DE VALKUILEN VAN SECURITY MONITORING

Dr. ir. Tom Kleiberg is security consultant bij Pinewood.
Tom is te bereiken via Tom.Kleiberg@pinewood.nl en http://nl.linkedin.com/in/tjkleiberg

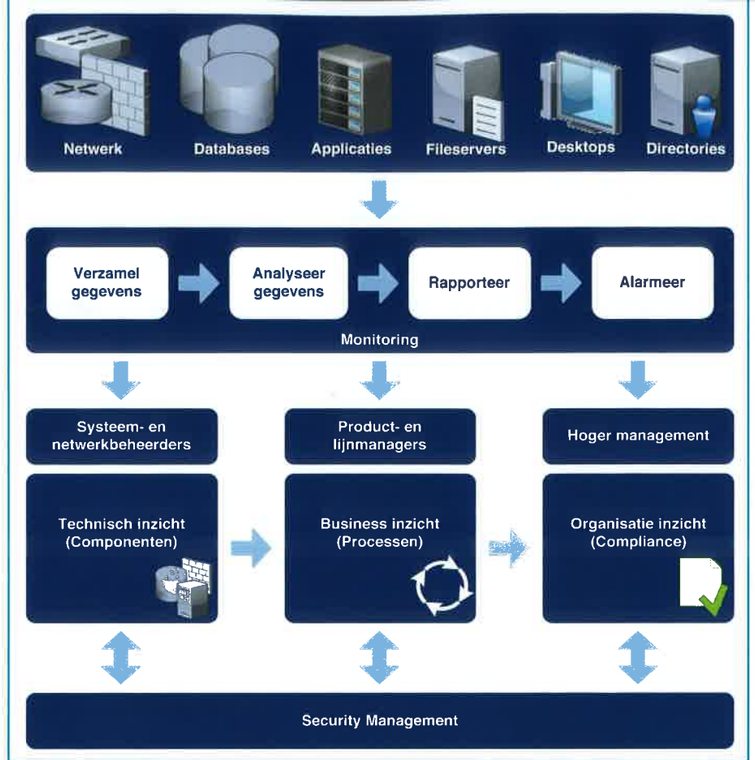
Security monitoring is een belangrijke maatregel met als voornaamste doel tijdig en adequaat te kunnen acteren op bijzondere of afwijkende gebeurtenissen. Security monitoring gaat verder dan systeembewaking of compliance monitoring. Waar compliance monitoring vooral (automatisch) toeziet op naleving van wet- en regelgeving door controle op de *aanwezigheid* van maatregelen, bewaakt security monitoring continu de informatieveiligheid door óók de correcte *werking* en *effectiviteit* van maatregelen inzichtelijk te maken. Security monitoring biedt actueel inzicht in de gedragingen in de ICT-infrastructuur en door betekenis te geven aan bepaalde ICT-gebeurtenissen kan alert en adequaat gereageerd worden op afwijkende en risicovolle situaties.

De belangrijkste aanleiding voor veel organisaties om te starten met security monitoring is gelegen in compliance. Standaarden en baselines als PCI-DSS en Baseline Informatiebeveiliging Rijksdienst (BIR) schrijven voor dat security monitoring wordt toegepast binnen de organisatie en zodoende wordt vaak ijverig gestart met aanschaf van tooling, gevolgd door implementatie. In de praktijk blijkt echter dat de weg naar een succesvolle implementatie en aanwending is behept met vele valkuilen. De toegevoegde waarde van security monitoring wordt vaak niet bereikt of zelfs gezien door organisaties. Want afgezien van de vaak forse financiële investeringen, blijkt regelmatig dat organisaties die wel security monitoring geïmplementeerd hebben, na een "succesvol" implementatietraject stuiten op een teleurstellende opvolging. De inzet van security monitoring moet daarom zeer goed doordacht worden vóór aanschaf van tooling en de betrokkenheid van de organisatie is daarbij onontbeerlijk. Dit artikel gaat in op de voornaamste valkuilen en misverstanden.

Valkuil 1 - ICT als promotor
Organisaties die security monitoring vanuit een compliance behoefte initiëren, behandelen dit vaak als een technisch vraagstuk. Hierdoor belandt de projectuitvoering en opvolging bijna automatisch bij ICT. ICT heeft ogenschijnlijk het grootste belang bij security en krijgt als zodanig de rol van promotor naar zich toegeschoven. Hierdoor ontstaat de perceptie dat security monitoring vooral ICT-processen ondersteunt en geen directe toegevoegde waarde heeft voor de business. De betrokkenheid van de business is daardoor niet vanzelfsprekend. Security monitoring is echter *juist* een business tool en ondersteunt deze door risico's, ten gevolge van ICT-gedragingen, inzichtelijk te krijgen en dus beheersbaar te maken. ICT is verantwoordelijk voor de operationele staat van systemen, maar kan de *business value* van de informatie op deze systemen niet inschatten. De business is nodig om aan te geven welke informatie belangrijk is en hoe deze informatie geïnterpreteerd moet worden. Het is daarom essentieel de business vroegtijdig te betrekken bij het project en ze bekend te maken met de mogelijkheden van security monitoring (tools). Zorg dat de doelstellingen van security monitoring aansluiten bij de business doelstellingen en laat tijdens het project bijvoorbeeld regelmatig wat rapportages zien. Zo leert de business de mogelijkheden kennen van security monitoring, inclusief de uitgebreide toepassingen ervan. Dit leidt tot een verbeterde acceptatie en inzet van security monitoring en verhoogt de toegevoegde waarde.

Valkuil 2 - Technisch beheer wordt te laat aangehaakt bij de implementatie
Security monitoring bestaat uit het verzamelen en analyseren van (veel!) informatie. Afstemming over welke informatiesystemen moeten aanleveren en in welke vorm is essentieel. De medewerking van beheerders is hierbij onmisbaar. Zij weten welke configuratie-onderdelen belangrijk zijn, wat het formaat is van de logs en welke betekenis gegeven moet worden aan verschillende ICT-gebeurtenissen. Beheerders zitten echter lang niet altijd te wachten op dergelijke implementaties. Hun primaire taak is ervoor te zorgen dat "hun kindje" in de lucht blijft, er geen verstoringen optreden, etc. Zodra er sprake is van installatie van een agent, er aanpassingen nodig zijn op het systeem of extra koppelingen aangelegd moeten worden, ontstaat er vaak weerstand. Neem deze weerstand weg door beheerders ervan te overtuigen dat deze tools ook voor hen waardevol zijn. Laat zien hoe deze tools hun werk gemakkelijker kunnen maken doordat ze bepaalde taken uit handen nemen. Voorkom hiermee ook dat beheerders zich gecontroleerd voelen, omdat een security monitoring tool hun "fouten" kan detecteren. Dergelijke tools helpen de beheerder juist verder en dragen bij aan het kwaliteitsproces.

Valkuil 3 - Processen voor gebruik en onderhoud van de tools worden pas na oplevering ingericht
Doordat security monitoring tools zijn gekoppeld aan veel informatiebronnen, vereisen ze veel onderhoud en worden ze onvermijdelijk onderdeel van diverse (ICT) processen. Regelmatig kom je tegen dat vergeten wordt nieuwe systemen toe te voegen aan de security monitoring tool of dat bijwerken van een bewaakt systeem leidt tot een onleesbaar logformaat, met als gevolg dat deze bron wegvalt. Voorkom deze problemen door vooraf processen



Security monitoring in een schematische weergave

in te richten voor het beheer van de security monitoring tools en beoordeel de impact op bestaande ICT-processen. Wacht dus niet met het inrichten en wijzigen van deze processen totdat het ICT-implementatietraject is afgerond, maar zorg ervoor dat er voldoende aandacht is voor de periode erna.

Valkuil 4 - Er is niet nagedacht over een security organisatie die past bij de security monitoring
Security monitoring resulteert bijna automatisch in meer meldingen over je ICT-omgeving. Deze meldingen zullen afgehandeld moeten worden en dit verlangt een verandering in de organisatie. Adequaat en alert reageren op afwijkend ICT-gedrag vereist in de eerste plaats dat specialistische kennis aanwezig is voor de analyse van de verzamelde gegevens op relevante afwijkingen. Daarnaast is het van belang dat de juiste rollen, taken en verantwoordelijkheden belegd zijn binnen de organisatie. Op het moment dat een calamiteit zich voordoet, moeten deze bekend zijn, zodat men niet ten tijde van de calamiteit nog moet uitvinden waar de verantwoordelijkheden liggen. Bedenk vooraf welke personen betrokken moeten worden bij het afhandelen van de meldingen en welke informatie nodig is in geval van een calamiteit. Zorg ervoor dat in situaties waar op basis van 24x7 gealarmeerd moet worden, de organisatie dit kan ondersteunen.

Valkuil 5 - Tot aan het vinkje… En niet verder
Leveranciers van security monitoring tools spelen handig in op compliance vraagstukken door voorgeprogrammeerde sets aan te leveren voor het bewaken van de compliance status. Hierdoor wordt de indruk nog verder versterkt dat men na de implementatie achterover kan leunen en de tool zijn werk kan laten doen. Men is compliant en hoeft zich vervolgens voor een jaar geen zorgen meer te maken. Tot de volgende audit… Wat de auditor dan vaak aantreft is een security monitoring tool die nauwelijks nog is afgestemd op de werkelijke situatie. De ICT-omgeving is dermate veranderd dat niet langer (de juiste) informatie wordt verzameld. Daardoor mist men veel loginformatie van de afgelopen periode en kan de auditor niet beoordelen of zich geen bijzonderheden hebben voorgedaan in de voorbije periode. Bovendien ligt er voor de

ICT-organisatie weer een hoop werk klaar om ervoor te zorgen dat de omgeving weer correct gemonitord wordt. Dit brengt vaak veel extra kosten met zich mee. In enkele gevallen leidt het er zelfs toe dat het monitoringsysteem opnieuw dient te worden geconfigureerd en men feitelijk weer vanaf nul moet beginnen. Bedenk dus dat ook voor compliance toepassingen het noodzakelijk is beheer in te richten. De voorgeprogrammeerde sets zijn vooral een hulpmiddel, de werkelijke kracht komt nog steeds uit de organisatie zelf.

Valkuil 6 - Gebrek aan resources
Tot slot is de tijd die de ICT-organisatie heeft voor security monitoring een probleem. Regelmatig wordt de uitvoering van ICT-projecten ondergebracht bij beheer. Zij zijn echter al overbelast met beheerwerkzaamheden en kunnen onvoldoende tijd vrijmaken voor zo'n ingrijpend project (waarvan ze zelf ook niet altijd het belang zien). De prioriteiten moeten van bovenaf duidelijk worden gemaakt en bij "bovenaf" moet dus ook duidelijk zijn dat de implementatie gedragen moet worden door de organisatie. Er moeten (aanzienlijke) resources vrijgemaakt worden bij beheer, zowel tijdens als na de implementatie. Duidelijke communicatie over hun rol hierin is daarom onontbeerlijk. Zorg ervoor dat voldoende projectbudget wordt ingeruimd tijdens de implementatie en houd hierbij rekening met de complexiteit van deze projecten. Bedenk eveneens dat na oplevering er extra taken komen te liggen bij beheer. Houd dus ook hier rekening met extra resources om zo te komen tot een succesvol project!

Samenvattend kan worden gezegd dat betrokkenheid van de business bij security monitoring van vitaal belang is. Niet alleen tijdens het voortraject, maar ook na oplevering blijft betrokkenheid essentieel. Maak hierbij wel een realistische inschatting van de inzet en benodigde resources, zodat aan de verwachtingen kan worden voldaan. Dit verhoogt de kans van slagen van security monitoring projecten aanzienlijk en draagt bij aan een succesvolle opvolging! ●