoniem de resultaten worden gedeeld over actieve dreigingen die worden waargenomen in de netwerken van de ondernemers. Hierop kan ook weer een advies worden gegeven door aan te geven hoe ondernemers zich tegen de gevonden dreiging kunnen wapenen. Hierdoor creëer je bewust wording bij de ondernemers. Ook zal het goed zijn om ondernemers maandelijks te informeren over hoe hun netwerk er voor staat, ook als er geen dreiging is en het goed gaat. Dit zorgt er voor dat de ondernemer gerust kan zijn over zijn of haar netwerkbeveiliging.

Een aantal vragen voor vervolgonderzoek die Jan Martijn aanbeveelt, zijn:

- Hoe kijken IT-dienstverleners aan tegen de rol van de stichting?
- Hoe kan de stichting IT-dienstverleners helpen met het opzetten van SOC dienstverlening?
- Kan SecureMe2 een geanonimiseerde lijst beschikbaar maken die aantoont welke dreigingen zij hebben herkend?

2.3 Interviews ondernemers

Tijdens het onderzoek is er al snel gebleken dat de meldingen in huidige staat niet naar de ondernemer moeten. Hierom is er ook maar met één ondernemer een gesprek gehouden.

2.3.1 Interview Klaas Holtman

Klaas Holtman is ondernemer en adviseur. Hij geeft ook aan dat het niet verstandig is om de melding direct naar de ondernemer te sturen. Ook geeft Klaas aan dat 100 euro per maand een stevige prijs is voor dit product. Hij ziet wel potentie als de SAM afgenomen kan worden met korting via de verzekering. Klaas ziet vooral potentie in het beveiligen van het IoT-gedeelte van het netwerk. Hij geeft aan dat dit gedeelte meestal nog minder goed beveiligd is dan de rest van het netwerk. Hierin vindt hij het ook belangrijk dat er een overzicht of een melding wordt verstuurd als er dingen goed gaan op IT-gebied. Dit zorgt ervoor dat de ondernemer er zeker van is dat hij/zij de zaken goed geregeld heeft.

2.4 Online bronnenonderzoek

Online is er onderzoek gedaan naar verschillende bronnen die dit onderzoek kunnen aanvullen.

Eerst is onderzoek gedaan naar hoe weerbaar het MKB momenteel is tegen cybercrime en wat de adviezen zijn die uit deze onderzoeken naar voren zijn gekomen. Uit verschillende van deze onderzoeken blijkt dat de bewustwording bij ondernemers nog niet op een acceptabel niveau is. Hierdoor werden er binnen deze onderzoeken vooral aanbevelingen gedaan op het gebied van bewustwording en niet zo zeer op technische middelen. Het updaten van systemen en het in de basis veilig configureren van het netwerk waren wel punten waar kort een aanbeveling over gegeven werd. Er werd niet in gegaan op netwerk detectiesystemen voor het MKB. (NIPO, 2015)

Om toch een duidelijk beeld te krijgen van een netwerkdetectie systeem die al breed wordt ingezet is gekeken naar het elektriciteitsnet. Hier is een uitgebreid onderzoek naar gedaan die via de HBO-kennisbank beschikbaar was. Dit onderzoek ging in op welke wijze een netwerkdetectiesysteem geïmplementeerd moest worden om het elektriciteitsnet veilig te houden. Naar aanleiding van het lezen van dit onderzoek is er verder onderzoek gedaan naar de algoritmes die gebruikt worden in het analyseren van het netwerkverkeer. Het is van belang om op deze algoritmes te kunnen vertrouwen en de werking op hoofdlijnen te begrijpen. (Sluis, 2019)

Verder waren er online bijna geen verdere onderzoeken beschikbaar die ingingen op het inrichten van een netwerkdetectie systeem.

2.5 Experimenten

In dit hoofdstuk zullen de opzet en de resultaten van de experimenten naar voren komen.

2.5.1 Bedrijfsverzamelgebouw

Voorafgaand aan de experimenten bij MKB-bedrijven is de SAM drie maanden getest in een bedrijfsverzamelgebouw. Dit netwerk is op de locatie van de Stichting en was al aanwezig voor dat dit project gestart was. In dit gebouw zijn ongeveer 5 ondernemingen gevestigd die werkzaam zijn in verschillende sectoren. In deze periode zijn relatief weinig meldingen met een hoge prioriteit naar voren gekomen. Twee keer kwam er een melding naar voren over een portscan en één keer kwam er een melding naar voren dat een systeem een malafide website had bezocht.

Binnen deze periode zijn ook verschillende handmatige portscans uitgevoerd. Om zo een melding met een hoge prioriteit te forceren. Na deze portscans is geen enkele keer een melding hiervan naar voren gekomen. Dit roept wel vragen op over de betrouwbaarheid van de SAM-oplossing en de algoritmes die gebruikt worden.

2.5.1.1 Algoritme SAM

Nadat deze bevinding gedeeld was met SecureMe2 hebben ze contact opgenomen (met mij) om in meer detail de technische werking van de SAM uit te leggen. Uit dit gesprek is naar voren gekomen dat de algoritmes die gebruikt worden tijdens de netwerkanalyse zeer snel lerend zijn en elke 15 minuten nieuwe dreigingsinformatie gevoed krijgen. Ook wordt naar de historie van het netwerkverkeer gekeken om zo meldingen van zogenaamde false positives te beperken. Mede hierdoor is het lastig om de detectie van verdacht netwerkverkeer en het forceren van een melding goed te testen. Doordat de portscan werd uitgevoerd door een laptop die al veel vaker verbonden is geweest met het netwerk, en door een scan uit te voeren die in de praktijk te veel zou opvallen. Is er geen melding verstuurd naar het dashboard. SecureMe2 gaf aan dat er een melding verstuurd zou worden als deze scan over meerdere dagen werd uitgevoerd en een minder opvallende methode gebruikt was.

2.5.2 MKB-netwerk

De SAM heeft vier weken bij een IT dienstverlener in het netwerk gehangen en al het verkeer gemonitord wat er in deze vier weken voorbij kwam. Hieruit zijn de volgende bevindingen vast gesteld.

2.5.2.1 Implementatie fase

Tijdens de implementatie fase is de SAM door mij in het netwerk gehangen van de IT-dienstverlener. Hier zaten helaas wat haken en ogen aan, omdat de SAM al eerder was ingezet in een ander netwerk en de SAM niet als DHCP-client geconfigureerd was. Helaas was het hierdoor niet mogelijk om de SAM via het netwerk opnieuw in te stellen. Omdat er geen console kabel aanwezig was, was het ook niet mogelijk om de SAM op deze wijze in te stellen als DHCP-client. SercureMe2 heeft daarom een nieuwe SAM opgestuurd die wel ingesteld stond als DHCP-client. Deze was binnen een half uur operationeel binnen het netwerk en de eerste meldingen verschenen hierna in het dashboard.

2.5.2.2 Testfase

In de periode van vier weken waar in de SAM in het netwerk van de IT-dienstverlener heeft gehangen zijn er verschillende meldingen naar voren gekomen. Helaas ging het hier niet om één of meerdere meldingen met een hoge prioriteit. Dit is vanuit het oogpunt van de IT-dienstverlener natuurlijk positief. Wel kwamen er veel meldingen naar voren met prio’s 3, 4 en 5. Deze meldingen vielen voornamelijk in de categorie “Remote Admin”. Dit was te verwachten omdat de IT-dienstverlener

veel hulp op afstand, uitvoert. De een na grootste categorie was “Instant Messaging”. De meldingen in deze categorie waren voornamelijk meldingen die betrekking hadden op de chat dienst Telegram.

2.5.2.3 Evaluatie fase / resultaten pilot

Dit was de laatste fase van de pilot bij de IT-dienstverlener. Na het testen van de SAM-oplossing in het netwerk is er een evaluatie met de IT-dienstverlener ingepland. De vragen die hier centraal stonden en de antwoorden op deze vragen, staan verwerkt in de volgende paragraaf.

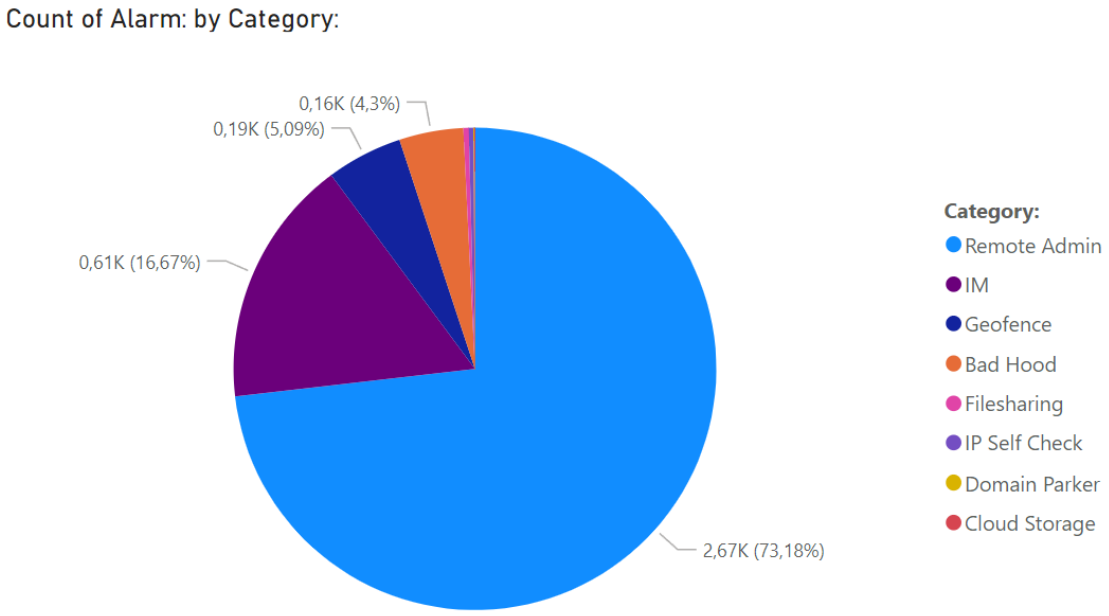
Ziet de IT-dienstverlener de SAM-oplossing als aanvulling op hun dienstverlening naar MKB-ondernemers?

Ja, de SAM-oplossing geeft veel inzicht in het netwerk dat gemonitord wordt. Hierdoor kunnen ook risicovolle trends ontdekt worden. Aan de hand van deze informatie kunnen weer risico verlagende maatregelen worden toegepast.

Het is nog niet haalbaar om dit bij het kleine Mkb’ers in te zetten. Voornamelijk omdat de basisbeveiligingsmaatregelen nog niet volledig zijn toegepast. Hierover volgt een advies in hoofdstuk 3.

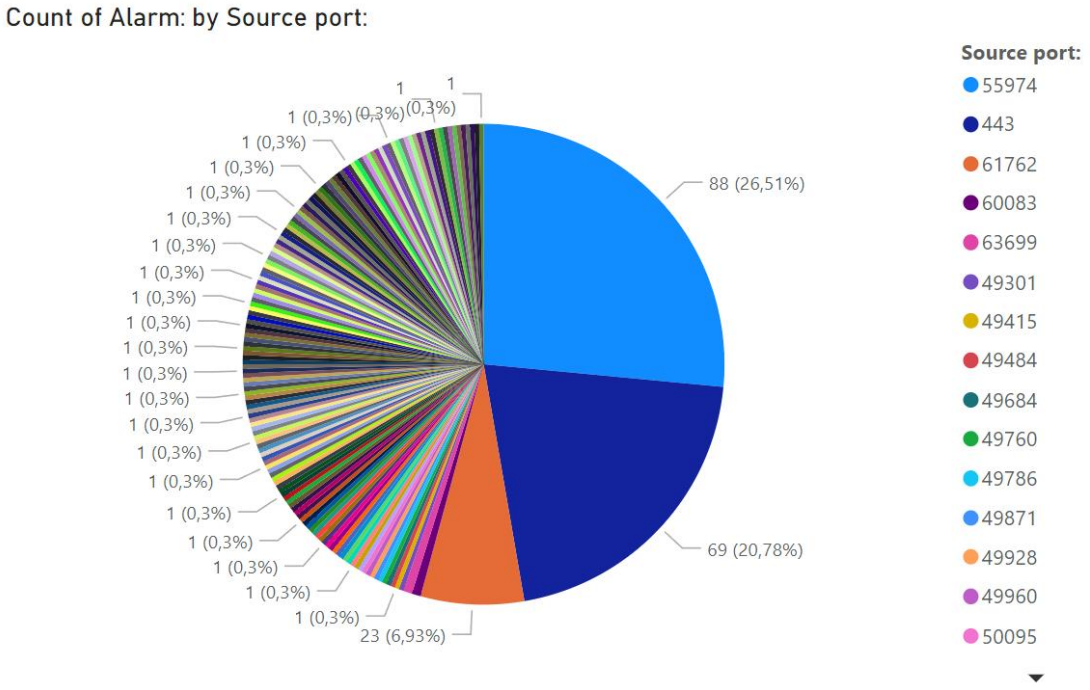
Welke meldingen komen er naar voren in het netwerk van de IT-dienstverlener?

Om een duidelijk beeld te krijgen van welke meldingen de SAM-oplossing verstuurd, zijn deze verwerkt in verschillende diagrammen.



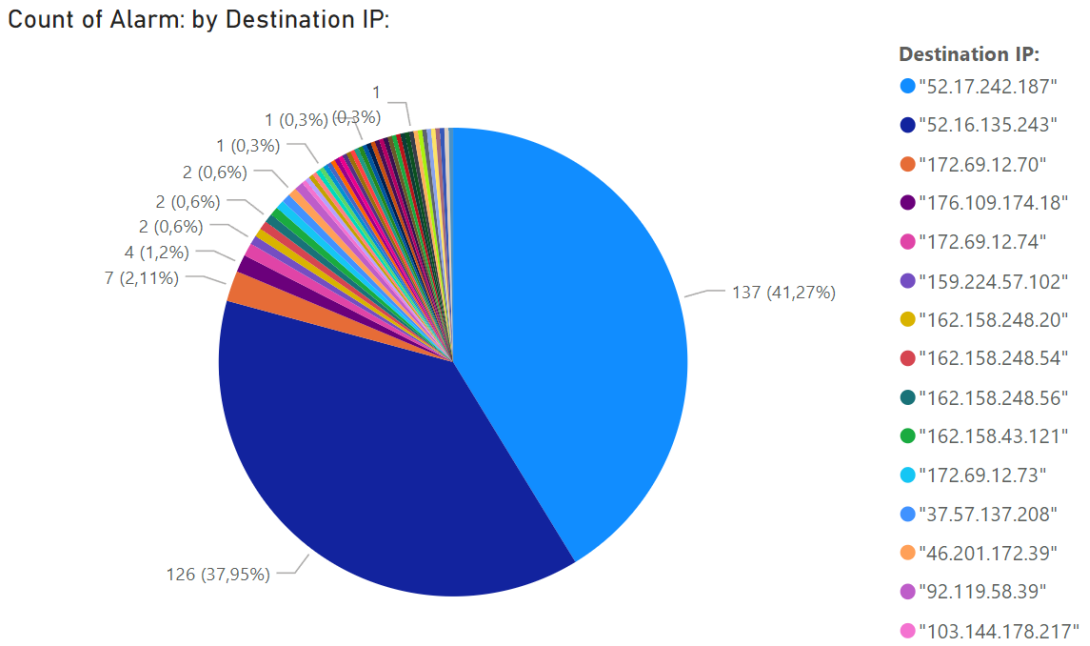
Figuur 1 - Totaal van alarmen, gesorteerd op categorie

Hieruit kan worden geconcludeerd dat de top 3 meest voorkomende categorieën: Remote Admin, IM en Geofence zijn. Dit was in lijn met de verwachtingen omdat er veel Remote Admin software gebruikt wordt. Ook is het te verwachten dat IM hoog boven aan de lijst staat omdat IT-personeel vaker Telegram en andere chat diensten gebruiken dan een standaard gebruiker. De categorie Geofence was niet helemaal in lijn met de verwachtingen. Omdat Geofence meldingen genereerd voor netwerk verkeer van en naar onder andere Rusland en Oekraïne. Ook al is dit maar een klein percentage van alle meldingen.



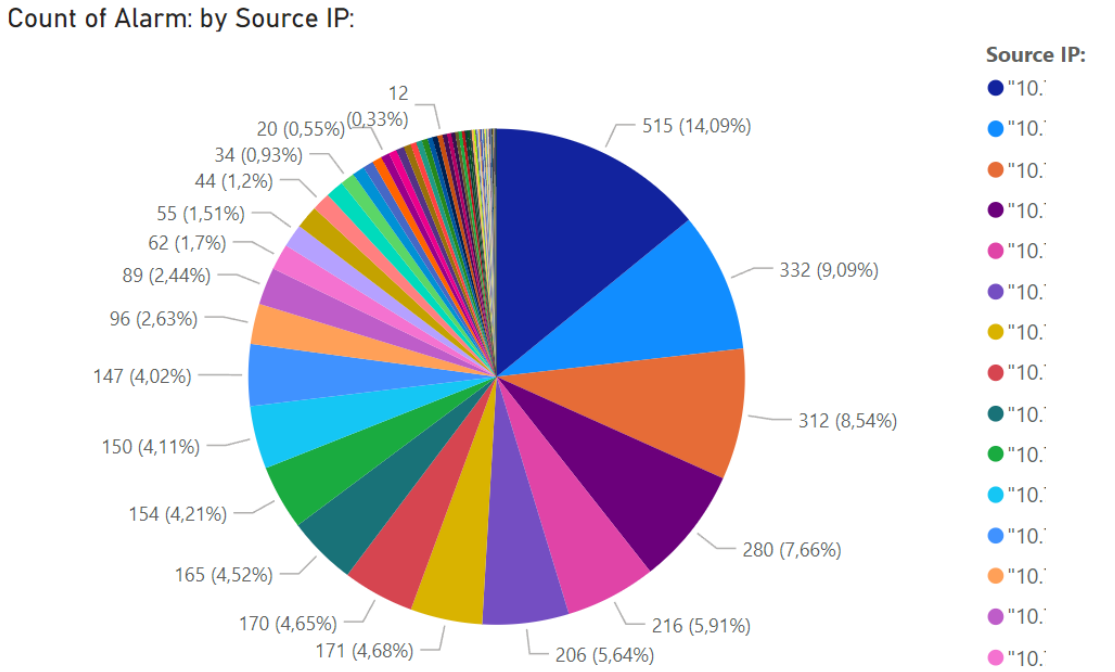
Figuur 2 - Totaal van alarmen, gesorteerd op source port

Uit dit diagram kan worden vastgesteld dat de top 3 poorten: 55974, 443 en 61762 zijn. De poort 55974 en 61762 waren poorten die in lijn waren met de verwachtingen. Omdat deze poorten vaak gebruikt worden om lokaal verbindingen op te zetten. Poort 443 was niet in lijn met de verwachtingen omdat deze vaak als doelpoort wordt gebruikt en niet zo zeer als bronpoort.



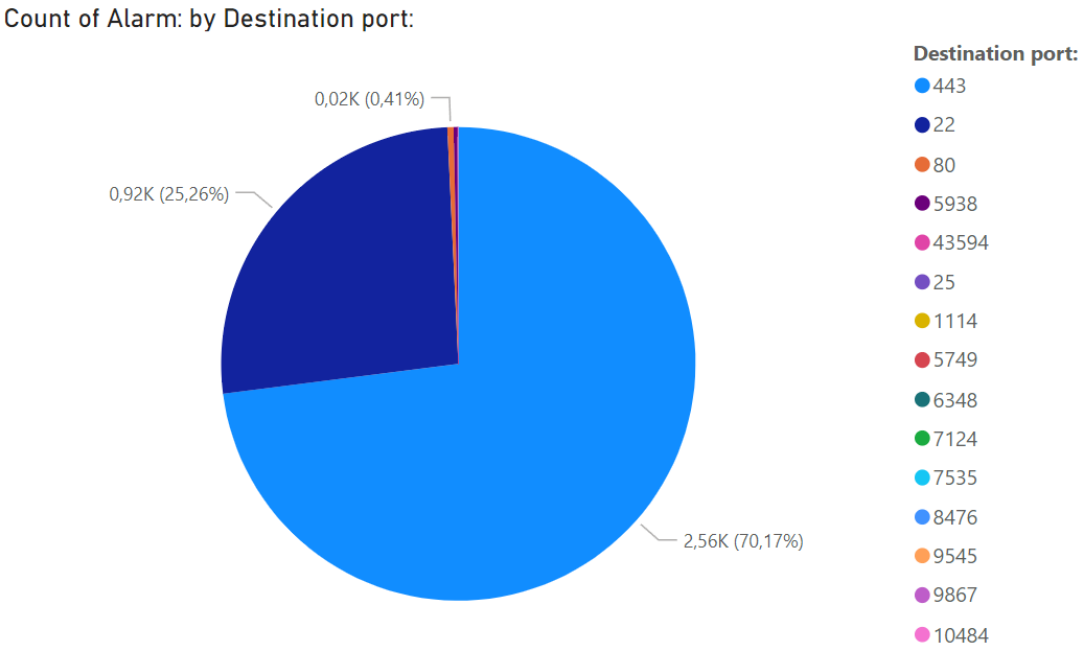
Figuur 3 - Totaal van alarmen, gesorteerd op bestemmings-IP-adres

De eerste 2 IP-adressen zijn waarschijnlijk IP-adressen van de Remote Admin tool die gebruikt wordt. Dit mede omdat er zoveel meldingen in de categorie Remote Admin naar voren zijn gekomen.



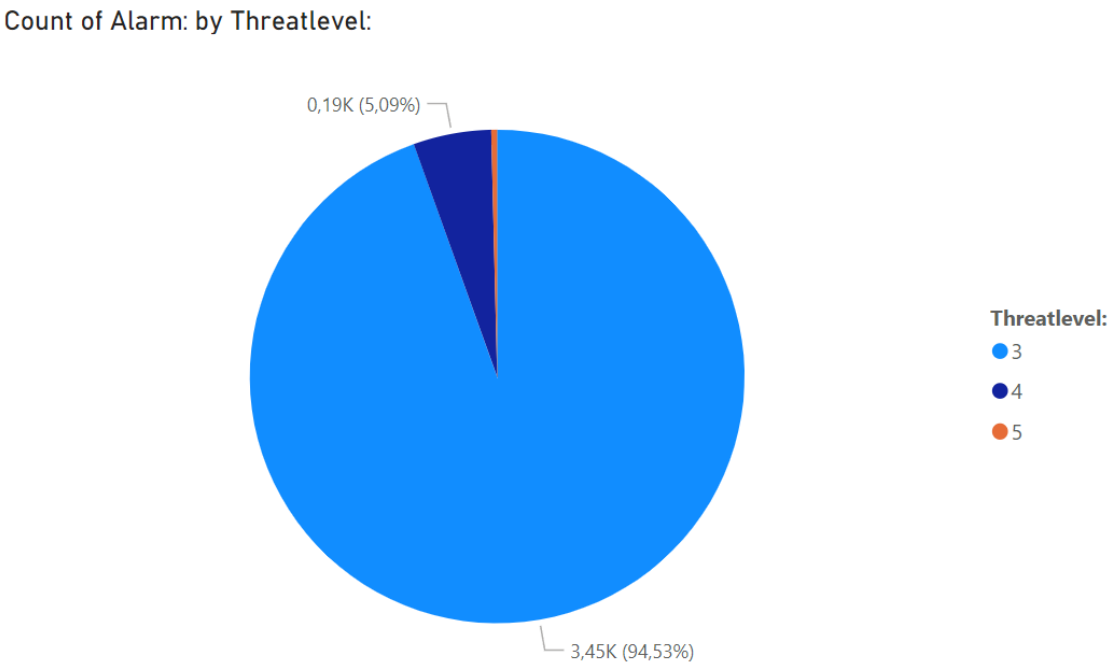
Figuur 4 - Totaal van alarmen, gesorteerd op bron IP

In dit figuur is te zien dat binnen het netwerk van de IT-dienstverlener een IP-adres iets meer alarmen genereerd. De rest zit ongeveer tussen de 150 en 280 meldingen in.



Figuur 5 - Totaal van alarmen, gesorteerd op bestemmings-poort

Aan de hand van dit diagram is af te lezen dat het meeste verkeer waarop meldingen zijn verstuurd, verkeer is dat via SSL versleuteld over poort 443 verstuurd is. Hierna zijn er relatief veel meldingen verstuurd over verkeer op poort 22 (SSH). Dit is te verklaren omdat vaak op servers wordt ingelogd via SSH.



Figuur 6 - Totaal van alarmen, gesorteerd op dreigingsniveau

Zoals aan de hand van dit diagram kan worden vastgesteld, is dreigingsniveau 3 het dreigingsniveau waar de meeste meldingen in naar voren kwamen. Hierna volgt dreigingsniveau 4 met 5 procent van het totaal aantal meldingen.

Uit deze diagrammen kan worden opgemaakt dat de SAM-oplossing veel verschillende meldingen kan versturen. Door deze data te analyseren krijgt de belanghebbende partij een duidelijk beeld van de risico's binnen het netwerk.

Wat doet de IT-dienstverlener met de meldingen die naar voren komen?

Tijdens te pilot zijn er helaas geen meldingen met een hoge prioriteit naar voren gekomen. Alle meldingen met een lage prioriteit zijn alleen bekeken tijdens het evaluatiegesprek. Uit het analyseren van deze meldingen zijn geen bijzonderheden naar voren gekomen.

Is de supportafdeling van de IT-dienstverlener instaat om een risico inschatting te maken van een melding? En hier adequaat op te reageren?

Dit sluit aan bij het vorige punt. Hier is niet op ingegaan omdat de support afdeling geen meldingen met een hoge prioriteit heeft ontvangen.

2.6 Waarom geen IPS?

Het lijkt heel vanzelfsprekend om van de IDS een Intrusion Prevention System (IPS) te maken zodat bedreigingen gelijk geblokkeerd worden. Hierbij zie je belangrijke aspecten over het hoofd. Het gaat hier om een strategische keuze van SecureMe2 om dit niet als IPS aan te bieden. De volgende aspecten spelen hier een rol:

1. Een organisatie wil dat een IDS niet zichtbaar is in het netwerk. Enerzijds om te voorkomen dat een hacker het IDS vindt. SecureMe2 hanteert als best-practice om de output van een IDS in een afgescheiden subnet te plaatsen dat op geen enkele wijze kan communiceren met het productienetwerk van een klant. Anderzijds omdat een organisatie niet wil dat de leverancier van een IDS door kan stappen in het netwerk van de klant. Een organisatie wil risico's verminderen, niet laten toenemen. Ook SecureMe2 moet dus als zero-trust beschouwt worden.

2. Een organisatie wil niet dat een IDS een actief onderdeel van het netwerkpad wordt. Uitval van een inline IDS/IPS is per definitie een extra risico voor de continuïteit.

Een organisatie kan natuurlijk wel slim omgaan met technologie waar die voor ontwikkeld is: Een IDS is goed in detecteren en een firewall is goed in blokkeren. De combinatie levert dus een IPS, en door de functionele scheiding blijft het strategische belang van een onvindbaar IDS gehandhaafd.

SecureMe2 biedt een API aan waar een klant de alarmen en details kan ophalen en op basis daarvan de API van zijn firewall kan aanspreken. Eventueel met een service-management tool (of SIEM/SOC) ertussen.

SecureMe2 ziet veel all-in-one oplossingen (Fortigate, Ubiquity, Sonicwall etc.). Deze hebben allemaal het nadeel dat ze een integraal onderdeel van het netwerk vormen en eenvoudig te herkennen en hierdoor te omzeilen zijn.

3 Advies

In dit hoofdstuk wordt een concreet advies gegeven over de SAM-oplossing.

3.1 Probleemstelling

Het doel van de Stichting is het digitaal weerbaarder maken van het MKB. Binnen dit onderzoek is gekeken hoe een IDS-systeem hieraan een bijdrage kan leveren. De oplossing moet makkelijk te beheren, makkelijk in te richten en makkelijk uit te rollen zijn. Ook moet het de weerbaarheid op een hoger niveau tillen in verhouding tot de kosten. Dit zijn complexe doelstellingen om allemaal in één oplossing terug te kunnen vinden. Omdat het niet haalbaar is om de SAM-oplossing als los product aan kleine MKB-bedrijven aan te bieden, zal de focus worden gelegd op de faciliterende rol van de Stichting.

3.2 De Stichting als faciliterende partner voor IT-dienstverleners

De Stichting kan helpen met het opzetten van SOC dienstverlening die IT-dienstverleners collectief zouden kunnen aanbieden aan kleine MKB-bedrijven. Dit kunnen zij doen door de volgende middelen in te zetten:

- Een project definiëren voor het opzetten van een SOC
- Subsidie ontvangen om medewerkers binnen de IT-dienstverleners trainingen te geven
- Experts inhuren die verstand hebben van SOC dienstverlening
- De SAM-oplossing met korting in een grote hoeveelheid inkopen

Het helpen opzetten van SOC dienstverlening bij een IT-dienstverlener zou als projectvorm worden aangeboden. Waarbij de Stichting experts kan leveren die binnen dit project de IT-dienstverlener van kennis kan voorzien. Ook kan de Stichting medewerkers van de betreffende IT-dienstverlener trainen om SOC dienstverlening aan te bieden. Als de Stichting de SAM-oplossing met korting kan inkopen kan het geld wat hiermee bespaard wordt, gebruikt worden om projecten op te starten en trainingen te geven. De SAM-oplossing is een middel die voldoet aan alle eisen die in de probleemstelling zijn gesteld. Hierdoor zal het netwerkmonitoringsgedeelte van de SOC dienstverlening snel en effectief van de grond komen.

Gezien de huidige staat van het MKB zou het momenteel niet uit kunnen om dit als Stichting te faciliteren. Ook zijn er al veel volwassen organisaties die moeite hebben met het opzetten van een SOC en bij behorende dienstverlening. Naar mijn mening is het zinvoller om eerst de focus te leggen op de basisbeveiligingsmaatregelen en bewustwording. Als deze op een hoger niveau zijn, dan zou SOC dienstverlening en de hierbij aanbevolen SAM-oplossing kans van slagen hebben. Mocht dit in de toekomst wel van de grond komen, dan zou het MKB hierna op een zeer hoog volwassenheidsniveau zitten qua IT-beveiliging.

3.3 Conclusie

Uit de gesprekken die zijn gevoerd met IT-security professionals is gebleken dat netwerk monitoring een essentieel deel is van een goede beveiligingsstrategie. Het is nog lastig om dit kosten efficiënt te implementeren bij het kleinere MKB. Naar aanleiding van dit onderzoek is gebleken dat het zinvol is om eerst de basis beveiliging op orde te hebben. Zoals bijvoorbeeld; goede antivirus en een updatebeleid. Hierna kan netwerk monitoring worden toegevoegd.

De SAM-oplossing is een zeer handig product om een netwerk mee te monitoren op verdachte activiteit. Er is een API beschikbaar waarmee de meldingen naar een SIEM gestuurd kunnen worden. Dit is in dit project niet onderzocht, maar biedt wel mogelijkheden en kansen. Het algoritme dat door de SAM-oplossing wordt gebruikt werkt eigenlijk zo goed, dat je de SAM-oplossing lastig kunt testen. Dit geeft ook aan dat, mocht er zich een hacker in het netwerk schuilhouden, deze bijna geen kans heeft om niet ontdekt te worden. Het is wel van belang om dit goed te testen voordat de oplossing wordt ingezet. Hierdoor kan je aantonen dat de SAM-oplossing dreigingen van verschillende niveaus kan detecteren.

Naar mijn idee is het (nog) niet haalbaar om een SOC-dienst met de SAM-oplossing aan te bieden bij kleine MKB-ondernemers die tussen de 2 en 50 medewerkers in dienst hebben. Ook al is dit zeer afhankelijk van de sector waar deze ondernemer in zit en met welke data deze ondernemer werkt. Een MKB-ondernemer die bijzondere persoonsgegevens verwerkt en zeer afhankelijk is van IT-systemen, is sneller geneigd om meer te investeren in een goede beveiligingsoplossing. Een MKB-ondernemer die weinig tot geen persoonsgegevens verwerkt en minder afhankelijk is van IT-systemen, zal eerder geneigd zijn om deze investering links te laten liggen.

3.4 Vervolgonderzoek

Er zijn een paar onderwerpen waar verder onderzoek naar gedaan moet worden. Deze zijn:

1. Hoe werken de algoritmes die SecureMe2 heeft ontworpen? Moet dit transparanter?
2. Is het via collectieve inkoop aantrekkelijk voor het MKB om deze oplossing af te nemen?
3. Hoeveel Mkb’ers moeten de oplossing minimaal collectief inkopen om het product rendabel te maken?
4. Hoe wordt een centrale SOC ingericht die alle SAM apparaten in het veld uit kan lezen?
5. Hoeveel personeel en middelen zijn er nodig om een SOC op deze schaal in te richten?
6. Is de SAM oplossing het juiste product om deze doelstelling te behalen?
7. Hoe kan de SAM getest worden zodat het hoge prio meldingen verstuurt en zo het algoritme getoetst kan worden?

Bijlagen

B1 Interview opzet

De volgende vragen hebben gediend als leidraad bij het voeren van de interviews:

- Waar in het MKB zou deze oplossing het best passen volgens jou?
- Hoe denk jij dat een MKB ondernemer zonder IT medewerker met een melding moet omgaan?
- Is het automatisch afleveren van een melding aan een IT dienstverlener een goed idee? Misschien opnemen in de SLA?
- Denk jij dat er toegevoegde waarde is voor het MKB om deze oplossing te implementeren?
- Denk jij dat er vanuit privacy oogpunt nog bezwaar zal zijn op deze toepassing?
- Zou een IT leverancier dit wel kunnen aanbieden aan MKB bedrijven? Inclusief beleid en proces (iemand die de monitoring in de gaten houd, weet wat er moet gebeuren met elke melding)

Bibliografie

CBS, R. (2021, 06 25). *het-nederlandse-midden-en-kleinbedrijf-europees-vergeleken*. Opgehaald van cbs.nl: https://www.cbs.nl/nl-nl/longread/diversen/2021/het-nederlandse-midden-en-kleinbedrijf-europees-vergeleken?onepage=true#:~:text=In%20Nederland%20waren%20in%202018,telde%2024%2C9%20miljoen%20bedrijven.

Doorne, K. v. (2021, 10 14). *cybercrime-alle-alarmbellen-moeten-rinkelen*. Opgehaald van mkb.nl: https://www.mkb.nl/column/cybercrime-alle-alarmbellen-moeten-rinkelen

KPN, R. (2020, september 15). *zakelijk/blog/mkb-steeds-vaker-slachtoffer-van-cybercrime.htm*. Opgehaald van kpn.com: https://www.kpn.com/zakelijk/blog/mkb-steeds-vaker-slachtoffer-van-cybercrime.htm

NIPO, v. d. (2015). *ebook_cybersecurity_in_het_mkb*. Opgehaald van https://www.interpolis.nl/~/media/files/ebook_cybersecurity_in_het_mkb.pdf.

Raoul Notté, L. S. (2016/2017). Opgehaald van dehaagsehogeschool: https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/expertisecentra/coecs/infographic-cybersecurity-mkb.pdf

Sluis, C. v. (2019, 05 31). *Cyber Security for Power System operators*. Opgehaald van hbo-kennisbank.nl: https://hbo-kennisbank.nl/details/sharekit_hh:oai:surfsharekit.nl:3113021b-6112-4d86-9308-a7ff843d6574?q=%22Sluis%2C+Casper+van+der%22