DE VOLGENDE FASE VAN SIEM: SITUATION AWARE SECURITY OPERATION CENTER

DE CONVERGENTIESLAG

De bekende security industrieanalist en visionair Steve Hunt schreef er in 2005 al over, convergentie tussen SIEM en PSIM. In de visie van Steve Hunt levert integratie van SIEM met PSIM veel efficiency voordelen op. Immers incidenten en events kunnen grotendeels door hetzelfde proces worden afgehandeld. Er ontstaat vanuit één centraalpunt een overzicht over alle ICT en non-ICT security incidenten [1].

Door het continue monitoren en analyseren van systemen en logging kan men veel proactiever handelen op mogelijke security issues. Geheel volgens de visie van Steve Hunt introduceerden technologie providers zoals NICE [2] en Proximex [3] (onderdeel van TYCO security) in 2011 de eerste commercieel verkrijgbare SIEM/PSIM oplossingen gedreven vanuit de NERC-CIP regelgeving.

In november 2013 startte de Europese Unie het project Situation AWare Security Operation Center (SAWSOC) [4]. Doel van het SAWSOC is vaststellen en implementeren van technieken die nodig zijn voor de convergentie tussen physical en cybersecurity. SAWSOC is een samenwerkingsproject tussen een aantal onderzoeksinstellingen, universiteiten en IT bedrijven uit Ierland, Engeland, Israël, Finland, Duitsland en Polen. Dit project wordt gesponsord door de Europese Commissie vanuit het FP7-SECURITY Programma (SEC-2012.2.5-1 Convergence of physical and cybersecurity – Capability Project). De gedachte achter SAWSOC is dat door de holistische benadering en verbeterde technieken bewuster en betrouwbare (d.w.z. juist, tijdig en betrouwbaar) detectie en analyse van aanvallen kan plaatsvinden. Dit dient uiteindelijk te leiden tot het verwezenlijken van de twee grote belangrijke doelstellingen van SAWSOC.

1. **De belofte voor bescherming/beveiliging van burgers en goederen**
2. **Het verbeteren van de perceptie van veiligheid door burgers**

Het totale SAWSOC-project duurt 30 maanden en kent een budget van ongeveer 5 miljoen euro, waarvan 3,4 miljoen wordt bijgedragen door Europese commissie. Het project kent 11 partners uit 7 landen. Het project SAWSOC dient in mei 2016 een platform op te leveren op basis waarvan systemen kunnen worden ontworpen en wat echte convergentie van physical en cyber security technologieën bewerkstelligd en wat verdere versnippering voorkomt.

Wasdom

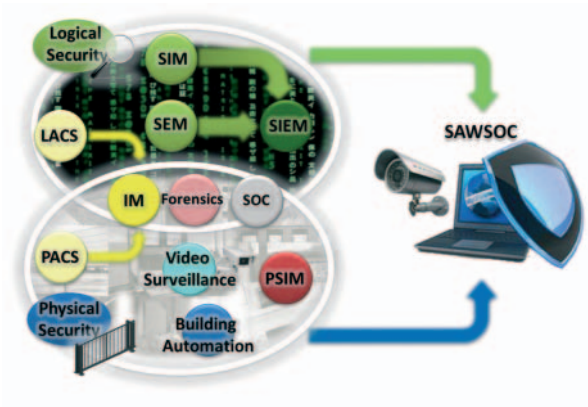
Willen we echt wat kunnen met SAWSOC dan is het van belang dat de drie belangrijkste elementen in SAWSOC tot wasdom komen. De belangrijkste elementen binnen SAWSOC zijn:

1. **Security Information & Event Monitoring (SIEM)**
2. **Physical Security Information Management (PSIM)**
3. **Identity Management (IM)**

Security Information & Event Monitoring (SIEM) is binnen de ICT security ondertussen een geworteld begrip. Een SIEM geeft grip en inzicht in alle mogelijke netwerkbeveiliging risico's en bedreigingen. SIEM maakt het geautomatiseerd monitoren en controleren van het beveiligingsbeleid van een organisatie mogelijk. Een SIEM doet dit door real-time informatie te verzamelen uit logfiles van netwerk- componenten, tools, security-componenten, servers, laptops, desktops, applicaties en databases en deze vervolgens te correleren en te analyseren en te presenteren en om security threats te detecteren. Een belangrijk aspect hierbij is de correlatie, waarbij verbanden tussen logs gezocht worden. Hierdoor geeft een SIEM een overzichtelijk beeld van de actuele status van de ICT security. Wat een

Ronald Eygendaal. Ronald is freelance verslaggever en tijdschriftschrijver. Hij schrijft sinds 1999 in de vakbladen over informatiebeveiliging, elektronische & technisch beveiliging, fraude detectie & bestrijding en bewaking & beveiliging in het bijzonder. Hij is bestuurslid bij de Vereniging Beveiligingsprofessionals Nederland (VBN).

SIEM doet in de ICT security wereld, doet een PSIM (Physical Security Information Management) voor de physical security wereld.



Een PSIM is een software platform dat verschillende losse (beveiliging)systemen integreert die beheert worden via een uitgebreide meestal grafische gebruikersinterface. Hierdoor kan men dagelijkse operationele handelingen, incident management en crisisbeheersing op een duidelijke, gestructureerde en controleerbare wijze uitvoeren. Zo worden camerasystemen, toegangscontrole, inbraakdetectie en ander soortgelijke systemen samengebracht in PSIM. In de basis hebben een SIEM en een PSIM een vijftal identieke hoofdfuncties, te weten:

1. Collection - via onafhankelijke device management software kan het systeem gegevens verzamelen van een willekeurig aantal uiteenlopende beveiligingssystemen en apparaten.
2. Analyse - het systeem kan gecollecteerde informatie zoals data, gebeurtenissen, alarmen en andere belangrijke gegevens, analyseren en correleren.
3. Verificatie - de gegevens uit de analysefase worden gefilterd, geïdentificeerd en geperiodiseerd op zodanige wijze dat ze inzichtelijk worden voor de security operators
4. Resolutie (incident response) - het systeem voorziet in een unieke set van standaard operationele procedures (SOP's) welke afgeleid zijn van beleid en best practices afspraken van de organisatie. Door deze stap-voor-stap instructies zijn security operators in staat de gebeurtenissen af te handelen in het geval van een noodsituatie.
5. Rapportage - het systeem verzamelt niet alleen informatie aan het begin, maar regisseert ook alle informatie en overzicht van genomen acties en maatregelen. Dit kan achteraf worden gebruikt voor rapportage doeleinden.

In SAWSOC komen SIEM en PSIM echt samen.

Identity Management

Voor de convergentie tussen SIEM en een PSIM is het hebben van één identiteit in zowel de physical en cyberwereld noodzakelijk. Immer hoe kan je anders relatie leggen tussen de virtuele en fysieke persoon. Sinds 2009 is er een trend gaande om Logical Access Control Systems (LACS) en Physical Access Control Systems (PACS) samen te voegen tot Identity Management. Convergentie naar één identiteit brengt onder meer authenticatie naar een hoger model.

Zo kun je naast de drie klassieke authenticatie-elementen (wat je weet, wat je hebt, wie je bent) nu ook een vierde element namelijk 'waar je bent', in het authenticatieproces worden gebruikt. Een ander groot voordeel van convergentie naar één identiteit is kostenreductie. Geïsoleerde oplossingen bieden onvoldoende garantie: gaten in proces van uitgifte en inname van rechten kunnen gemakkelijk ontstaan. Door convergentie tussen de physical en cybersecurity werelden kunnen de processen rond rechtenbeheer worden vereenvoudigd en verbeterd en worden kosten bespaard. Kortweg betekent convergentie meer veiligheid tegen minder kosten.

Conclusie

SAWSOC zal een geavanceerde Security Operations Center (SOC) platform opleveren. Hierdoor kunnen accurate, tijdige en betrouwbare detectie en diagnose van aanvallen worden ondersteund. Daarnaast kan met correlerende gebeurtenissen uit een breed scala van fysieke en logische beveiligingsbronnen een verbeterde situational awareness worden ontwikkeld.

Echter, in de dagelijkse praktijk zien we nog een stringente scheiding tussen de physical en cyber domeinen. Zo worden PSIM systemen geleverd door de elektrotechnische beveiligingsinstallateurs en SIEM wordt veelal geleverd voor de IT security bedrijven. Bedrijven die in beide werelden succesvol actief zijn, kan men op één hand tellen en succesvolle samenwerkingen tussen deze bedrijven zijn gering. Gezien de huidige legacy, de vervangingscyclus (10 jaar) en de wet en regelgeving ten aanzien van fysieke beveiliging zal het zeker nog een aantal jaren duren voordat convergentie tussen PSIM en SIEM zal plaatsvinden. Ook de benodigde convergentie naar één identiteit kent nog de nodige obstakels. Ook bij deze convergentie is de stringente scheiding tussen de domeinen één van de grootste obstakels. Dit wordt nog verstrekt doordat we qua organisatorische bedrijfsindelingen vaak de twee domeinen nog gescheiden houden. Zo is veelal facilities verantwoordelijk voor physical Security en IT voor ICT security. Pas als al deze hobbels genomen zijn kan SAWSOC tot wasdom komen.

Tenslotte, binnen het SAWSOC project ontbreken de grote leveranciers uit zowel de PSIM en SIEM securitywereld, vraag blijft daarom: gaat SAWSOC echt zorgen voor de volgende fase van SIEM? Of verbranden we 3,4 miljoen Europees geld voor niets?

Links:

[1] http://www.surveillance-magazine.com/2014/01/05/the-converging-roles-of-physical-and-it-security-and-the-rise-of-psim
[2] http://www.nice.com/news/newsletter/more2.php?page_id=467&edition=11_9s
[3] http://www.securitysquared.com/2010/03/psim-and-siem-proximex-arcsight.html
[4] http://www.sawsoc.eu/