Security monitoring in de zorgsector

COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

ZA CERT

Inhoud

1. Introductie

Voorkomen is beter dan genezen. Het is een bekend gezegde en zeker ook van toepassing op het informatiebeveiliging domein. We weten echter ook dat voorkomen niet altijd gaat. Niet in de zorg, en ook niet in de IT-security. Maatregelen zijn niet geïmplementeerd, niet volledig of niet goed bijgehouden en kunnen daarom falen. Daarom is het belangrijk om een vangnet te hebben: weten wanneer het mis gaat (en dus wanneer incidenten ontstaan), zodat daar vervolgens effectief op gereageerd kan worden. Op deze manier houden we de impact van security incidenten zo klein mogelijk. Security monitoring is een belangrijk middel in vaststellen dat een security incident gaande is. Deze whitepaper beschrijft hoe security monitoring in de zorgsector kan worden vormgegeven.

1.1. Security monitoring

Security monitoring is een belangrijk middel om te detecteren dat een security incident gaande is. Door snel en adequaat te handelen kan het security incident in de kiem gesmoord worden, waardoor de impact van security incidenten beperkt kan worden. Security monitoring stelt de organisatie in staat om meer proactief om te gaan met security incidenten. Daarnaast speelt het ook een rol in het voorkomen van security incidenten door vast te stellen dat beheersmaatregelen falen of onvoldoende goed zijn ingericht.

Om op een goede manier vorm te kunnen geven aan security monitoring is een aantal ingrediënten noodzakelijk:

- De juiste tooling
- De juiste processen
- De juiste mensen

1.1.1. Security monitoring tooling

Voor security monitoring wordt traditioneel gebruik gemaakt van Security Information & Event Management (SIEM) systemen. Een SIEM systeem kan worden gevoed met logging uit de gehele infrastructuur, van netwerk- en security-componenten tot servers en applicaties, en brengt deze samen. Op deze samengebrachte informatie worden vervolgens logische zoekopdrachten uitgevoerd die kunnen resulteren in een alarm. Een belangrijk kenmerk van SIEM systemen is dat deze in Near Real-Time (NRT) werken, wat concreet inhoudt dat de detectie binnen enkele minuten na het registreren in de logging plaatsvindt. De verdere opvolging is afhankelijk van de juiste processen.

Andere of aanvullende manieren om vorm te geven aan security monitoring is met behulp van monitoring op de eindsystemen waar medewerkers gebruik van maken (endpoint detectie en response, EDR), monitoring in het netwerk (netwerkdetectie en response (NDR)) of detectie door middel van geavanceerde deceptie technologie. Ook dreigingsinformatie, zoals de informatie die gedeeld wordt in het Zorg Detectie Netwerk (ZDN), wordt vaak actief verwerkt in security monitoring om zorg te dragen dat actuele dreigingen snel gedetecteerd worden.

Verzamelen van logging

Zoals aangegeven werken SIEM systemen op basis van informatie (logging) die in de infrastructuur gegenereerd wordt. Deze logging wordt vervolgens op een veilige manier opgehaald uit de infrastructuur door het SIEM systeem (pull methodiek) of verzonden naar het SIEM systeem (push methodiek). Het voeden van het SIEM systeem met de juiste informatie is niet altijd triviaal. Allereerst is het belangrijk dat de juiste logging gegenereerd wordt. Het kan nodig zijn om de instellingen voor het genereren van logging aan te passen. Daarnaast is het uiteraard ook noodzakelijk om de push- en pull-mechanismen goed te laten werken. Vaak betekent dit dat wijzigingen in de infrastructuur (zoals de firewall) noodzakelijk zijn. Bij netwerken die in kleinere delen (segmenten) opgedeeld zijn, kan dit complex zijn. Ook kan het nodig zijn om additionele accounts aan te maken die rechten hebben op de logging, of om de juiste API toegang en calls toe te staan.

> **“Security monitoring stelt de organisatie in staat om meer proactief om te gaan met security incidenten.”**

Concreet betekent dit dat een organisatie zich bewust moet zijn van de inspanningen die nodig zijn om aan te kunnen sluiten op security monitoring tooling. Weten welke apparatuur zich in het netwerk bevindt is daarbij een belangrijk uitgangspunt. Daarnaast gaat bijzondere aandacht uit naar het aansluiten van niet-standaard apparatuur. Voor die apparatuur is het belangrijk dat binnen de organisatie voldoende kennis is over de werking van de apparatuur en de mogelijkheden om logging op te (laten) vragen.

“Een organisatie moet zich bewust zijn van de inspanningen die nodig zijn om aan te kunnen sluiten op security monitoring tooling.”

1.1.2. Security monitoring processen

De processen rondom security monitoring zijn met name gericht op de juiste opvolging van meldingen uit security monitoring tooling. Deze meldingen moeten worden beoordeeld om vast te stellen of inderdaad sprake is van een mogelijk security incident (triage). Afhankelijk van de uitkomst van de triage zal bepaald worden op welke wijze en met welke prioriteit opvolging gegeven moet worden aan het mogelijke incident. Bij die afweging spelen veel factoren een rol, zoals de aard van de melding en het belang van het systeem wat de melding genereert. Een melding van een virus dat geblokkeerd is, behoeft veel minder prioriteit dan een vreemde toegangspoging tot één van de kernsystemen.

Opvolging

Detectie van security incidenten met behulp van security monitoring heeft weinig waarde als het voor de organisatie niet mogelijk is om goede opvolging te geven aan de gevonden incidenten. Het is daarom zaak om bij de invoering van security monitoring ook direct zorg te dragen voor een gedegen security incident response. Daarbij moet nagedacht worden over welke middelen voor ingrijpen bij het incident response team liggen en onder welke condities ingegrepen mag worden. Ook als een organisatie gebruik maakt van

een security serviceprovider voor het leveren van SOC-diensten, is het van belang de incident response goed in te richten. Bedenk daarbij dat 24/7 dienstverlening door de SOC leverancier ook 24/7 bereikbaarheid voor de eigen organisatie betekent.

Use cases

Naast opvolging vormen ook use cases een belangrijk proces binnen security monitoring. Een use case beschrijft een specifieke dreiging, hoe deze zich kan manifesteren en hoe deze gedetecteerd kan worden. Vooral dat laatste is belangrijk in de context van security monitoring. Feitelijk bepaal je met behulp van use cases wat je precies wilt detecteren. Het is daarom erg belangrijk om goed na te denken over waar de detectie zich op moet richten. Bekijk een dreiging vanuit verschillende perspectieven, zowel vanuit top-down (vanuit risico's) als vanuit bottom-up (vanuit bekende aanvals-technieken en log analyse) om niets over het hoofd te zien.

Organisatie-specifieke use cases

Bij de top-down aanpak vanuit risico's kunnen ook use cases gedefinieerd worden die specifiek zijn voor de organisatie. Deze zullen technisch vertaald worden naar betrokken applicaties en infrastructuur. Vervolgens wordt op basis van de logging bepaald onder welke condities een alarm gegenereerd wordt. Dit alarm wordt door de security analisten beoordeeld. Voor het realiseren van niet-standaard use cases geldt, net zoals voor niet-standaard log collectie, dat binnen de organisatie voldoende kennis moet zijn van de betrokken applicaties en infrastructuur. Daarnaast moet ook voldoende kennis aanwezig zijn van de inhoud en de betekenis van de logging die gegenereerd wordt.

False positives

Met regelmaat komt het voor dat een alarm gegenereerd wordt en opgevolgd wordt door een analist, maar dat er geen sprake is van een security incident. In dat geval spreken we van een false positive. Bij false positives wordt onderscheid gemaakt in foutief gegenereerde alarms waarbij de condities voor het alarm niet kloppen en false positive incidenten, waarbij het alarm terecht is afgegaan maar geen sprake is van een security incident. Vaak moet een analist contact opnemen met medewerkers in de organisatie om navraag te doen over specifieke situaties.

Allow listing
False positive incidenten leiden vaak tot het opbouwen van een zo-genaamde allow list. Daarin wordt bijgehouden in welke specifieke situaties een bepaald alarm niet hoeft af te gaan. Het is van groot belang om de registratie van de inhoud van de allow list zorgvuldig te doen en regelmatig te evalueren, zodat voorkomen wordt dat een groeiende blinde vlek in de monitoring ontstaat.

> **“Security analisten staan centraal in security monitoring en bepalen in grote mate de kwaliteit en snelheid van het security monitoring proces.”**

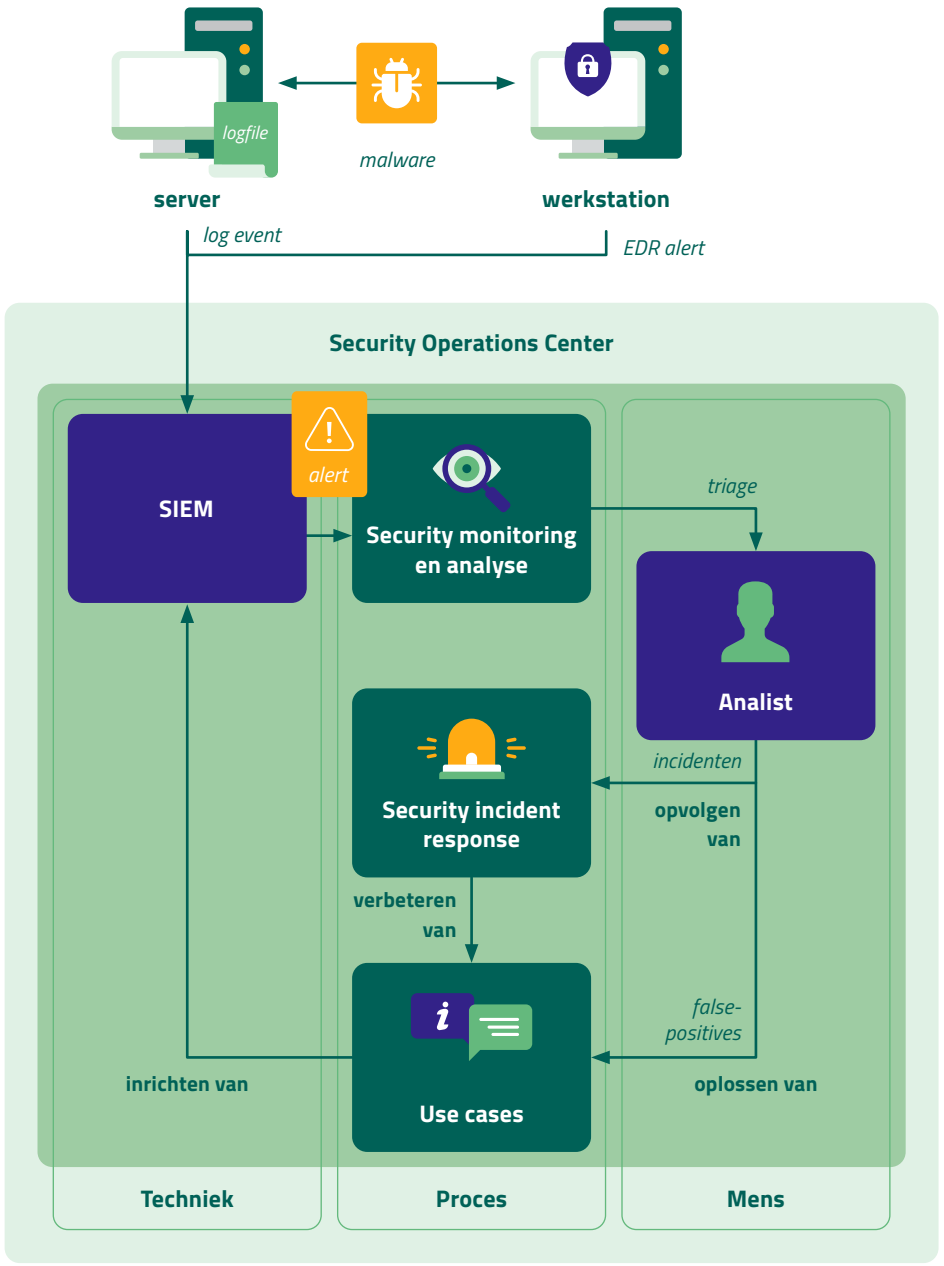
1.1.3. Security analisten

Nu de techniek en de processen beschreven zijn, is het ook zaak om naar de mensen achter deze techniek en processen te kijken: de security analist. Security analisten staan centraal in security monitoring en bepalen in grote mate de kwaliteit en snelheid van het security monitoring proces. Security analisten zijn bekend met de technieken die aanvallers gebruiken, goed op de hoogte van recente ontwikkelingen in cyber security, getraind in het gebruik van de tooling en efficiënt en effectief in de omgang met de processen. Hierdoor zijn security analisten in staat om, ook onder hoge druk, de juiste inschattingen en afwegingen te maken om te komen tot adequate opvolging.

1.2. Security Operations Centers

Security monitoring is een activiteit die veelal door een security operations center (SOC) uitgevoerd wordt. Die is een afdeling die belast is met preventie, detectie en response voor cyber security incidenten. Een eenduidige definitie van een SOC bestaat eigenlijk niet, omdat veel verschil bestaat tussen SOCs onderling en met name de inrichting en het palet aan diensten wat aangeboden wordt door het SOC aan de organisatie. Security monitoring en (initiële) security incident response zijn activiteiten die in ieder geval veelal uitgevoerd worden. Een SOC heeft de technologie, processen en mensen om invulling te geven aan deze diensten.

Het figuur hiernaast toont hoe malware leidt tot het uitvoeren van security incident response door analisten in het security operations center. Dat kan enerzijds via logging die verwerkt wordt door het SIEM systeem, of een directe integratie vanuit een security component op een werkstation (end-point detectie en response), die ontvangen wordt door het SIEM systeem en 1-op-1 een melding doorzet naar de analist.



Figuur 1: malware alert opvolging door het SOC

Naast de kernactiviteiten security monitoring en security incident response (en use case management als ondersteunende activiteit) zijn moderne SOCs vaak ook bezig met threat intelligence (weten waar de aanvallers mee bezig zijn) en threat hunting (proactief op zoek gaan naar signalen van digitale inbraak). Ook security automatisering technologie zoals Security Orchestration en Automated Response (SOAR) speelt een steeds grotere rol om efficiënt en effectief om te kunnen gaan met meldingen.

> **“Het is mogelijk om, met behulp van een MSSP, een security monitoring dienst te realiseren die voldoet aan de eisen die gesteld worden door de organisatie.”**

1.2.1. Managed security service providers

Veel organisaties kiezen ervoor om niet zelf een SOC te gaan bouwen. Dat komt met name door het gebrek aan security analisten in de markt en de significante investering die gedaan moet worden in een SOC wat op het juiste niveau van volwassenheid acteert. Om die reden wordt vaak gekeken naar dienstverlening van Managed Security Service Providers (MSSPs). Dit zijn commerciële partijen die security dienstverlening aanbieden, waaronder steeds vaker ook SOC dienstverlening. Het is mogelijk om, met behulp van een MSSP, een security monitoring dienst te realiseren die voldoet aan de eisen die gesteld worden door de organisatie. Bedenk daarbij dat ook in een situatie van uitbestede dienstverlening de organisatie zelf coördinatie zal moeten uitvoeren, door het navragen van meldingen binnen de organisatie en het uitvoeren van incident response binnen de organisatie, al dan niet gesteund door een externe partij.

2. Security monitoring in de zorgsector

In het voorgaande hoofdstuk is uiteengezet wat security monitoring is, en hoe dit veelal ingericht wordt. In dit hoofdstuk wordt aandacht besteed aan de specifieke eisen die aan security monitoring in de zorg gesteld worden.

2.1. Specifieke aandachtspunten voor de zorg

Binnen de zorg is een aantal specifieke aandachtspunten van belang:

1. **Specialistische apparatuur.** Zorginstellingen werken vaak met specialistische apparatuur. Deze apparatuur wordt soms op een afwijkende manier geüpdatet (jaarlijks in plaats van maandelijks). Het installeren van een end-point oplossing of het verzamelen van logging uit dergelijke apparatuur is daarnaast vaak niet mogelijk. Het is daarom met name zaak om monitoring in te richten op netwerk toegang tot deze apparatuur.

2. **Patiëntveiligheid.** Security incidenten in het netwerk van zorginstellingen kunnen een direct effect hebben op de veiligheid van patiënten. Ransomware kan bijvoorbeeld voor grootschalige uitval van IT-apparatuur zorgen, wat tot gevolg heeft EPD niet beschikbaar is en patiënten moeten uitwijken naar andere ziekenhuizen.

3. **Gesegmenteerd netwerk.** Gesegmenteerde netwerk zijn verplicht conform de NEN 7510 en komen daarom vaak voor in zorginstellingen. Met goede segmentering wordt het moeilijker

gemaakt voor aanvallers om binnen een netwerk te bewegen. De aansluiting op security monitoring kan daardoor echter ook lastiger worden, omdat vanuit de verschillende segmenten naar een centrale omgeving gelogd moet worden. Een gedegen ontwerp van de infrastructuur voor het verzamelen en doorsturen van logging (bijvoorbeeld met log forwarders) is dan noodzakelijk.

4. **Uitbestede IT dienstverlening.** Veel zorginstellingen werken met dienstverleners voor IT. Bij het invoeren van security monitoring is het dan zaak om ook met de andere partijen duidelijke afspraken te maken over navraag en opvolging van alarmen en incidenten. Instellingen met veel IT-partners krijgen daarmee een sterke coördinerende rol, waar rekening mee gehouden moeten worden. Ook zijn niet alle leveranciers bereid om actief mee te werken aan aansluiten op monitoring door derden. Goede contractuele afspraken spelen daarbij een belangrijke rol.

5. **Vertrouwelijkheid van informatie.** Zorginstellingen werken met bijzondere persoonsgegevens, die passend beveiligd moeten worden (zoals patiëntinformatie). Deze informatie kenmerkt zich door een hoge mate van vertrouwelijkheid. Security monitoring helpt om deze vertrouwelijkheid te bewaken. Echter betekent de invoering van security monitoring ook dat extra toegang (op systeem- en netwerkniveau) noodzakelijk is om de logging op te halen. Het is van groot belang deze toegang zorgvuldig in te richten en te controleren om te voorkomen dat misbruik via de security monitoring paden plaatsvindt.

6. **Omgang met incidenten.** Kleinere organisaties hebben minder security capaciteit. De afhandeling van kleine incidenten en het navragen van alarmen gaat wel goed, maar de expertise om gedegen opvolging te geven aan grotere security incidenten ontbreekt. Het is dan zaak om goede afspraken te hebben met externe partijen die kunnen ondersteunen. Een dergelijke afspraak wordt een retainer genoemd. Deze retainer kan vastgelegd worden met dezelfde partij zijn die de security monitoring dienstverlening biedt of met een andere partij.

Naast bovenstaande punten zijn ook de NEN7510, 7512 en 7513 normen specifiek voor de zorg. Deze worden hierna behandeld.

2.2. Regelgeving rond informatiebeveiliging

Voor security monitoring in de zorg is de regelgeving zoals beschreven in de NEN7510 en NEN7513 vooral van belang, naast algemene regelgeving zoals AVG.

2.2.1. NEN7510

In de NEN7510-2 wordt beschreven op welke manier vormgegeven moet worden aan *'verslaglegging en monitoren'*. Onder de beheersmaatregel *'gebeurtenissen registreren'* (paragraaf 12.4.1) wordt het volgende gesteld:

"Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld."

Hierna geven we een aantal voorbeelden van type gebeurtenissen die beoordeeld dienen te worden, waaronder gebeurtenissen die zijn gedetecteerd door security componenten op de systemen zelf. Daarnaast stelt de NEN7510-2 dat *"Logbestanden van gebeurtenissen [...] de basis [vormen] van geautomatiseerde monitorsystemen die geconsolideerde rapporten en waarschuwingen over systeembeveiliging kunnen verzamelen".* Met de eerdergenoemde SIEM systemen en de andere genoemde security monitoring technologie, kan invulling gegeven worden aan de eis voor geautomatiseerde monitoringsystemen die gespecialiseerd zijn in het detecteren van security dreigingen binnen de infrastructuur. De analisten geven vervolgens invulling aan het *beoordelen* van de gebeurtenissen zoals bedoeld in paragraaf 12.4.1.

2.2.2. NEN7513

De NEN7513 gaat specifiek over toegang tot patiëntendossiers en vormt daarmee een belangrijke use case binnen de security monitoring in de zorg. Ongeautoriseerde toegang tot patiëntendossiers schaadt de privacy van de patiënt en daarmee het vertrouwen in de zorginstelling. Het vaststellen of sprake is geweest van ongeautoriseerde toegang tot een elektronisch patiëntendossier kan achteraf, door het beoordelen van de audit logging of het doen van een steekproef. Als onregelmatigheden worden aangetroffen, kunnen deze verder onderzocht worden. Dergelijke controles vinden echter allemaal plaats nadat de ongeautoriseerde toegang (mogelijk veelvuldig) heeft plaatsgehad, waarmee het vertrouwen en de privacy van de patiënt al is geschaad.

Door een security monitoring use case te realiseren voor de NEN7513 is het mogelijk om real-time te detecteren dat er sprake kan zijn van ongeautoriseerde toegang. De organisatie wordt dan veel sneller in staat gesteld om te acteren, waardoor de impact van een dergelijk incident veel kleiner kan blijven. Voor het realiseren van een dergelijke use case is het noodzakelijk om de logging van de toegang tot het elektronische patiëntendossier door te sturen naar het SIEM systeem. Voor het vormgeven van de use case moet goed in kaart gebracht worden onder welke condities sprake kan zijn van ongeautoriseerde toegang. Deze condities worden vertaald naar technische condities. Het is zaak om met regelmaat de configuratie van deze condities te valideren, om te zien of deze nog voldoende zijn om ongeautoriseerde toegang adequaat te kunnen detecteren en niet te veel 'false positives'' gegenereerd worden.

Stuur alleen die informatie naar het SIEM systeem die daadwerkelijk nodig is voor het realiseren van de gewenste use case. Het versturen van informatie over patiënten moet voorkomen worden.

2.3. 10 best practices voor security monitoring in de zorg

Ter afsluiting van deze whitepaper worden in deze paragraaf 10 best practices beschreven voor security monitoring in het algemeen, en voor de zorg in het bijzonder.

1. **Zorg voor een intern response team (eventueel met hulp van een externe partij)**

Het interne incident response team is verantwoordelijk voor de opvolging van incidenten of afwijkende gebeurtenissen. Zonder adequate opvolging is het niet zinvol om security monitoring uit te voeren. Bedenk bij de inrichting van security incident response ook welke 'openingstijden' gehanteerd worden. Kan er iemand gebeld worden als in het weekend of in de nacht een verdachte situatie ontstaan is?

2. **Maak goede afspraken met bestaande IT-leveranciers en monitor deze afspraken**

Indien gebruik gemaakt wordt van bestaande IT-leveranciers, is het zaak om duidelijke afspraken te maken en deze vast te leggen in een dienstenniveau overeenkomst (DNO). Deze afspraken moeten gaan over opvolging van vragen en incidenten (en de response tijden die daar mee gemoeid zijn), maar ook over het aanleveren

van informatie (logging) aan het security monitoring systeem. De coördinatie en regie over de leveranciers ligt bij de organisatie. Daar moet voldoende aandacht naar uit gaan. Let daarbij op dat niet alleen het maken van de afspraken belangrijk is, maar ook het evalueren of de leverancier zich daadwerkelijk houdt aan de afspraken.

3. Zorg voor monitoring van de gehele keten

Veel organisaties hebben ketenpartners die nodig zijn voor de dienstverlening. Sommige van deze ketenpartners zijn IT-partners, en hebben mogelijk een directe (netwerk) of indirecte (email of software) verbinding met de organisatie. In de security monitoring moeten dit soort koppelvlakken bijzondere aandacht krijgen, omdat cyber criminelen ook via dergelijke 3e partijen digitaal proberen in te breken.

4. Stem af met privacy over in de invoering van security monitoring

Met security monitoring worden gedragingen van medewerkers in kaart gebracht. Afhankelijk van hoe de infrastructuur is opgezet en welke logging aangeleverd wordt aan het security monitoring systeem kunnen dat gedragingen in applicaties zijn, maar ook surf-gedrag. Security monitoring heeft altijd impact op de privacy van de medewerker op de werkplek. Stem daarom goed af met privacy en besteed aandacht aan doelbinding (waarom wordt het gedaan) en proportionaliteit (wat is er echt nodig om het doel te behalen). Hou daarbij ook rekening met wat de AVG op dit gebied voorschrijft.

5. Betrek medewerkers bij de invoering van security monitoring

Omdat security monitoring impact heeft op de privacy van de medewerker op het werk, is het belangrijk om de medewerkers tijdig op de hoogte te stellen van de invoering van security monitoring en wat dat voor hen betekent. Zo kunnen er vragen gesteld worden over hun activiteiten op computersystemen. Dat kan het gevoel geven dat men “bespioneerd” wordt. Transparantie over het proces is een belangrijke factor om dit tegen te gaan. De invoering van security monitoring en de mogelijke aanpassingen van het beleid om dat mogelijk te maken, moeten doorgaans door de Ondernemingsraad goedgekeurd worden.

6. Voorkom dat gevoelige informatie in een security monitoring systeem terecht komt

Gevoelige informatie, zoals informatie over zorg aan patiënten, is veelal niet nodig voor het uitvoeren van security monitoring activiteiten. Het is daarom belangrijk om actief zorg te dragen dat deze informatie niet verstuurd wordt aan het security monitoring systeem. Door het uitvoeren van een Privacy Impact Analyse (PIA) kan vastgesteld worden aan welke eisen het security monitoring systeem moet voldoen, welke informatie verwerkt kan worden en hoe lang deze informatie bewaard mag worden.

7. Voer actief life cycle management uit op security monitoring use cases en logbronnen

Use cases zijn niet statisch. Aanvalstechnieken veranderen, de infrastructuur verandert, applicaties veranderen en regelgeving (zowel intern als extern) verandert. Om de security monitoring met deze veranderingen mee te laten bewegen, is het noodzakelijk om actief life cycle management uit te voeren op de use cases. Daarmee kan de actualiteit van de security monitoring dienstverlening geborgd worden. Ook logbronnen moeten actief onderhouden worden, omdat wijzigingen in het log-formaat tot gevolg kunnen hebben dat monitoring niet meer werkt.

8. Zorg voor beleid wat security monitoring ondersteunt

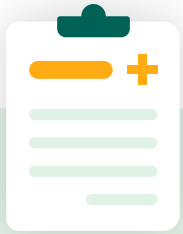
Om tot een effectieve inrichting van security monitoring te komen is het belangrijk om beleid te hebben wat ondersteunend is aan security monitoring. Denk daarbij aan beleid voor incident response, met het mandaat om in te kunnen grijpen onder bepaalde omstandigheden. Maar ook een duidelijk auditing en logging beleid, waarin uiteengezet wordt welke logging gegenereerd moet worden en hoe deze opgeslagen moet worden, is belangrijk. Tenslotte dient ook in beleid vastgelegd te worden dat aansluiting op security monitoring verplicht is.

9. Zorg voor voldoende capaciteit en kennis om infrastructuur te kunnen aansluiten

Aansluiten op een SIEM systeem is niet altijd triviaal. Zorg er daarom voor dat intern voldoende kennis en kunde is om de aansluiting te realiseren. Deze kennis en kunde moet zicht richten op netwerk connectiviteit, configuratie van logging, access control en least privilege voor log collectie en inhoudelijke kennis van de betekenis van logging. Dit laatste is met name belangrijk voor organisatie-specifieke use cases.

10. Valideer de werking van detectie en response

Tenslotte is het ook erg belangrijk om de werking van de detectie en response zoals uitgevoerd door het SOC te valideren. Dat kan door het uitvoeren van een assessment op het SOC (bijvoorbeeld met hulp van de open source SOC-CMM self-assessment tool) en als technische validatie met een red team oefening. In een red team oefening wordt een aanval gesimuleerd. Daarbij wordt geprobeerd om digitaal in te breken op een infrastructuur. Het doel van de red team oefening is om de werking van de preventieve maatregelen te toetsen, maar ook de kwaliteit van detectie van de digitale inbraak en de effectiviteit en efficiency van de incident response na detectie van het incident door het SOC vast te stellen. Binnen de zorg wordt red teaming uitgevoerd met het ZORRO programma (**ZO**rg **R**edteaming **R**esilience **O**efeningen).



2.4. Conclusie

In deze whitepaper is beschreven wat verwacht kan worden van security monitoring en SOC dienstverlening. Met security monitoring dienstverlening, uitgevoerd door een SOC, kan gezorgd worden voor vroege detectie van security incidenten binnen een organisatie. Met security monitoring kan ook vorm gegeven worden aan de eisen in de NEN7510 rondom de beoordeling van logging en continue bewaking op inzage in elektronische patiëntendossiers.

Echter is de invoering van security monitoring geen sinecure. Belangrijk is dat dit type dienstverlening extra inzet en middelen vraagt van de organisatie. Denk daarbij aan:

- Het realiseren van de technische aansluiting van log bronnen
- Het bedenken, uitwerken en technisch realiseren van organisatie-specifieke use cases
- Het coördineren van incidenten en alarmen binnen de organisatie
- Het coördineren met verschillende andere IT dienstverleners
- Het managen en bewaken van de kwaliteit en actualiteit van de security monitoring dienst

De allocatie van voldoende middelen is een randvoorwaarde voor de inzet van security monitoring. Door invulling te geven aan deze randvoorwaarde en met inachtneming van de best practices zoals beschreven in dit document is het mogelijk om een succesvolle implementatie van security monitoring uit te voeren. Gebruik maken van een managed security service provider zal voor veel organisaties de gewenste manier zijn om in te voeren, waarbij de organisatie zelf de regie en de coördinatie houdt tussen de SOC-dienstleverancier, de medewerkers, de overige leveranciers en de ketenpartners.

Stichting Z-CERT
Stationsplein 121
3818 LE Amersfoort
033 737 06 09

info@z-cert.nl
www.z-cert.nl