SIEM: dé oplossing voor het beveiligings-beheer van het IT-landschap?

M.J.J. de Boer RE CISA MSc
is werkzaam bij KPMG IT Advisory. Hij heeft zich gespecialiseerd in beveiligingsoplossingen met een geautomatiseerde component, met een sterke focus op risicobeheer. Hieronder vallen zowel geautomatiseerde autorisatiescans (waaronder Access Governance) als geautomatiseerde beveiligingsmonitoring (waaronder SIEM).

deboer.maarten@kpmg.nl

Ir. A.H.P. van Vliet
is werkzaam bij KPMG IT Advisory als junior adviseur. Zijn werkterrein ligt op het gebied van informatiebeveiliging. In die hoedanigheid voert hij zowel advies- als auditopdrachten uit. Zijn expertise ligt met name op geautomatiseerde monitoringoplossingen zoals SIEM en Database Activity Monitoring (DAM).

vanvliet.arjan@kpmg.nl

Maarten de Boer RE CISA MSc en ir. Arjan van Vliet

Het steeds complexer wordende IT-landschap betekent voor organisaties een groeiende uitdaging dit aantoonbaar onder controle te houden. De eerste uitdaging is het in kaart brengen van de beveiligingsstatus van dit landschap. Deze informatie is niet alleen nodig in verband met compliance-eisen vanuit wet- en regelgeving zoals de Sarbanes-Oxley (SOx), privacywetgeving en de Payment Card Industry Data Security Standard (PCI DSS), maar het stelt organisaties ook in staat tijdig en adequaat te reageren op belangrijke beveiligingsmeldingen en de steeds complexer en professioneler wordende externe dreigingen. De tweede uitdaging ligt in het adequaat handelen naar aanleiding van de gedetecteerde beveiligingsmeldingen en -dreigingen. Dit stelt organisaties beter in staat te reageren op dreigingen en geeft hen ook meer inzicht in het risico dat zij lopen. Dit artikel geeft een introductie tot Security Information & Event Management (SIEM) als oplossing voor de gerezen vraagstukken.

Inleiding

Moderne computernetwerken staan onder een continue dreiging van hackers en ongeautoriseerde handelingen van (malafide) medewerkers. IT-omgevingen worden complexer, onder andere door fusies en acquisities. Externe IT-dienstverleners krijgen een steeds grotere rol juist doordat zeer specialistische kennis nodig is voor specifieke IT-omgevingen. De afhankelijkheid van informatietechnologie groeit. Hierdoor neemt het aantal (bekende) beveiligingsincidenten dagelijks toe en stijgen de kosten daarvan ([KPMG10], [McAf11]).

In reactie hierop hebben organisaties geprobeerd zichzelf te beschermen door het implementeren van beveiligingsmaatregelen zoals antivirussoftware, firewalls en intrusion detection systemen. Deze producten zijn stuk voor stuk nuttig maar creëren ook nieuwe problemen. Immers, de complexiteit van het IT-landschap neemt toe, net als het aantal beveiligingsmeldingen. Dit stelt bedrijven voor twee uitdagingen. Enerzijds het in kaart brengen van de beveiligingsstatus van het IT-landschap en anderzijds adequaat handelen naar aanleiding van de gedetecteerde beveiligingsmeldingen en -dreigingen.

Aan deze uitdagingen zijn twee belangrijke aspecten verbonden: 'inzicht' en 'tijdigheid'. De uitdaging is om op grond van de miljoenen beveiligingsmeldingen te komen tot tijdige

en relevante inzichten. Dit op een slimme geautomatiseerde manier. Deze 'slimme manier' moet de menselijke factor in de operationele uitvoering zo klein mogelijk houden om de reactiesnelheid en de kosten zo laag mogelijk te houden. De alternatieven, zoals het (laten) uitvoeren van een grote hoeveelheid IT-audits of het (periodiek) handmatig doorzoeken van logbestanden, zijn vaak geen reële optie. Deze alternatieven kennen vaak een vrij lange aanloop- en doorlooptijd, met veel menselijke betrokkenheid en daarmee relatief hoge kosten.

De markt heeft deze wens inmiddels onderkend. Onder de naam Security Information & Event Management (SIEM) ontplooien diverse organisaties en leveranciers initiatieven die handig inspelen op de geschetste situatie en de wensen van het management. Dit artikel heeft als doel helderheid te scheppen over zaken die meespelen in de volgende vragen: Wat is SIEM? En hoe kan een SIEM-voorziening helpen de wensen over 'tijdig inzicht' in te vullen? Daarnaast zullen we ingaan op leerervaringen uit de praktijk.

Wat is SIEM?

In de loop der tijd zijn diverse definities en interpretaties van SIEM ontstaan, mede doordat SIEM tevens een marketingconcept is geworden. SIEM kan begrepen worden als:

> *... de combinatie van software en hardware die is toegewezen om geautomatiseerd IT-gerelateerde beveiligingsinformatie te verzamelen, te combineren en te analyseren, met als doel om tijdig inzicht te krijgen en proactief te reageren op activiteiten die een negatieve invloed kunnen hebben op de vertrouwelijkheid, integriteit of beschikbaarheid van data of IT-middelen.*

Onder 'IT-gerelateerde beveiligingsinformatie' verstaan wij het volgende:

- Gebeurtenissen die een negatieve invloed hebben op het beveiligingsniveau. Een voorbeeld is het aanmaken van een gebruikersaccount met beheerrechten op een kritieke applicatie.
- Afwijkingen van de technische configuratiestandaarden (baselines). Denk hierbij bijvoorbeeld aan een incorrect wachtwoordbeleid op een server.
- Kwetsbaarheden binnen de IT-middelen. Bijvoorbeeld het toestaan van onveilige communicatie naar een server.

Kort gezegd maakt een SIEM-voorziening gebruik van bestaande logging- en monitoringfaciliteiten. Zij combineert deze informatie tot relevante informatie en rapporteert hierover. Deze rapportages kunnen zowel betrekking hebben op de beveiligingsstatus van IT-middelen als op beveiligingsgerelateerde activiteiten. Enkele veelvoorkomende voorbeelden van het gebruik van SIEM zijn:

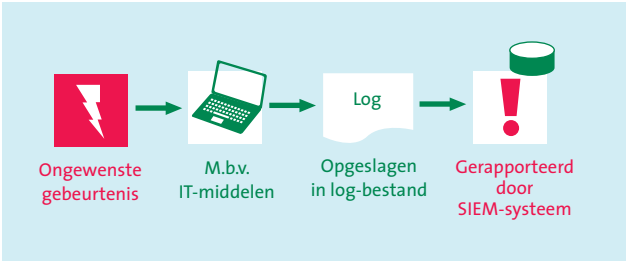
- het geautomatiseerd monitoren van systemen, applicaties en/of databaselogging met de mogelijkheid in een vroeg stadium misbruik van systemen te detecteren en hierover te rapporteren;
- het geautomatiseerd monitoren van systemen, applicaties en/of databaselogging met als doel continu inzicht te hebben in de staat van de 'compliance' met interne of externe vereisten;
- het ondersteunen in het onderzoek naar een incident door loginformatie uit het verleden te analyseren en de verschillende gebeurtenissen op de verschillende systemen (grafisch) weer te geven.

Deze definitie en voorbeelden zijn nog steeds vrij breed, vandaar wellicht ook dat SIEM inmiddels een paraplubegrip is geworden. Het is daarom nuttig om aan te geven wat wij *niet* verstaan onder SIEM:

- Een Service Level Management-voorziening. Er zijn producten op de markt die bijvoorbeeld de beschikbaarheid en prestaties van IT-middelen bewaken. Deze gegevens worden vervolgens gebruikt om aan te tonen dat (al dan niet) aan (klant-) afspraken is voldaan. SIEM-systemen kunnen hier wel een bijdrage aan leveren, maar richten zich meer op de activiteiten die op deze IT-middelen worden uitgevoerd.
- Een gecentraliseerde opslagfaciliteit van logbestanden. Sommige producten bieden de functionaliteit logbestanden beveiligd op te slaan. Het doel hiervan is om bij beveiligingsincidenten achteraf te kunnen vaststellen wat er is gebeurd. Een SIEM-voorziening bewaakt het IT-landschap continu en vrijwel realtime. Zij beperkt zich niet tot analyse nadat beveiligingsincidenten of fraude in volle omvang aan het licht zijn gekomen.
- Een voorziening die volledige beveiliging geeft, of de werking van alle andere beveiligingsproducten overneemt. De effectiviteit van een SIEM-voorziening zal juist mede afhangen van de logbestanden van de andere beveiligingsproducten.

Hoewel SIEM-voorzieningen soms worden ingezet om te valideren of systemen kwetsbaar zijn voor bepaalde aanvallen door hackers, gaan we hier in dit artikel niet op in.

Een SIEM-voorziening maakt waar mogelijk gebruik van bestaande logging- en monitoringfaciliteiten



Figuur 1. **Schematische weergave van het gewenste procesverloop bij beveiligingsincidenten.**

Er zijn diverse grote spelers op de markt die SIEM-voorzieningen aanbieden. Vaak wordt een complete oplossing in één suite aangeboden. In een aantal gevallen wordt echter onderscheid gemaakt tussen Security Event Management (SEM) en Security Information Management (SIM). Een SEM-voorziening richt zich op het 'real-time' monitoren en managen van beveiligingsgebeurtenissen. SIM-voorzieningen richten zich op het opslaan van loginformatie en het gebruik van deze informatie voor het genereren van compliancerapporten.

Grote spelers op de SIEM-markt zijn onder andere ([Gart10]):
- *ArcSight:* ArcSight – onlangs overgenomen door HP – biedt één van de meest complete SIEM-voorzieningen.
- *RSA Envision:* RSA Envision wordt geleverd door EMC en biedt een volledige SIEM-voorziening.
- *QRadar SIEM:* QRadar SIEM wordt geleverd door Q1 labs en biedt een volledige SIEM-voorziening.
- *Symantec Security Information Manager (SSIM):* wordt geleverd door Symantec en biedt een volledige SIEM-voorziening.
- *LogLogic:* LogLogic levert losstaande SEM- en SIM-producten die samen een volledige SIEM-voorziening vormen.

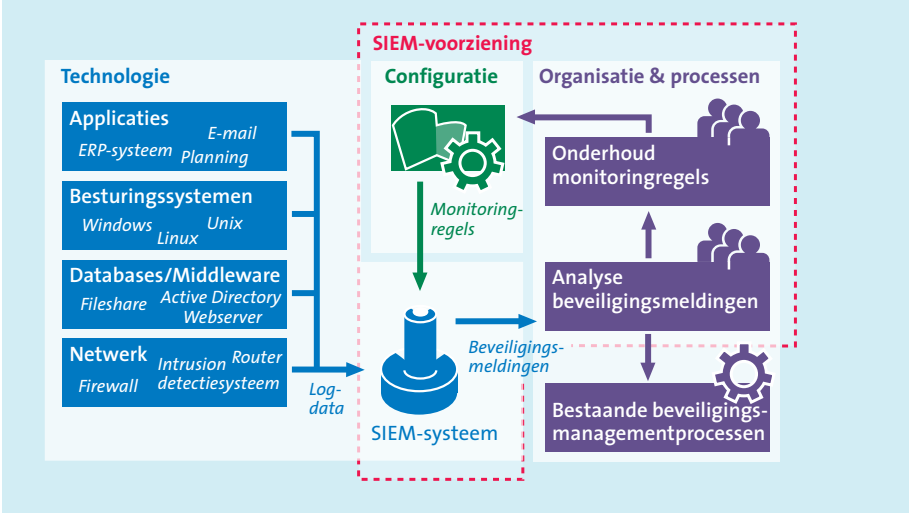
SIEM: het bereiken van 'tijdig inzicht' over het gehele IT-landschap

Hoe kan een SIEM-voorziening helpen de wensen over 'tijdig inzicht' in te vullen? De kracht van een SIEM-voorziening zit er met name in dat zij organisaties in staat stelt loginformatie uit het gehele IT-landschap te verzamelen en te analyseren op beveiligingsgebeurtenissen, configuratieafwijkingen en kwetsbaarheden. Dit levert een totaalbeeld op van de beveiligingsstatus van het IT-landschap.

Het IT-landschap kan grofweg worden onderverdeeld in vier verschillende lagen:
- *applicaties*, bijvoorbeeld ERP-programma's zoals SAP;
- *besturingssystemen*, bijvoorbeeld Windows-, Linux- en Unix-varianten;
- *middleware en databases*, bijvoorbeeld webservers, Oracle en MS SQL;
- *netwerk*, bijvoorbeeld firewalls en intrusion detection systemen.

Op elk van de vier lagen kan onderscheid worden gemaakt tussen ongewenste gebeurtenissen, afwijkingen van configuratiestandaarden en kwetsbaarheden.

De grote hoeveelheid loginformatie waarmee de SIEM-voorziening wordt gevoed, vertegenwoordigt niet alleen relevante beveiligingsgebeurtenissen. Een groot deel van de gelogde activiteiten bestaat uit toegestane gebeurtenissen of gebeurtenissen die opzichzelfstaand geen incident vertegenwoordigen. Een typisch voorbeeld is het vastleggen van foutieve inlogpogingen. Wanneer de foutieve inlogpoging zich slechts eenmaal voordoet is dit geen incident. Wanneer binnen korte tijd tien of meer foutieve inlogpogingen van dezelfde gebruiker zijn gedetecteerd, is er mogelijk wel sprake van een incident (wellicht probeert een onbevoegd persoon het wachtwoord te raden). In het hiervoor genoemde voorbeeld zal de SIEM-voorziening slechts één melding weergeven; tien foutieve inlogpogingen door gebruiker 'x' op systeem 'y'. Dit samenvoegen van vergelijkbare gebeurtenissen tot één gebeurtenis wordt *aggregeren* genoemd.



Figuur 2. **Positionering van de SIEM-voorziening binnen een applicatielandschap.**

Het zojuist beschreven voorbeeld gaat nog steeds uit van loginformatie van één bronsysteem. De ware kracht van een SIEM-voorziening zit in het combineren van loginformatie uit verschillende bronsystemen. Stel dat tijdens

Organisatierisico	Mogelijke monitoringregel	Betrokken IT-laag
De privacy van patiënten wordt geschaad waardoor patiënten het vertrouwen in de organisatie kunnen verliezen en de organisatie boetes kunnen worden opgelegd.	Genereer een melding bij vijf of meer foutieve inlogpogingen op een systeem met medische informatie vanuit hetzelfde gebruikers-ID binnen 15 minuten.	• *Besturingssystemen*: logs van foutieve inlogpogingen op het besturingssysteem waar de medische data zijn opgeslagen (bijv. fileshare of het besturingssysteem waarop de database draait). • *Databases en middleware*: logs van foutieve inlogpogingen op de database waarin de medische data zijn opgeslagen. • *Applicatie*: logs van foutieve inlogpogingen op de (web)applicatie die toegang geeft tot de medische data.
Er wordt fraude gepleegd met financiële transacties waardoor de organisatie financiële schade lijdt.	Genereer een melding wanneer een financiële transactie wordt uitgevoerd op een vreemd tijdstip ('s nachts of in het weekeinde) en vanuit een locatie zonder financiële afdeling met een waarde boven de €100.000.	• *Applicatie*: logs van financiële transacties binnen het financiële systeem, bijvoorbeeld een ERP-pakket.
Gevoelige autorisaties worden ten onrechte toegekend waardoor mogelijk een ongeautoriseerd persoon toegang krijgt tot gevoelige informatie of ongeautoriseerde systeemwijzigingen kan doorvoeren.	Genereer een melding wanneer beheerrechten worden toegewezen aan een account.	• *Alle lagen*: logs met toekenningen van autorisaties.
Belangrijke bedrijfsinformatie wordt verwijderd waardoor gebruikers hun werk (tijdelijk) niet goed meer kunnen uitvoeren.	Genereer een melding wanneer binnen 10 minuten tien of meer bestanden van een server worden verwijderd.	• *Besturingssysteem*: logs van verwijderen van bestanden op (file) servers. • *Applicatie*: logs van verwijderen van bestanden in een documentmanagementsysteem.
Een ongeautoriseerd persoon krijgt toegang tot gevoelige informatie of kan deze zelfs wijzigen.	Genereer een melding wanneer het Intrusie Detectie Systeem (IDS) een serie van verdachte gebeurtenissen op de Active Directory server detecteert, gevolgd door een succesvolle inlogpoging vanuit dezelfde locatie.	• *Netwerk*: logs met meldingen van het IDS. • *Databases en middleware*: logs van succesvolle inlogpogingen op de Active Directory server.
Belangrijke IT-systemen worden platgelegd waardoor er (tijdelijk) niet gewerkt kan worden.	Genereer een melding zodra op een dag op meer dan dertig systemen (afhankelijk van de organisatiegrootte) hetzelfde virus is gedetecteerd.	• *Applicatie*: logs van virusmeldingen die gerapporteerd zijn door de antivirusinstallaties aan de antivirusmanagementapplicatie.

Tabel 1. **Overzicht met enkele mogelijke organisatierisico's en hoe SIEM deze helpt te beperken.**

een scan een kwetsbaarheid is gevonden op de e-mailserver (beveiligingsmelding 1), dat een IDS een bekende aanval detecteert op de e-mailserver (beveiligingsmelding 2) en dat daarna e-mails van diverse accounts worden doorgestuurd (beveiligingsmelding 3). De drie verschillende beveiligingsmeldingen zijn afkomstig uit verschillende systemen, maar zijn allemaal gerelateerd aan een succesvolle aanval. Het combineren van voornoemde beveiligingsinformatie afkomstig uit loginformatie van verschillende bronsystemen wordt *correleren* genoemd.

Tabel 1 geeft een overzicht van organisatierisico's met daarbij een mogelijke monitoringregel die dit risico kan beperken. Daarnaast zijn de IT-lagen opgenomen die informatie moeten aanleveren aan de SIEM-voorziening om een juiste analyse te kunnen maken. De monitoringregels kunnen gericht zijn op één laag of systeem uit het IT-landschap, maar ook op een combinatie van lagen en systemen.

Voorgaande beschrijving en tabel tonen al aan dat een SIEM-voorziening de loginformatie uit verschillende bronsystemen analyseert en filtert. Een goede filtering bevordert dat er weinig irrelevante meldingen (valse positieven) zijn, wat een te grote werklast zou betekenen voor de analisten van de SIEM-voorziening. Tegelijkertijd wil men ook geen relevante beveiligingsmeldingen ('valse negatieven') missen.

Het voorbeeld in het kader illustreert hoe een monitoringsysteem gericht op een specifieke component uit het IT-landschap, gebruikt kan worden binnen een SIEM-implementatie.

Een SIEM-voorziening verschaft organisaties meer inzicht in de risico's van het steeds complexer wordende IT-landschap, maar een volwaardige SIEM-voorziening kan meer. SIEM-voorzieningen stellen organisaties in staat op elk gewenst moment analyses uit te voeren op de grote hoeveelheid verza-

Het monitoren van databases binnen de 'middleware en database'-laag

Veel applicaties slaan hun gegevens op in databases. Het is daarom niet vreemd dat tot 92 procent van de gelekte data afkomstig is van databases ([Veri10]).

Aangezien databases veel gebruikt worden binnen organisaties, is het (handmatig) monitoren van elke individuele database lastig en tijdrovend. Om deze uitdaging te verhelpen zijn er databasemonitoringsystemen op de markt. Deze systemen bieden SIEM-functionaliteit, maar dan specifiek voor databases. Databasemonitoringsystemen stellen organisaties in staat centraal log- en monitoringregels vast te stellen die voor alle gekoppelde databases gelden.

Om deze centrale log- en monitoringregels te kunnen valideren, zal een koppeling moeten worden gemaakt met elke database. Dit is mogelijk door het installeren van een softwarekoppeling en het aanmaken van een account op de databaseserver. Het databasemonitoringsysteem controleert aan de hand van de ingestelde regels op onjuiste configuraties en op activiteiten die mogelijk ongeautoriseerd zijn.

Bij koppeling met een SIEM-voorziening kan ervoor gekozen worden alle informatie uit het databasemonitoringsysteem beschikbaar te stellen aan de SIEM-voorziening, of slechts een relevant deel daarvan. Voor beide mogelijkheden zijn valide argumenten te geven. Wanneer alle databaseinformatie doorgestuurd wordt naar de SIEM-voorziening, dan wordt deze mogelijk overbelast. Mogelijke gevolgen zijn traagheid en ontoereikende opslagruimte.

Wanneer slechts het relevante deel naar een SIEM-voorziening wordt gevoerd, worden mogelijk relevante gebeurtenissen gemist. Immers, wanneer de SIEM-voorziening bepaalde data niet ontvangt, kan zij deze ook niet analyseren en correleren. Het is daarom van belang om tijdens het ontwerp en de inrichting van de SIEM-voorziening een informatieanalyse uit te voeren, die ingaat op dit soort aspecten. Dit voorkomt het achteraf moeten doorvoeren van (kostbare) wijzigingen.

melde loginformatie. De meeste SIEM-voorzieningen hebben standaardrapportages gedefinieerd die voldoen aan de informatievereisten vanuit SOx of PCI DSS. Deze informatie stelt de organisatie en de auditor in staat zich niet alleen een tijdiger, maar ook een volledige beeld te vormen van de compliancestatus van het IT-landschap van de organisatie.

Welke leerervaringen kennen we uit de praktijk?

De recente geschiedenis leert dat IT-implementatietrajecten een vrij hoge faalkans kennen ([Else08]). SIEM-implementaties kennen een sterke technische component: een SIEM-voorziening moet immers gekoppeld worden aan een diversiteit van systemen. Toch is de technische component niet de grootste uitdaging voor een succesvolle implementatie. Waarop moeten bedrijven dan anticiperen om tot succesvolle SIEM-implementatie te komen?

Vijf belangrijke succesfactoren voor een SIEM-implementatie zijn 'focus', 'analyseprocessen voor beveiligingsmeldingen', 'organisatie', 'fasering' en 'onderhoud'.

Hieronder gaan we in op deze succesfactoren.

Focus

Alle beschikbare loginformatie voor analyse naar de SIEM-voorziening sturen, kan verleidelijk zijn. Echter, dit stelt niet alleen hoge eisen aan het systeem, ook is de kans groot dat dit een enorme hoeveelheid beveiligingsmeldingen oplevert. Deze hoeveelheid beveiligingsmeldingen kan de analisten overspoelen. Als gevolg daarvan onderzoeken de analisten mogelijk willekeurige meldingen in plaats van alleen de belangrijke meldingen. Het is daarom essentieel om focus aan te brengen. Het gebruik van onderstaande doelen kan helpen focus aan te brengen in de gewenste informatie:

- *Compliance*. Welke informatie wil de organisatie inzichtelijk hebben om aantoonbaar te voldoen aan de interne compliancevereisten, maar ook aan de extern opgelegde compliancevereisten vanuit bijvoorbeeld SOx, PCI DSS (voor creditcardgegevens) of HIPAA (voor medische gegevens)?
- *Risicobeheer*. In welke beveiligingsinformatie is de organisatie geïnteresseerd om zowel interne als externe dreigingen en fraude te identificeren? Enkele voorbeelden zijn het saboteren van systemen, het lekken van (gevoelige) informatie, een Denial of Service-aanval of het aanmaken van nieuwe gebruikers met gevoelige autorisaties.
- *Netwerkbeheer*. Monitoring van de beschikbaarheid en belasting van kritieke systemen ter voorkoming van een beschikbaarheidsincident.

Naast het in kaart brengen van de gewenste informatie, dient bepaald te worden welke systemen te monitoren. Een aanpak die vaak goed werkt is om eerst te bepalen welke gebeurtenissen het hoogste organisatierisico opleveren (bijvoorbeeld de top 20 van organisatierisico's). Vervolgens kan bepaald worden welke systemen hier een rol in spelen. Dit zijn systemen met een hoog risicoprofiel, waardoor het nuttig is om deze systemen aan te

sluiten op de SIEM-voorziening. Zo kan de SIEM-voorziening het risicoprofiel van een organisatie concreet helpen verlagen.

Ook compliancevereisten kunnen de focus bepalen. Bij een dergelijke focus ligt de nadruk op de bewaking van systemen die vanuit wet- en regelgeving speciale aandacht vragen. Zo is PCI DSS-compliance-informatie alleen relevant voor systemen die creditcardgegevens verwerken en zijn SOx-vereisten alleen relevant voor systemen die belangrijk zijn voor de jaarrekeningcontrole.

Analyse van de beveiligingsmeldingen

Een SIEM-voorziening kent een sterke procescomponent. Dit betreft met name de analyse en afhandeling van beveiligingsmeldingen. Voor de introductie van een SIEM-product zullen deze processen vormgegeven moeten worden. Veelal vereisen de diverse typen beveiligingsmeldingen verschillende afhandelprocessen. De analyse en vervolgstappen bij een serie ongeautoriseerde handelingen zullen anders zijn dan bij een foutieve configuratie. Voor elk van de processen dient te worden bepaald wie verantwoordelijk is voor de verschillende (sub)stappen. Als onderdeel hiervan dient een escalatieprocedure te worden ingericht. Het vaststellen van verantwoordelijkheden en escalatieprocedures is extra belangrijk wanneer derde partijen ook IT-diensten leveren.

Veel organisaties die een SIEM-voorziening implementeren, stappen over van een meer reactieve manier van reageren op beveiligings- of compliance-incidenten naar de proactieve vorm. Deze overstap kan bijvoorbeeld ingegeven zijn door auditbevindingen of recente beveiligingsmeldingen. De kans is dan groot dat er niet alleen nieuwe processen moeten worden opgesteld voor het analyseren van beveiligingsincidenten, maar dat ook huidige incidentmanagementprocessen moeten worden aangepast. De proactieve aanpak van SIEM zal immers meer input voor de bestaande IT-beheerprocessen genereren, aangezien op basis van de beveiligingsmeldingen corrigerende maatregelen getroffen zullen worden.

Organisatie

Gerelateerd aan de voorgaande stap is een derde belangrijk aspect het vormgeven van een opvolgingsteam dat de beveiligingsmeldingen zal gaan verwerken. Binnen veel grotere organisaties is al een afdeling rondom beveiliging ingericht. Mogelijk kan het opvolgingsteam binnen deze afdeling worden ingepast. Dit heeft als voordeel dat weinig wijzigingen noodzakelijk zijn op organisatorisch vlak.

Vaak blijkt dat deze afdeling rondom beveiliging meer met beleid en controle bezig is dan met operationaliteit. Deze afdeling zal daardoor geen beveiligingsmeldingen van de SIEM-voorziening onderzoeken. Dit wetende kunnen verschillende oplossingsrichtingen worden gekozen.

Ten eerste kan worden gekozen voor een compact intern opvolgingsteam, of een wat uitgebreidere inrichting in de vorm van een Security Operations Centre (SOC), een extern opvolgingsteam. Daarnaast kan gebruik worden gemaakt van een SOC van een grote IT-dienstverlener waarvan al een dienst wordt afgenomen. Door voor deze weg te kiezen kan op de kosten bespaard worden en daarnaast zijn vaak verschillende soorten serviceniveaus mogelijk waarmee beter afgestemd kan worden op de specifieke behoeften. Nadeel is het risico van belangenverstrengeling wanneer beveiligingsmeldingen worden veroorzaakt door de IT-dienstverlener zelf. Een derde mogelijkheid is daarom om een onafhankelijke externe leverancier in te huren. Nadeel hiervan is dat vertrouwelijke gegevens zullen worden verstuurd aan een extra externe partij. Hierover zullen dus aanvullende afspraken moeten worden gemaakt en op de naleving hiervan zal moeten worden toegezien.

Belangrijke randvoorwaarde is in ieder geval dat goede contractuele afspraken worden gemaakt. Hierin moeten in ieder geval afspraken worden gemaakt over beschikbaarheid, reactiesnelheid (ook buiten kantooruren), de rapportagelijnen, het mandaat en hoe de mankracht het meest adequaat ingezet kan worden.

De introductie van een SIEM-voorziening zal meer beveiligingsmeldingen opleveren die allemaal moeten worden geanalyseerd en waarvan een groot deel opvolging vereist. De implementatie van een SIEM-voorziening zal dus ook invloed hebben op bestaande IT-afdelingen binnen de organisatie.

De diverse typen beveiligingsmeldingen vereisen veelal verschillende afhandelprocessen

Fasering

Zoals hierboven geschetst, kennen SIEM-implementatietrajecten een sterke IT-component, maar ook een sterke organisatie- en procescomponent. Dit maakt dergelijke trajecten tot een interessante uitdaging. Een goede manier om hiermee om te gaan is het opstellen van een gefaseerd implementatieplan.

Aandachtspunten bij deze fasering zijn om op relatief korte termijn de toegevoegde waarde van SIEM aan te kunnen tonen, terwijl het traject tegelijkertijd beheersbaar blijft. Een goede

aanpak maakt gebruik van de vastgestelde focus. De implementatie kan beginnen met een beperkt aantal doelsystemen en activiteiten die een groot deel van het risicoprofiel van een organisatie vormen. Deze aanpak omvat de organisatie, techniek en processen. Hierdoor worden op deze vlakken parallel verbeteringen doorgevoerd en is de toegevoegde waarde van de SIEM-voorziening snel zichtbaar.

Het is goed om tijdens de implementatie rekening te houden met bekende valkuilen. Zo zal geen enkele SIEM-voorziening exact alle regels kunnen configureren waar een organisatie behoefte aan heeft. Dit heeft te maken met zowel technische beperkingen als het ontbreken van logginginformatie op het juiste detailniveau. Daarnaast zullen veel (risicovolle) handelingen op het IT-landschap zijn toegestaan, maar hoe kan de SIEM-voorziening geautomatiseerd vaststellen of een risicovolle handeling is toegestaan?

De in de SIEM-voorziening geconfigureerde regel zal lang niet altijd de doelstelling van deze regel geheel afdekken. Dit kan zowel valse positieve meldingen opleveren, als valse negatieve meldingen. Een valse positieve melding krijg je als een regel te soepel is gedefinieerd. De SIEM-voorziening genereert daardoor meer meldingen dan nodig is. Die meldingen moeten in principe allemaal onderzocht worden. Een valse negatieve melding is een melding die ten onrechte niet wordt gegenereerd omdat een regel te strak is gedefinieerd.

Het is zaak het aantal meldingen te stabiliseren tot een acceptabel niveau alvorens de functionaliteit uit te breiden of nieuwe systemen aan te sluiten. Dit voorkomt dat de organisatie overstelpt wordt met beveiligingsmeldingen. Aan de andere kant voorkomt deze aanpak het bieden van schijnveiligheid.

Onderhoud

De wereld is continu in beweging en daarmee verandert het risicoprofiel waarmee organisaties te maken hebben. Tevens kan de risicotolerantie van organisaties veranderen. Daarom is het van belang periodiek te evalueren of de SIEM-voorziening aanpassing behoeft. Tijdens de evaluatie kan aan bod komen of:

- de organisatierisico's zijn veranderd;
- de doelstelling van de SIEM-voorziening moet veranderen (bijvoorbeeld aanvullende aandacht voor beveiligingsincidenten ten opzichte van compliance);
- de relatie tussen de doelstelling en de bewaakte IT-middelen juist is;
- de diepgang van de bewaking juist is;
- de bewaakte systemen zijn aangepast, vervangen of worden uitgefaseerd en daarmee of de aggregatie en correlatie van logging nog adequaat verloopt;
- de beveiligingsmeldingen en rapportages nog voldoen aan de doelstellingen en wensen;
- aan de organisatie- of proceskant wijzigingen moeten worden doorgevoerd om te waarborgen dat aan de kwaliteitseisen die van toepassing zijn op de SIEM-voorziening voldaan wordt;
- de bescherming van het SIEM-product zelf nog adequaat is, zodat hierin geen beveiligingslekken ontstaan. Dit betreft zowel het doorvoeren van patches als het controleren of de logische toegangsbeveiliging adequaat is ingericht.

Deze periodieke evaluatie waarborgt dat de effectiviteit van de SIEM-voorziening niet wegebt in de loop der tijd.

Conclusie

De ontwikkelingen rondom beveiligingsoplossingen zoals SIEM gaan in rap tempo. Dit is mede ingegeven door een sterke managementbehoefte aan een tijdig inzicht in het risicoprofiel van het IT-landschap en aan snelheid van handelen bij incidenten. Hierdoor kunnen SIEM-systemen zich verheugen in een toenemende aandacht van organisaties. Interessant hierbij is dat SIEM-voorzieningen in grote mate kunnen worden aangepast naar de focus die een organisatie heeft. Dit kan resulteren in kleinschalige SIEM-voorzieningen, maar ook in SIEM-voorzieningen die hun nut bewijzen als onderdeel van brede beveiligingsprogramma's.

Echter, het implementeren van een SIEM-voorziening is niet eenvoudig. Dit is mede te verklaren doordat een dergelijke voorziening raakt aan de organisatie, beveiligingsprocessen, IT-beheerprocessen en natuurlijk aan techniek. Dit vraagt om een gebalanceerde en weloverwogen implementatieaanpak. Het is daarom van belang om de leerervaringen uit de praktijk in acht te nemen. Dit stelt organisaties in staat SIEM-voorzieningen goed in te passen in hun initiatieven ten aanzien van risicobeheer en de krachtige mogelijkheden van SIEM volledig te benutten.

Referenties

[Else08] Elsevier, 'Geen Rolls-Royces meer', 13 september 2008.

[Gart10] Gartner, *Magic Quadrant for Security Information and Event Management*, May 2010.

[KPMG10] KPMG, *Data Loss Barometer*, november 2010, http://www.datalossbarometer.com.

[McAf11] McAfee Foundstone Professional Services and McAfee Labs, *Global Energy Cyberattacks: Night Dragon*, 10 February 2011.

[Veri10] Verizon Risk Team in cooperation with the United States Secret Service, *2010 Data Breach Investigations Report*, 2010.