Cybersécurité : parution du Livre blanc de l'ENISA :
Comment tirer les leçons des incidents de sécurité touchant les systèmes de contrôle industriels/les systèmes SCADA ?

L'Agence européenne de cybersécurité ENISA a publié aujourd'hui un Livre blanc dispensant des recommandations pour la prévention et l'élaboration de réponses flexibles et complètes face aux incidents et aux cyber-attaques contre les Systèmes de contrôle industriels (SCI)/systèmes SCADA. Récemment, la forte augmentation du nombre d'incidents touchant les Systèmes de contrôle industriels (SCI)/systèmes SCADA a soulevé des interrogations quant aux capacités de certains organismes à répondre aux incidents critiques et à les analyser. L'Agence souligne ainsi qu'il est nécessaire de mettre en place un environnement d'apprentissage proactif dans ce domaine.

Les SCI sont très largement utilisés afin de contrôler les processus de fabrication, de production et de distribution des produits industriels. Les logiciels usités à cet effet sont souvent commerciaux et obsolètes. Les systèmes de télésurveillance et acquisition de données, (supervisory control and data acquisition - SCADA), une sous-catégorie des SCI, sont l'un des types de logiciels les plus connus.

Les incidents ayant récemment touché les SCI et les systèmes SCADA révèlent l'importance d'une bonne gouvernance et d'un contrôle efficace des infrastructures SCADA. L'Agence souligne notamment que la **capacité à répondre aux incidents critiques, mais aussi à analyser les conséquences d'une cyber-attaque afin d'en tirer des leçons, est un point crucial**.

Une analyse post-incident permet de comprendre plus en détail l'incident. Celle-ci donne la possibilité de :

- S'appuyer sur des preuves solides pour pouvoir répondre à la nature changeante des menaces domestiques et extérieures ;
- S'assurer qu'une formation suffisamment efficiente est mise en place afin de construire des systèmes résistants.

Afin de créer cet environnement d'apprentissage proactif permettant de répondre aux cyber-attaques et d'effectuer des analyses post-incidents judicieuses, quatre points clés ont été identifiés :

- Renforcer les compétences actuelles grâce à une expertise provenant de l'analyse post-incident et comprendre les chevauchements entre les équipes en charge des incidents critiques cybernétiques et celles en charge des incidents critiques physiques ;
- Faciliter l'intégration des processus de réponse cybernétiques et physiques par une meilleure compréhension de l'origine potentielle des preuves numériques et des moyens appropriés pour les préserver ;
- Programmer et configurer des systèmes permettant de garder en mémoire les preuves numériques ; et
- Encourager les efforts de coopération inter-organisationnels et interétatiques.

Le directeur exécutif de l'ENISA, le Professeur Udo Helmbrecht, a déclaré que : « Les systèmes SCADA sont souvent implantés dans des secteurs faisant partie des infrastructures critiques d'un Etat, comme par exemple les infrastructures de contrôle de la distribution et des transports, les

transformant en cible privilégiée pour de potentielles attaques toujours plus nombreuses et perpétrées par des individus mal intentionnés, des groupes dissidents et même des Etats étrangers. De tels systèmes devraient être examinés de façon à permettre la collecte et l'analyse des preuves numériques et l'identification des causes liées aux failles de sécurité ».

Pour trouver le rapport complet et d'autres recommandations :
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/can-we-learn-from-scada-security-incidents
Pour trouver des informations sur le contexte : http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
Pour toute demande d'interview, veuillez contacter : Ulf Bergström, porte-parole, e-email : press[at]enisa.europa.eu, téléphone portable : +30 6948 460 143, ou l'experte Adrian Pauna, e-mail : resilience[at]enisa.europa.eu

Veuillez noter: traduction. La version anglaise est la seule version officielle
www.enisa.europa.eu/media/enisa-en-francais/
www.enisa.europa.eu