ICS Cybervision sécurise les réseaux industriels

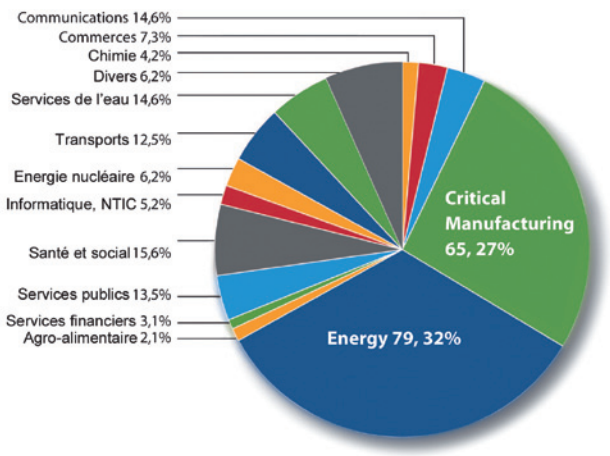
Depuis que les systèmes de commande industriels sont la cible d'attaques informatiques, les entreprises doivent apprendre à se protéger de cette nouvelle forme de cybercriminalité. La start-up française Sentryo propose à cette fin, une solution alliant matériels, logiciels et veille technologique.

L'Internet industriel couvre les réseaux machine-to-machine et tous les systèmes qui interagissent avec le monde réel au point que l'on parle aujourd'hui de système cyber-physique (cyber physical systems). Il regroupe les systèmes de contrôle-commande (ICS / SCADA), s'étend à l'Internet Industriel des objets (IIoT) et constituera le système nerveux de l'Industrie du Futur.

Les systèmes de contrôle industriels sont aujourd'hui ouverts et intégrés avec les réseaux de l'entreprise et ils s'appuient de plus en plus sur les standards exploités de longue date par les services informatiques. Partant, ils sont vulnérables aux attaques informatiques. Or, s'ils ont bien été conçus avec un objectif de sûreté fonctionnelle, il n'a pas été prévu que ces systèmes pourraient être la cible de malveillances. En outre, les solutions de cybersécurité exploitées par les services informatiques ne satisfont pas aux contraintes de fonctionnement de ces réseaux.

Depuis quelques années, les incidents de sécurité se sont multipliés et on a vu apparaître des malwares comme Havex, BlackEnergy ou Dragonfly qui ciblent spécifiquement les systèmes de contrôle industriel. Il y a moins d'un an par exemple, le système de contrôle d'une aciérie allemande a été compromis causant la destruction d'un haut fourneau. Les gouvernements, conscients du risque, répondent par de nouvelles réglementations exigeant des exploitants d'infrastructures critiques la mise en œuvre de meilleures pratiques en matière de cybersécurité. De leur côté, les

Incidents de cybersécurité identifiés aux Etats-Unis en 2014 (source ICS-Cert)



industriels poussés par leurs actionnaires cherchent à se protéger de cette menace inédite.

Une mise en observation discrète

C'est précisément pour combler les manques criants dans le domaine de la cybersécurité des systèmes industriels que Thierry Rouquet et Laurent Hausermann ont créé Sentryo en juin 2014. La start-up a mis au point un système de protection appelé, Sentryo ICS CyberVision. Ses principales fonctions consistent à surveiller le réseau, prévenir les risques de compromission et détecter les comportements anormaux. Il s'agit d'une solution entièrement passive, ce qui est une condition préalable à toute installation d'un système de surveillance sur de tels réseaux. De plus, elle permet une étroite collaboration entre automaticiens et experts en informatique ; un facteur de succès en la matière.

Le serveur ICS Cybervision et une sonde passive.

ICS Cybervision se présente sous la forme d'un serveur équipé de son propre système d'exploitation et bien sûr, des logiciels et des applicatifs conçus par l'équipe de Sentryo. La solution se présente en deux parties. On trouve d'une part, des sondes compactes au format Din qui s'installent dans les armoires techniques et qui écoutent de manière passive, les réseaux Modbus, Ethernet/IP, Siemens S7, etc. Ces sondes décodent les données qui transitent et remontent des informations pertinentes vers le serveur qui compose la seconde partie de la solution.

Dès ses premières minutes de fonctionnement, le système recense les équipements connectés et établit une cartographie du réseau, repérant les relations et les interdépendances. Le niveau de détail obtenu à propos des équipements supportés (Schneider Electric, Siemens ou encore, Rockwell Automation), repose sur la capacité de Sentryo à capturer les informations utiles en reconnaissant le protocole de communication. Par exemple, un automate contacté par une station Unity va lui transmettre son identification et des données techniques (version de firmware, etc.). Après quelques heures ou quelques jours, ICS Cybervision dispose d'une cartographie précise et exhaustive qui va servir de référence dès lors que tous les éléments connectés sont en fonctionnement et bien sûr, supportés. Au fil du développement, de nouveaux protocoles seront reconnus comme OPC-UA et BACnet qui viendront s'ajouter courant 2016.

Premier avantage, ICS Cybervision permet de faire de la prévention en fournissant une vision détaillée du réseau industriel. Le système permet par exemple, d'identifier si des patchs de mise à jour ou de sécurité doivent être appliqués et sur quels automates. Il repère aussi les accès déportés restés ouverts alors que le sous-traitant concerné n'a plus de raison d'intervenir. Il permet encore de savoir qu'un équipement nouvellement installé se connecte périodiquement à Internet pour récupérer des mises à jour alors que cela va à l'encontre des règles de sécurité. Bien sûr, il identifie les mots de passe par défaut non changés, recense les serveurs web, ftp ou telnet ouverts, etc.

L'interface utilisateur est facile d'accès et simple d'emploi afin que la solution puisse être utilisée par des personnes qui ne sont pas spécialisées dans la sécurité informatique. Par exemple, les rapports consolident les données dans des fichiers au format PDF ou XLS. Il s'agit d'une caractéristique primordiale puisqu'elle permet aux automaticiens de mieux collaborer avec les équipes IT.

Un référentiel de sécurité

Les premières phases de fonctionnement permettant aussi de qualifier l'état normal de l'installation, il est donc ensuite possible de détecter les anomalies susceptibles de survenir.

Sentryo dispose d'un laboratoire de sécurité technique qui entretient une base de connaissances pour tous les événements globaux relevant de la sécurité informatique industrielle (menaces, vulnérabilités connues des automates, tactiques de hacking, etc.). Les données alimentent une base de sécurité qui va ensuite être diffusée vers les serveurs ICS Cybervision afin d'assurer une surveillance des réseaux industriels en ayant la capacité de détecter les comportements suspects avec une acuité sans cesse remise à jour.

Parmi les autres fonctions assurées, on trouve l'édition d'un journal d'événements classés en fonction de leur gravité. Il peut être exporté au moyen du protocole Syslog pour l'envoyer vers un logiciel de cybersécurité SIEM (Security information event management) qui est fréquemment utilisé dans les grandes entreprises et même, dans les ETI et les PME par l'intermédiaire de prestataires de services. ▮