/// Security Information & Event Management (SIEM)

1 INTRODUCTIE

Als lokaal bestuur doet u er vanzelfsprekend alles aan om cybercriminelen buiten te houden door de nodige beveiligingsmaatregelen in acht te nemen. Maar wat gebeurt er wanneer cybercriminelen proberen in te breken in uw beveiligingsmaatregelen? Of proberen toegang te krijgen tot uw systemen en data? Wordt u hiervan op de hoogte gehouden? Of ontdekt u het enkel als het te laat is?

Om deze geschetste situaties te voorkomen bestaan er Security Information & Event Management oplossingen (SIEM). Deze oplossingen monitoren en analyseren uw cyberlandschap en gaan op zoek naar bewijs van potentiële datalekken of vijandige infiltraties.
Ze geven u als lokaal bestuur vroegtijdig signalen wanneer er cybercriminelen actief zijn rondom of binnen uw netwerken.

Security Information & Event Management (SIEM) geeft beveiligingsteams een centrale plek om grote hoeveelheden gegevens uit een hele organisatie te verzamelen, te aggregeren en te analyseren om beveiligingswerkstromen effectief te stroomlijnen. Security Information & Event Management (SIEM) biedt ook operationele mogelijkheden zoals compliancerapportage, incidentbeheer en dashboards die bedreigingsactiviteit prioriteren. Concreet geeft een Security Information & Event Management (SIEM)-oplossing lokale besturen zicht op de cyberactiviteiten binnen hun netwerk met een transparante en integere organisatie als resultaat.

Om een succesvol beheer te implementeren is het ook belangrijk het toezicht van dit beheer toe te wijzen aan één beleidsmedewerker. Deze persoon heeft de verantwoordelijkheid en bevoegdheid om de toepassing en naleving van het beleid op te volgen en eventuele inbreuken te rapporteren.

2 WET- EN REGELGEVING

Er bestaat geen specifieke bindende nationale of Europese regelgeving rondom Security Information & Event Management (SIEM). Lokale besturen moeten wel rekening houden met de Algemene Verordering Gegevensbescherming (AVG) of GDPR (General Data Protection Regulation)[1]. Deze regelgeving schrijft voor dat alle bedrijven, overheidsdiensten, organisaties en instellingen die in Europa persoonsgegevens verwerken, gebruiken, registreren of bewaren, moeten voldoen aan bepaalde richtlijnen. Deze richtlijnen stellen dat gegevens volgens een voldoende veiligheidsniveau moeten worden verwerkt binnen een organisatie. Met andere woorden, om te voldoen aan de AVG wordt er verwacht dat potentiële data lekken of vijandige

infiltraties gesignaleerd en opgelost worden. Om dit resultaat te krijgen zijn er Security Information & Event Management (SIEM)-oplossingen.

3 BELEID

Organisatorische maatregelen

Organisatorische maatregelen verwijzen naar het hebben van duidelijke processen, procedures en verantwoordelijkheden met betrekking tot Security Information & Event Management (SIEM). Vanuit een organisatorisch perspectief is het belangrijk om vastgestelde criteria en standaarden te definiëren waaraan de Security Information & Event Management (SIEM)-analyses moeten voldoen. Bijkomend is het belangrijk om de juistheid en actualiteit van het organisatorisch beleid te monitoren, rapporteren en op te volgen.

Technische maatregelen

Technische maatregelen verwijzen naar het hebben van documentatie waarin de werking, voorwaarden, verantwoordelijkheden en onderhoud met betrekking tot de verschillende Security Information & Event Management (SIEM)-taken en -procedures beschreven staan. Vanuit een technisch perspectief is het belangrijk om logmanagement, security event correlation en security alerts te definiëren en deze op een professionele manier in te organiseren. Logmanagement omschrijft voorwaarden met betrekking tot het centraal verzamelen en standaardiseren van gebeurtenissen op verschillende netwerken. Security event correlation omschrijft voorwaarden met betrekking tot het maken van (ingewikkelde) relaties tussen gebeurtenislogs. Security alerts verwijst naar voorwaarden met betrekking tot het managen van verschillende communicatiekanalen om IT-medewerkers te alarmeren in het geval van detectie van mogelijke dreigingen.

Mensgerichte maatregelen

Security Information & Event Management (SIEM) is behoorlijk technisch en de procedures en processen worden hoofdzakelijk uitgevoerd door IT-medewerkers. Buiten dat het belangrijk is om voldoende kennistrainingen voor IT-medewerkers te organiseren en Security Information & Event Management (SIEM) gebruiks- en onderhoudsvriendelijk te houden, is het ook belangrijk om de bevindingen van Security Information & Event Management (SIEM) op een toegankelijke manier te presenteren. Zorg er dus voor dat uw Security Information & Event Management (SIEM)-oplossing beveiligingsinformatie weergeeft via afbeeldingen of gemakkelijk te lezen dashboards. Hierdoor zien niet alleen gespecialiseerde medewerkers de beveiligingsinformatie, maar kan de informatie ook duidelijk aan het management gepresenteerd worden.

4 AANBEVELINGEN

Organisatorische maatregelen

- Zorg ervoor dat de verantwoordelijkheden rond het implementeren en onderhouden van Security Information & Event Management (SIEM)-processen en -procedures goed gedefinieerd en bekend zijn.

- Zorg voor de aanwezigheid van duidelijke gedefinieerde criteria, standaarden en rapporterings-templates waarin de voorwaarden van de werking van Security Information & Event Management (SIEM)-oplossingen omschreven staan.
- Definieer Security Information & Event Management (SIEM)-KPI's en monitor en review deze op geplande tijdstippen.
- Organiseer regelmatig een audit die uw Security Information & Event Management (SIEM)-beleid controleert en evalueert
- Optimaliseer op basis van de auditresultaten

Technische maatregelen

- Gebruik een Security Information & Event Management (SIEM)-oplossing voor het uitvoeren en assisteren van technische taken zoals logmanagement, security event correlation en security alerts.
- Zorg ervoor dat processen, procedures en verantwoordelijkheden rond het verzamelen en standaardiseren van gebeurtenissen (logs) beschreven staan.
- Zorg ervoor dat de processen, procedures en verantwoordelijkheden rond het analyseren van loggegevens beschreven staan.
- Zorg ervoor dat de processen, procedures en verantwoordelijkheden rond het communiceren van mogelijke bedreigingen beschreven staan.
- Gebruik verschillende communicatiekanalen (dashboardupdate, e-mailwaarschuwing, sms-waarschuwing) om IT-medewerkers in te lichten over mogelijke bedreigingen.

Mensgerichte maatregelen

- Presenteer Security Information & Event Management (SIEM)-bevindingen op een behapbare manier.
- Organiseer voldoende kennistrainingen voor IT-medewerkers.
- Zorg voor een gebruiks- en onderhoudsvriendelijk configuratiebeheer.

5 VERKLARENDE WOORDENLIJST

Term	Verduidelijking	Link naar meer informatie
Logmanagement	Logmanagement verwijst naar het managen van gebeurtenissen op hardware en software van een organisatie.	https://www.nist.gov/publications/guide-computer-security-log-management
Security event correlation	Security event correlation verwijst naar het gebruik maken van geavanceerde analyses om datapatronen te identificeren en te begrijpen.	Event Correlation - Glossary | CSRC (nist.gov)

REFERENTIES

- Veiligheidslogging en monitoring (SIEM) Minimale Maatregelen Digitaal Vlaanderen: Vo_Informatieclassificatie_-_Minimale_maatregelen_-_SIEM_bcglh8.pdf (vlaanderen.be)