ZOLDER

AUTOMATISERING VAN SECURITY OPERATIONS - EEN VERSTANDIGE KEUZE

Whitepaper

ZOLDER

INHOUDSOPGAVE

1

Inleiding

Deze whitepaper is specifiek opgesteld voor de bestuurders en directieleden van mkb-organisaties, zorginstellingen en overheidsinstanties die zich voorbereiden op de naleving van NIS2 en/of die overwegen om dienstverlening in te kopen op het vlak van SOC, SIEM, MDR en/of security operations. In veel gevallen beschikken organisaties van deze omvang niet over uitgebreide interne IT-teams, wat het lastig maakt om de behoefte aan security-diensten goed te formuleren.

Deze whitepaper is geschreven om hulp te bieden bij de selectie van een passende dienstverlener. Daarbij ligt de focus op standaardisatie en automatisering. De reden? Op dit moment zijn security operations veelal niet gautomatiseerd en tegelijkertijd doet zich anno nu een groot tekort aan security experts voor.

Door op deze twee aspecten in te zetten, ontstaat kostenefficiëntie en schaalbaarheid. Waar de meeste SOC-diensten leunen op menselijke, handmatige processen, zijn deze doorgaans onbetaalbaar voor het mkb. Bovendien zal door de introductie van NIS2 de vraag naar security operations-diensten enorm toenemen, waardoor het tekort aan benodigde experts almaar toeneemt.

Dit heeft aanzienlijke gevolgen voor bedrijven die moeten voldoen aan NIS2 maar niet over de juiste mensen en middelen beschikken. Hierdoor zullen deze organisaties uiteindelijk niet in staat zijn om veiliger en conform NIS2 te opereren.

De oplossing bevindt zich in het automatiseren van beveiligingsoperaties. Deze whitepaper biedt een leidraad voor de standaardisatie van de IT waarop de security moet worden uitgevoerd.

2

NIS2

2.1 Security operations en NIS2 – welke vereisten brengt deze nieuw richtlijn met zich mee en hoe beïnvloedt dit uw organisatie?

Wat houdt NIS2 in? De nieuwe Network and Information Security Directive, oftewel de NIS2-richtlijn, is de opvolger van de oorspronkelijke NIS-richtlijn. Deze is in werking gesteld door de Europese Unie en heeft tot doel de cyberbeveiliging en de weerbaarheid van essentiële diensten in EU-lidstaten te versterken.

Sinds 16 januari 2023 is de NIS2-richtlijn van kracht voor bedrijven binnen de Europese Unie. Deze herziene versie breidt de eisen op het gebied van cyberbeveiliging uit en stelt striktere voorschriften voor de rapportage van incidenten. Het zal nog enige tijd duren voordat deze nieuwe Europese richtlijn wordt geïntegreerd in de Nederlandse wetgeving. Organisaties dienen zich vóór 17 oktober 2024 aan deze nieuwe normen te conformeren. Behalve dat de NIS2-richtlijn aangescherpte normen stelt voor beveiliging en rapportage van incidenten, breidt ze haar reikwijdte uit naar een bredere reeks sectoren, waaronder gezondheidszorg, digitale dienstverleners, productiebedrijven en post- en koeriersdiensten.

2.2 Wat betekent NIS2 voor uw organisatie?

De NIS2-richtlijn is dus van toepassing op sectoren die reeds onder de reikwijdte van de eerste NIS-richtlijn vallen, en op een aantal nieuwe sectoren. Een opvallend verschil ten opzichte van de eerste is dat de overheidssector er nu ook binnen valt.

Uw organisatie dient aan de nieuwe vereisten van de NIS2-richtlijn te voldoen. Dit houdt in dat u proactief risico's moet beheersen en uw cyberbeveiliging op hoog niveau moet hebben. Daarnaast moet u in staat zijn om cyberincidenten doeltreffend aan te pakken en binnen 24 uur te melden aan de relevante autoriteit. Het niet naleven van de NIS2-richtlijn kan resulteren in aanzienlijke sancties, waaronder boetes tot maximaal twee procent van uw totale jaarlijkse omzet.

> **"Vroeger was het nodig om een consultant over de vloer te krijgen. Bijvoorbeeld om M365 veilig in te richten. Nu zit de kennis van die consultant in een app."**
>
> BRITEBLUE - GERT-JAN BIERKENS

2.3 Welke verplichtingen schrijft de NIS2-richtlijn voor?

Mogelijk heeft u al eerder overwogen om de cyberbeveiliging van uw eigen organisatie te verbeteren, maar binnenkort wordt dit een verplichting noodzaak. In de praktijk betekent dit dat zogenaamde essentiële en belangrijke organisaties aan specifieke eisen moeten voldoen. Deze eisen omvatten:

• **Zorgplicht:** de NIS2-richtlijn omvat een zorgplicht die entiteiten verplicht om zelf een gedegen risicobeoordeling uit te voeren. Op basis van deze beoordeling moeten zij passende maatregelen treffen om de continuïteit van hun essentiële diensten te waarborgen en de vertrouwelijkheid van de gebruikte informatie te beschermen.

• **Meldplicht:** binnen de richtlijn wordt bepaald dat entiteiten binnen een termijn van 24 uur incidenten moeten melden aan de toezichthoudende instantie. Deze meldingsplicht heeft betrekking op incidenten die een aanzienlijke impact kunnen hebben op de verlening van essentiële diensten/taken. Daarnaast moet een cyberincident gemeld worden aan het Computer Security Incident Response Team (CSIRT), dat op zijn beurt ondersteuning en hulp kan bieden. Diverse factoren spelen een rol bij de vraag of een incident meldingswaardig is, waaronder het aantal personen dat door de verstoring getroffen is, de duur van de verstoring en mogelijke financiële schade.

• **Toezicht:** organisaties die onder de reikwijdte van de NIS2-richtlijn vallen, worden onderworpen aan toezicht. De richtlijn schrijft voor dat er een onafhankelijke toezichthouder (los van eventueel interbestuurlijk toezicht) belast wordt met het controleren van de naleving van de richtlijnverplichtingen, zoals de zorg- en meldplicht.

2.4 Hoe kunt u ervoor zorgen dat u aan deze nieuwe vereisten voldoet?

De voornaamste operationele uitdaging die voortvloeit uit de NIS2-richtlijn draait om de meldingsverplichting. Deze vereist dat incidenten op een effectieve manier worden behandeld en dat cyberincidenten binnen een tijdsbestek van 24 uur worden gerapporteerd. Dit impliceert dat zowel de detectie als de afhandeling van incidenten voortdurend paraat moeten zijn. Met andere woorden, de technologische aspecten - zowel software als hardware die alarmeren - dienen voortdurend operationeel te zijn. Eveneens moet er binnen de organisatie onmiddellijk opvolging worden gegeven aan dergelijke alarmeringen.

Dit heeft vooral invloed op uw beveiligingsactiviteiten, niet noodzakelijkerwijs beperkt tot een Security Operations Center (SOC), maar eerder op de bredere scope van de uit te voeren taken en werkzaamheden.

“In de checks van Attic zitten dingen waar je zelf niet aan denkt. En je kunt simpelweg in de app kijken of alles goed is.”

VERWATER - ARDJAN VISSERS

ZOLDER

Wat is een Security Operations Center? In de praktijk houdt een SOC zich bezig met het bewaken van de computer- en netwerkactiviteiten binnen een organisatie. Hierbij wordt informatie van zowel applicaties als apparaten in het bedrijfsnetwerk verzameld en onderworpen aan een grondige analyse om afwijkende patronen te identificeren. Deze gegevens kunnen afkomstig zijn van diverse bronnen, zoals servers, antivirussoftware, firewalls, webapplicaties, clouddiensten en zelfs industriële controlesystemen. Dit alles draait om het vergaren van relevante informatie met betrekking tot de beveiliging van alle systemen en apparaten. De verzamelde gegevens vormen gezamenlijk inzichten in de veiligheid van het netwerk, de systemen en de hardware- en softwarecomponenten die binnen de organisatie opereren.

Om een solide afweer te hebben tegen digitale aanvallen, is het essentieel om een duidelijk overzicht te hebben van uw organisatie’s digitale infrastructuur en de activiteiten die zich daarin afspelen. Een Security Operations Center vormt een effectief hulpmiddel om toezicht te houden op de veiligheid van bedrijfsinformatie en digitale dreigingen. De vraag is of een Center ook daadwerkelijk een oplossing is voor uw eigen organisatie.

2.5 Wat verstaan we onder Security Operations?

Met security operations verwijzen we naar de beveiligingswerkzaamheden zelf. Met andere woorden, niet de personen die beleid opstellen, risicoanalyses uitvoeren, awareness campagnes implementeren. Het draait om de experts die concreet verantwoordelijk zijn voor het uitvoeren van technische beveiligingsmaatregelen, het waarborgen van de correcte configuratie van deze maatregelen en het bewaken dat deze actief zijn. Een security operator is iemand die detecteert wanneer een ingestelde beveiligingsmaatregel een waarschuwing geeft en vervolgens deze waarschuwing onderzoekt. Zijn er geen waarschuwingen? Dan gaat de security operator “hunten” naar kwetsbaarheden of verdacht gedrag dat niet eerder was opgevallen.

Helaas komt het te vaak voor dat organisaties geavanceerde beveiligingstools aanschaffen maar geen duidelijke protocollen hebben voor het omgaan met de gegenereerde waarschuwingen. Dit resulteert erin dat de organisatie slechts een tool heeft die meldingen genereert, zonder dat dit daadwerkelijk de veiligheid van de organisatie aanzienlijk verbetert.

Grootzakelijke bedrijven beschikken doorgaans over een eigen IT-team dat verantwoordelijk is voor basis IT-taken. Ideaal gezien zou een dergelijke organisatie binnen dat IT-team, of juist erbuiten, een gespecialiseerde security-afdeling moeten hebben.

Bij organisaties in het kleine tot middelgrote segment is er meestal geen omvangrijke IT-afdeling aanwezig. In het gunstigste geval heeft een mkb-organisatie enkele medewerkers die verantwoordelijk zijn voor IT, maar vaak leunen deze sterk op externe partijen.

Wanneer externe expertise wordt ingeschakeld, is doorgaans één IT-partner verantwoordelijk voor het beheren van de basis IT, en bijvoorbeeld heel goed in Microsoft365. Dit betekent echter niet

automatisch dat deze partner expert in op het gebied van beveiliging. En als een mkb'er specifieke vragen heeft over cybersecurity, zoals het onderzoeken van verdachte activiteiten in het netwerk, valt dit vaak buiten de scope van hun dienstverlening.

Mkb-organisaties en kleinere zorg- en overheidsinstellingen komen daarom vaak voor de volgende uitdagingen te staan:

1. Ze hebben doorgaans **beperkte mogelijkheden** om een diepgaand **inzicht** te verwerven en een eigen inhoudelijk oordeel te vellen over de werkzaamheden binnen een SOC.

2. Als gevolg van **krapte op de arbeidsmarkt** worden ze vaak gedwongen om deze activiteiten uit te besteden.

3. Vanwege een gebrek aan kennis of ervaring neigen ze ertoe **verouderde best practices** te volgen bij het aanbesteden van SOC-diensten, vaak opgesteld door IT-consultants die opereren in omgevingen met tienduizenden werknemers.

In situaties waarin deze werkzaamheden al intern worden uitgevoerd, is de kans groot dat ze worden toegewezen aan iemand met bredere IT-taken, of dat nu iemand is binnen of buiten de organisatie. Hieruit ontstaat echter het probleem dat deze taken als secundair worden beschouwd. Een bijkomend gevolg is dat security operations hoogstwaarschijnlijk niet, niet goed of niet op consistente basis worden uitgevoerd, vooral vanwege een gebrek aan tijd en expertise.

Het uitvoeren van security operations gaat verder dan eenvoudige technische vaardigheden. Het vereist specifieke expertise en diepgaande kennis van geavanceerde aanvalsmethoden en inzicht in de werkwijzen van aanvallers, die ook nog eens continu evolueren. Alleen met deze expertise en kennis kunnen verdachte activiteiten worden geïdentificeerd, grondig worden onderzocht en op een doeltreffende manier worden tegengegaan. De volgende vragen zijn van essentieel belang voor een doordachte aanpak:

• Beschikt uw organisatie over het benodigde budget om toegewijd personeel in te zetten voor deze taak?

• Bent u in staat individuen aan te trekken met de juiste competenties en achtergrond om deze gespecialiseerde taken uit te voeren?

Voor veel mkb's blijkt het een aanzienlijke uitdaging om bovenstaande vragen positief te beantwoorden. In een uitgebreid SOC werken meerdere beveiligingsprofessionals samen aan uiteenlopende en complexe taken. Deze samenwerking stelt grotere organisaties in staat om snel en doelgericht te reageren op.

Echter, voor kleinere organisaties is dit vaak niet haalbaar. De beperkte schaal en middelen maken het moeilijk om op dezelfde manier te opereren. Het kan onmogelijk zijn om te concurreren met grotere spelers wanneer er binnen een kleinere instelling slechts één alarm per maand wordt geregistreerd.

Bij het overwegen van uitbesteding is het belangrijk om niet overhaast te handelen. Vele SOC-diensten zijn prijzig, met name voor kleinere organisaties. Een verstandige aanpak is om eerst de behoeften van uw organisatie te analyseren en vervolgens partners te selecteren die oplossingen bieden die aansluiten op uw budget en behoeften.

3

Standaardisatie

3.1 Start het inrichten van security operations bij het kiezen van de gewenste aanpak

Een Security Operations Center is een krachtig instrument om grip te houden op de beveiliging van bedrijfsinformatie en digitale dreigingen. Het inrichten ervan kost tijd, geld en moeite. Een kernaspect van een succesvol SOC ligt in het vermogen om gecontroleerd mee te groeien met de toenemende behoefte aan informatiebeveiliging binnen een organisatie.

Doorgaans zijn er twee verschillende aanpakken om een SOC op te zetten: top-down en bottom-up. Beide benaderingen hebben hun eigen voordelen en uitdagingen. Het is belangrijk om rekening te houden met de specifieke behoeften, middelen en cultuur van een organisatie om de meest geschikte aanpak te kiezen en te zorgen voor een effectieve beveiligingsstrategie.

Transparantie en communicatie met alle stakeholders zijn essentieel, ongeacht de gekozen benadering, om de acceptatie en het succes van het SOC te waarborgen.

Bij een top-down benadering initieert een onderneming de identificatie van bedrijfsrisico's door de nodige detectiemaatregelen vast te stellen. Potentiële problemen worden beschreven in zogenaamde use cases, waarna eerst in theorie bedacht wordt waar en hoe triggers kunnen worden ontwikkeld om het betreffende risico in beeld te brengen. Ook wordt overwogen wie en hoe er gereageerd moet worden op alarmen. Pas nadat alle stakeholders het eens zijn geworden welke use cases gebouwd moeten worden en in welke volgorde, begint de implementatiefase.

Aan de andere kant, bij de bottom-up benadering, wordt direct gestart met het ontsluiten en centraliseren van bronnen met logbestanden. Dit proces van centralisatie vormt vaak al een uitdaging, iets waar bij de top-down benadering doorgaans pas laat wordt ontdekt. Bij een bottom-up aanpak komen de eerste logbestande al snel binnen, waarna wordt geanalyseerd welke soorten gegevens erin zitten en welke verdachte patronen mogelijk kunnen worden waargenomen. Dat wordt uiteindelijk gekoppeld aan een geïdentificeerd risico.

Zolder adviseert om de aanvangsfase bescheiden te houden en de resultaten helder te communiceren naar de organisatie. Een open en transparante communicatie met alle betrokkenen, vormt de sleutel tot het succes van het SOC en de acceptatie ervan binnen de organisatie.

> **"De waarde van Attic zit hem in de content. En je hoeft niemand op te lijnen om de hele M365-tenant te beheren."**
>
> KAAK - SEBASTIAN BEIJERSBERGEN

Top-down benadering - **voordelen:**	Top-down benadering - **uitdagingen:**
Leidinggevenden starten strategische planning voor SOC in relatie tot ricisomanagement.	Lange tijd voor eerste detectiemaatregelen actief zijn, of deze technisch onuitvoerbaar blijken.
Dit vergt investeringen wat betreft snelheid en geavanceerde technologie.	Kosten en meetbaar rendement cruciaal.
Rapportage aan het management voor afstemming.	

Bottom-up benadering - **voordelen:**	Bottom-up benadering - **uitdagingen:**
Snel eerste alarmen actief in het SOC, klaar om opvolgingsproces te gaan inrichten en oefenen.	Mogelijke fragmentatie tussen initiatieven door gebrek aan coördinatie.
Geleidelijke, aanpasbare groei van SOC.	Onduidelijke relatie van detectiemaatregelen tot risicomanagement.
Meer draagvlak en begrip op de werkvloer.	
Kostenbeheersing omdat gespreid over tijd.	

Het is bij het advies van het Nationaal Cyber Security Centrum (NCSC) belangrijk om zich te realiseren dat een SOC een middel is, geen doel op zichzelf.

De zoektocht naar de juiste security operator is een uitdaging die niet onderschat mag worden. Zolder beveelt aan om in sterkte mate te kiezen voor automatisering en standaardisatie als een pragmatische benadering.

> **"Waar ik vooral enthousiast over ben is dat Zolder tegen een schappelijke prijs een dashboard en monitor maakt die MSFT mist in hun securityportal."**
>
> JOH. MOURIK & CO. HOLDING B.V. - GODFRIED BOSHUIZEN

In de meeste gevallen loopt een mkb-organisatie het hoogste risico op misbruik bij het behandelen van e-mailberichten en het uitwisselen van documenten. Veel van de kleinere bedrijven maken gebruik van Microsoft 365 of Google Workspace als basis voor hun activiteiten.

3.2 Standaardisatie levert de volgende pluspunten op:

1. Voorspelbaarheid: door de basis van IT te standaardiseren bereikt u uniformiteit en gemak in de toepassing van beveiligingsmaatregelen, wat de algehele veiligheid ten goede komt.
2. Geïntegreerde beveiligingsoplossingen: een gestandaardiseerde aanpak op basis van Microsoft 365 of Google Workspace levert direct diverse beveiligingsfuncties op die binnen deze diensten beschikbaar zijn, wat de effectiviteit van uw beveiligingsstrategie versterkt.
3. Vereenvoudigde centralisatie van beveiligingsgegevens: standaardisatie vereenvoudigt het centraal beheer van beveiligingsgegevens, waardoor een overzichtelijke blik op mogelijke bedreigingen ontstaat en snelle detectie mogelijk is.
4. Geautomatiseerde updates en patches: het gebruik van gestandaardiseerde systemen maakt geautomatiseerde beveiligingsupdates en patches mogelijk, waardoor kwetsbaarheden efficiënt worden aangepakt.
5. Geïntegreerde rapportage en analyse: standaardisatie legt de basis voor geïntegreerde rapportage en diepgaande analyse van beveiligingsgegevens, wat waardevolle inzichten oplevert om bedreigingen te herkennen en te beheersen.
6. Schaalbaarheid en flexibiliteit: een gestandaardiseerde aanpak met Microsoft 365 vergemakkelijkt schaalbaarheid en flexibiliteit, zodat uw beveiligingsinfrastructuur met uw organisatie kan meegroeien.
7. Ondersteuning van een ecosysteem van beveiligingspartners: standaardisatie creëert een omgeving waarin verschillende beveiligingspartners naadloos kunnen samenwerken en hun gespecialiseerde tools en diensten kunnen integreren.

Sinds 2019 biedt Microsoft met Azure Sentinel een alles-in-één oplossing voor het monitoren, analyseren en beveiligen van de cloud. Met Azure Sentinel kunnen beheerders van uitgebreide cloudomgevingen kwetsbaarheden en externe dreigingen snel identificeren en onschadelijk maken. Dit leidt tot een gigantische en actieve gebruikersbasis: binnen Sentinel van Microsoft zijn ongeveer tien keer zoveel actieve gebruikers die een bijdrage leveren als bij de nummer 2 aanbieder in deze sector, Splunk.

Binnen het kader van moderne zakelijke operaties blijkt dat mkb-organisaties, zorginstellingen en lagere overheidsinstanties te maken hebben met een intrinsiek risico: het potentiële misbruik van e-mailberichten en de uitwisseling van documenten. Deze essentiële communicatiekanalen vereisen bijzondere aandacht om de veiligheid te waarborgen. Veel organisaties maken gebruik van Microsoft 365 of Google Workspace als het om communicatie gaat.

Zowel Microsoft 365 als Google Workspace bieden een reeks uitgebreide hulpmiddelen die de uitvoering van security operations mogelijk maken, zonder dat externe partijen noodzakelijk zijn voor oplossingen. Misschien rijst bij u de vraag of u zich wilt neerleggen bij de dominante positie van deze twee giganten, met name Microsoft als het gaat om Office?

Ons standpunt voor besluitvormers binnen het mkb is om deze overweging niet al te zwaar te nemen. Kijk welke kansen het uw organisatie biedt en laat het beteugelen van marktdominantie over aan verantwoordelijke instanties. In plaats daarvan adviseren we te focussen op het versterken van de weerbaarheid van uw onderneming op een doeltreffende wijze.

Tal van de benodigde tools voor security operations zijn reeds opgenomen in uw Microsoft 365- of Google Workspace-abonnement. Met andere woorden, u hebt er al voor betaald; benut deze functionaliteiten eenvoudig door de juiste selectievakjes aan te vinken.

3.3 Standaardisatie op basis van de Microsoft- of Google-omgeving. Hoe gaat dat in zijn werk?

Om te beginnen, activeert u de tools voor security operations in uw Microsoft- of Google-omgeving die bedreigingsbewaking en aanvullende beveiligingsmaatregelen mogelijk maken. Deze tools sporen incidenten op en ondersteunen de opvolging ervan. In het geval van Microsoft is dit Sentinel en voor Google gaat het om Chronicle. Als deze tools eenmaal actief zijn en ingesteld om uw kantooractiviteiten te bewaken, heeft u al een groot deel van de veelvoorkomende bedreigingen aangepakt. Dit vormt in wezen het hart van uw eigen IT-beveiligingsinfrastructuur.

Een passende SOC-dienst zou de kern van IT als basis nemen om een automatiseringslaag te realiseren. Die automatisering zou zo worden opgezet dat er geleidelijk aan extra IT-componenten aan kunnen worden toegevoegd om mee te groeien en zich aan te passen aan de organisatie.

Zodra de monitoring van dit kerngedeelte actief is, bieden de security operations tools de mogelijkheid om meer logbronnen toe te voegen. Denk aan de logbestanden van uw firewall(s), uw CRM-software, ERP-systeem of productielijnen. Een deel van deze software kan op maat zijn gemaakt voor uw organisatie, maar doorgaans bevat software een standaardfunctie om logbestanden te verzenden naar een centrale opslag: uw beveiligingsinfrastructuur. Voer deze aanpassingen pas door wanneer uw organisatie hier daadwerkelijk klaar voor is en op een manier die eenvoudig op- en af te schalen is.

Naarmate uw organisatie groeit of verandert, verandert ook uw IT- en datalandschap. Het kan zijn dat sommige logbestanden niet langer relevant zijn, of juist nieuwe moeten worden toegevoegd. De basis, bijvoorbeeld Outlook en Excel, of Gmail en Google Docs, zal niet snel veranderen. De kern blijft solide en behoudt zijn plek.

4

Automatisering

4.1 De voordelen van geautomatiseerde SOC-processen zijn

- betrouwbaarder detectie en respons op bedreigingen
- verhoogde efficiëntie en productiviteit van cybersecurity-teams
- vermindering van menselijke fouten en incidentresponsvertragingen
- schaalbaarheid en flexibiliteit van cybersecurity-operaties, geen last van arbeidsmarktschaarste
- verbeterde kostenbeheersing en betaalbaarheid

Automatisering wordt een stuk makkelijker, als u inzet op standaardisatie op basis van bijvoorbeeld Microsoft 365 of Google Workspace. Hoe meer uw organisatie afhankelijk is van maatwerk in de IT, des te complexer het geheel wordt en des te hoger de kosten zullen zijn om effectieve cyberbeveiliging toe te passen. Houd het simpel en werk zoveel mogelijk vanuit de geïntegreerde functies van uw basis-IT.

4.2 Automatisering drukt de kosten

Uiteraard zijn de kosten van deze dienstverlening van groot belang. In het verleden, toen gestandaardiseerde IT-omgevingen nog niet gebruikelijk waren, vergde het veel handmatig werk voor een Managed Security Service Provider (MSSP) om ervoor te zorgen dat alarmsignalen werden geactiveerd EN vervolgens adequaat werden opgevolgd.

Echter, dankzij het advies om te kiezen voor standaardisatie, zijn veel van de security operations in uw omgeving nu automatiseerbaar. Cloudservices kunnen immers worden beheerd met behulp van scripts, en als deze scripts werken in uw Microsoft- of Google-cloud, dan zullen ze op exact dezelfde wijze werken voor alle andere klanten die dezelfde diensten gebruiken. En dat zijn er een heel veel!

Heeft de dienstverlener waarin u geïnteresseerd bent ingezet op automatisering? Dan zal de dienst in de basis waarschijnlijk goed betaalbaar zijn. Maar het heeft ook geen zin als de dienst alleen maar inhoudt dat u alarmen automatisch doorgestuurd krijgt. Worden onnodige alarmen – de zogenaamde false positives - uitgefilterd? Is er ook een deskundige beschikbaar om bij te springen als er een serieus incident optreedt? Een expert die kan onderzoeken wat een aanvaller heeft gedaan zodra hij toegang heeft gekregen. Of sinds wanneer? Die kan verifiëren dat de toegang daadwerkelijk goed is opgeheven? Het beantwoorden van dergelijke vragen wordt Incident Response genoemd en is meestal niet geïntegreerd in de basismonitoringdienst, maar is wel van essentieel belang om afspraken over te maken.

Een geschikte SOC-dienst zou deze kern van de IT als vertrekpunt moeten nemen om een automatiseringsplatform te creëren, dat geleidelijk aan extra IT-componenten kan toevoegen, meegroeiend en flexibel met uw organisatie.

Het vorengaande ligt ten grondslag aan de visie van Zolder bij de ontwikkeling van de eigen oplossing genaamd Attic Security om kleine en middelgrote organisaties te ondersteunen als experts in cybersecurity. Met behulp van deze tool waarborgen we de veiligheid van uw onderneming. Aangezien aanvallen onvoorspelbaar zijn, blijven we met u in contact via onze mobiele app. Zo kunnen we u te allen tijde informeren en adviseren, ongeacht uw locatie.

Attic Security integreert naadloos met Microsoft 365 om alle beveiligingsfuncties daar optimaal te configureren en incidenten te monitoren. Zodra we iets verdachts detecteren, ontvangt u direct een pushmelding en het bijbehorende advies dat u met één druk op de knop kunt activeren.

Onboarding in Attic duurt slechts vijf minuten, waarna de basis SOC-functie direct actief is. Hiermee is een continue incidentafhandeling gegarandeerd.

Attic maakt het eenvoudig om met minimale inspanning een goed inzicht te hebben in de security parameters van uw Microsoft 365-landschap

5

Conclusie en samenvatting

De NIS2-richtlijn, die voortbouwt op de NIS-richtlijn, heeft tot doel de cyberbeveiliging in EU-lidstaten te versterken. Deze richtlijn introduceert nieuwe normen en meldingsvereisten die van toepassing zijn op kleine en middelgrote ondernemingen binnen de EU. Concreet vereist NIS2 een proactieve aanpak van risicobeheersing, een hoog niveau van cyberbeveiliging en snelle melding van incidenten. Deze richtlijn omvat niet alleen de sectoren die al onder de vorige versie vielen, maar breidt zich ook uit naar de overheidssector. Het is van cruciaal belang om vóór 17 oktober 2024 aan deze richtlijn te voldoen om aanzienlijke sancties te voorkomen.

Een effectieve manier om de cybersecurity-activiteiten te versterken, bedreigingen sneller te detecteren en adequaat te reageren op incidenten, is door Security Operations Centers (SOC) te automatiseren.

Standaardisatie van de basis-IT maakt automatisering van security operations mogelijk en biedt een waardevolle mogelijkheid voor mkb-ondernemingen en kleine tot middelgrote zorg- of overheidsinstellingen om aan de eisen van NIS2 te voldoen. Volledig geautomatiseerde Security Operations Centers blijken bijzonder efficiënte oplossingen. Veel kleine tot middelgrote organisaties staan echter voor uitdagingen, zoals beperkte expertise en financiële middelen. Standaardisatie vereenvoudigt uniforme beveiliging, naadloze gegevensintegratie en schaalbaarheid.

Veel mkb-organisaties maken gebruik van populaire platforms zoals Microsoft 365 en Google Workspace, die geïntegreerde beveiligingshulpmiddelen bieden. Door deze hulpmiddelen optimaal te configureren en te benutten, kunnen de kosten van security operations worden verlaagd en de naleving van NIS2 worden verbeterd.

Een geautomatiseerd SOC, gebaseerd op Microsoft 365 of Google Workspace, kan op maat gemaakte beveiligingsoplossingen bieden. Het vinden van de juiste balans tussen automatisering en expertise is essentieel voor een effectieve respons op incidenten.

Al met al maakt automatisering van security operations het haalbaar voor kleine tot middelgrote ondernemingen om te voldoen aan de eisen van NIS2. De Attic Security-tool van Zolder, die integreert met Microsoft 365, is ontworpen om dit proces te vereenvoudigen.

> **“Attic geeft ons snel en goed inzicht en biedt ook de mogelijkheid direct aandachtspunten op te lossen voor de prijs van eigenlijk een no-brainer voor iedere gemeente om de basisconfiguratie in Microsoft 365 veilig in te richten en ingericht te houden. De inrichting was binnen 5 minuten gedaan en daarna konden we al de eerste optimalisaties doorvoeren.”**
>
> GEMEENTE BODEGRAVEN-REEUWIJK - RALPH WAGTER

Over Zolder

Zolder, opgericht door Rik van Duijn, Wesley Neelen, Theo Snelleman en Erik Remmelzwaal, brengt diverse expertise op het gebied van cybersecurity samen. In een wereld waar digitalisering via robotica, virtual reality en IoT in een snel tempo evolueert, voorziet Zolder in toegepast digitaal beveiligingsonderzoek.

Deze passie gedreven onderneming is ontstaan uit de vereniging van 'diehard' cybersecurity experts en softwareontwikkelaars, die hun vaardigheden hebben ontwikkeld vanuit een zolderkamer-mentaliteit.

Met meer dan vijftig jaar gecombineerde ervaring in cybersecurity research, biedt Zolder oplossingen voor beveiligingsuitdagingen in het digitale domein. Het bedrijf richt zich op hacking, malware, reverse engineering, data-analyse, ICT-beheer en meer. Zolder's team streeft ernaar om een solide basis te leggen voor cybersecurity werk, waarbij ze hun uitgebreide kennis inzetten voor digitale consultancy, virusuitbraken, en de strategische ontwikkeling van zowel security hardware als software.

Bibliografie

- https://www.ncsc.nl/onderwerpen/detectie/soc-inrichten
- Factsheet SOC inrichten: begin klein, Nationaal Cyber Security Centrum, 2 mei 2023
- https://digital-strategy.ec.europa.eu/en/policies/nis2-directive