Intégration de la PSIM et de la SIEM dans le Situation AWare Security Operation Center

La bataille de la convergence

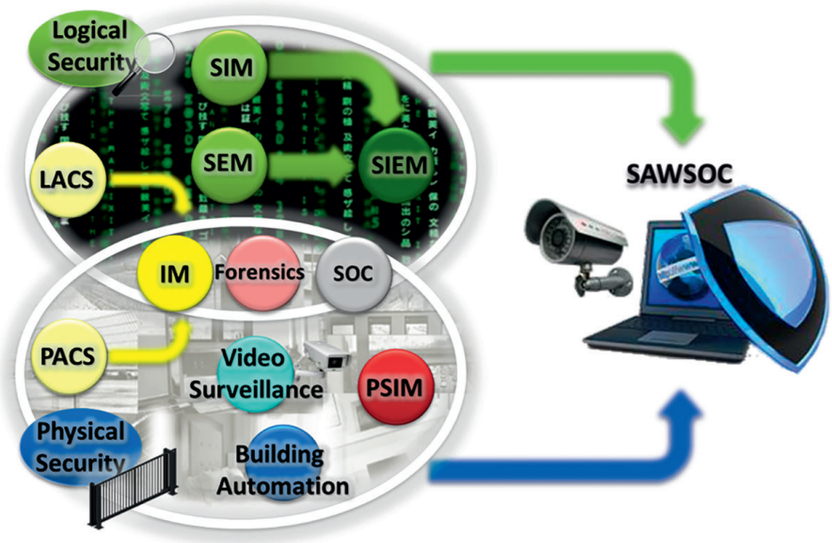
Le célèbre analyste et visionnaire de l'industrie de la sécurité, Steve Hunt, écrivait déjà à ce sujet en 2005 : Convergence entre la SIEM et la PSIM. Selon Steve Hunt, l'intégration de la SIEM et de la PSIM offre de nombreux avantages sur le plan de l'efficacité. Les incidents et les événements peuvent, en effet, être en grande partie traités selon le même processus. On obtient ainsi, d'un même point de vue central, un aperçu de tous les incidents de sécurité, qu'ils concernent l'informatique ou non. En matière de surveillance et d'analyse constante des systèmes et identifiants, on peut ainsi agir plus anticipativement sur les éventuels problèmes de sécurité. Les fournisseurs de technologie tels que NICE et Proximex (filiale de TYCO security) ont suivi, en 2011, avec les premières solutions SIEM/PSIM commercialisées, issues de la réglementation NERC-CIP.

Novembre 2013 a vu le démarrage du projet Situation AWare Security Operation Center (SAWSOC). Son objectif était de déterminer et mettre en œuvre les techniques nécessaires à la convergence entre sécurité physique et sécurité informatique. SAWSOC est un projet de collaboration entre un certain nombre d'instituts de recherche et d'entreprises informatiques d'Irlande, d'Angleterre, d'Israël, de Finlande, d'Allemagne et de Pologne. Ce projet est parrainé par la Commission européenne sur la base du FP7-SECURITY Program (SEC-2012.2.5-1 Convergence of physical and cyber security – Capability Project). L'idée derrière SAWSOC est qu'en raison de l'approche holistique et de l'amélioration des techniques, il est possible de réaliser une détection et une analyse délibérées et fiables des attaques. Ceci devrait conduire, en fin de compte, à la réalisation des deux grands objectifs importants de SAWSOC: protection/sécurisation des personnes et des biens, et amélioration de la perception de la sécurité par les citoyens. Le projet SAWSOC s'étale sur 30 mois et dispose d'un budget d'environ 5 millions d'euros, dont 3,4 millions sont apportés par la Commission européenne. Le projet regroupe 11 partenaires issus de 7 pays. Il doit aboutir, en mai 2016, à une plate-forme à partir de laquelle pourront être conçus des systèmes, mettant ainsi en œuvre une vraie convergence des technologies de sécurité physique et informatique, et prévenant un éparpillement ultérieur.

> **« La convergence signifie plus de sécurité pour un coût moindre.**

Éléments clés

Pour que le projet réussisse, il importe de développer les trois éléments les plus importants de SAWSOC : Security Information & Event Monitoring (SIEM), Physical Security Information Management (PSIM) et Identity Management (IM). La notion de « Security Information & Event Monitoring (SIEM) » s'est entre-temps imposée en termes de sécurité informatique (ICT security). La SIEM (Gestion des événements du système d'information) permet de comprendre et d'agir sur les protections du réseau ainsi que sur tous les risques et menaces possibles concernant ce dernier. La SIEM permet de réaliser la surveillance et le contrôle automatisés de la politique de sécurité d'une organisation. Pour ce faire, la SIEM collecte les informations en temps réel à partir du suivi au fil de l'eau (« logs ») des composants du réseau, des outils, des composants de sécurité, des serveurs, des ordinateurs portables ou fixes, des applications et des bases de données, pour ensuite les corréler, les analyser, et les présenter de manière à détecter les menaces pour la sécurité. L'un des aspects importants, en



la matière, est la corrélation, qui permet d'établir des liens entre « logs ».
La SIEM peut donner ainsi une image synoptique de l'état actuel de la sécurité informatique. Ce que fait la SIEM sur le plan de la sécurité informatique, la PSIM (Physical Security Information Management) le fait sur celui de la sécurité physique. Une PSIM (Gestion de l'information sur la sécurité physique) est une plate-forme logicielle intégrant différents systèmes (de sécurité), gérés au moyen d'une interface utilisateur exhaustive, souvent graphique. Elle permet d'exécuter de façon claire, structurée et contrôlable, les opérations quotidiennes, ainsi que la gestion des incidents et des crises. {La PSIM intègre ainsi les systèmes de vidéosurveillance, de contrôle d'accès, d'alarme intrusion et autres systèmes analogues. La SIEM et la PSIM possèdent quelque cinq fonctions principales en commun:

- Collecte : le système a la possibilité, via un logiciel indépendant de gestion d'appareils, de collecter les données d'un nombre quelconque d'appareils et de systèmes de sécurité divers.
- Analyse : le système peut ensuite analyser et corréler les informations collectées, telles que des données, des événements, des alarmes et autres données importantes.
- Vérification : les données issues de la phase d'analyse sont alors filtrées, identifiées, réparties en périodes, de façon à pouvoir être exploitées par les opérateurs de sécurité.
- Résolution (réponse aux incidents) : le système comporte une série unique de procédures opérationnelles standard ou SOP, dérivées de la politique et des pratiques d'excellence de l'organisation. Grâce à ces instructions pas-à-pas, les opérateurs de sécurité sont en mesure de traiter les événements en cas d'urgence.
- Établissement de rapports : le système collecte non seulement des informations au départ, mais gère aussi toutes les informations et établit une synthèse des actions menées et des mesures prises. Elles peuvent être utilisées par la suite à des fins d'établissement de rapports.

Dans SAWSOC, la SIEM et la PSIM sont vraiment intégrées.

Gestion des identités

Pour pouvoir réaliser la convergence entre la SIEM et la PSIM, il est indispensable de disposer d'une même identité tant dans le monde physique qu'informatique. Comment établir sinon une relation entre la personne virtuelle et la personne physique ? Depuis 2009, il existe une tendance au regroupement sous une seule Gestion d'identité (Identity Management), des Logical Access Control Systems (LACS) et des Physical Access Control Systems (PACS). La convergence vers une même identité entraîne en même temps une authentification d'un modèle supérieur. Outre les trois éléments classiques d'authentification (ce que l'on sait, ce que l'on a, ce que l'on est), il est à présent possible d'adjoindre au processus d'authentification un quatrième élément, à savoir « où l'on est ».

> **« Étant donné la situation actuelle, le cycle de remplacement (10 ans) ainsi que les lois et réglementations concernant la sécurité physique, il se passera certainement encore quelques années avant que la convergence entre PSIM et SIEM se fasse.**

Autre gros avantage de la convergence vers une seule identité, la réduction des coûts. Les solutions isolées offrent une garantie insuffisante : Il peut y avoir facilement des trous dans le processus d'attribution et d'acceptation des droits. La convergence entre les univers physique et cybernétique de la sécurité est susceptible de simplifier et d'améliorer les processus de gestion des droits et d'économiser des frais. En résumé, la convergence signifie plus de sécurité pour un coût moindre.

Conclusion

Le projet SAWSOC aboutira à une plate-forme avancée, le Centre opérationnel de la Sécurité, ou Security Operations Center (SOC). Ce dernier permettra une détection et un diagnostic précis, fiables et anticipatifs, des attaques. De plus, la corrélation d'événements issus d'un grand nombre de sources de sécurité physiques et logiques, permet une prise de conscience améliorée

de la situation. Toutefois, dans la pratique courante, on constate encore une séparation très nette entre les domaines physique et informatique. Ainsi, les systèmes de PSIM sont fournis par les installateurs électrotechniciens de la sécurité, et la SIEM est le plus souvent fournie par les entreprises de sécurité informatique. Les sociétés travaillant avec succès dans les deux secteurs, se comptent sur les doigts de la main, et les collaborations réussies entre ces entreprises sont limitées. Étant donné la situation actuelle, le cycle de remplacement (10 ans) ainsi que les lois et réglementations concernant la sécurité physique, il se passera certainement encore quelques années avant que la convergence entre PSIM et SIEM se fasse. La convergence nécessaire vers une seule identité connaît également des obstacles inévitables. Pour cette convergence aussi, la séparation très nette entre les domaines est l'un des plus grands obstacles. Ceci est encore renforcé par le fait que les deux domaines sont souvent maintenus séparés sur le plan de l'organisation de l'entreprise. Ainsi, les Services généraux sont souvent responsables de la sécurité physique et le Service informatique, de la sécurité informatique. Ce n'est qu'une fois ces obstacles surmontés que SAWSOC pourra atteindre son plein développement. Pour conclure, il manque au projet SAWSOC, les gros fournisseurs, tant du domaine de la PSIM que de la SIEM. La question se pose donc : SAWSOC assurera-t-il vraiment le passage à la phase suivante de SIEM ? Ou dépenserons-nous 3,4 millions d'euros de subventions européennes pour rien?

(Par Ronald Eygendaal)

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