04/12/2013
EPR/17/2013

www.enisa.europa.eu

Atténuer les attaques contre les Systèmes de contrôle industriel (SCI) ; le nouveau guide de l'Agence européenne ENISA

L'Agence européenne de cybersécurité ENISA publie un nouveau manuel proposant des solutions afin d'atténuer au mieux les attaques contre les Systèmes de contrôle industriel (SCI), en soutenant les processus industriels vitaux mis en place en priorité pour les infrastructures d'information critiques (notamment dans les domaines des transports chimiques et de l'énergie) où le manque de connaissances se fait souvent ressentir. Les SCI étant désormais souvent connectées aux plateformes internet, des précautions de sécurité supplémentaires doivent être mises en place. Ce nouveau guide fournit des solutions clés nécessaires aux équipes chargées de développer les Capacités de réponse aux urgences informatiques des SCI (SCI – CERC).

Les **S**ystèmes de **c**ontrôle **i**ndustriel sont indispensables pour un grand nombre de processus industriels, comprenant la redistribution de l'énergie, le traitement de l'eau, les transports, ainsi que les procédés alimentaires, chimiques, gouvernementaux ou encore relatifs à la défense. Les SCI, constitués de groupes criminels, de services de renseignement étrangers, d'hameçonneurs, de « spammers » ou encore de terroristes, sont des cibles lucratives pour les malfaiteurs. Les incidents cybernétiques affectant les SCI peuvent avoir des effets désastreux sur l'économie d'un pays et sur la vie quotidienne de ses citoyens. Ils peuvent entraîner des coupures de courant prolongées, paralyser les transports et causer des catastrophes écologiques. Ainsi, améliorer les capacités de réponse aux incidents touchant les SCI et d'atténuation de leur impact est essentiel pour protéger les infrastructures d'information critiques et pour élever la cybersécurité à un niveau national, européen et mondial. L'ENISA propose donc un guide de bonnes pratiques afin de prévenir les incidents et de préparer les institutions dotées de SCI-CERC et souligne notamment les conclusions suivantes ;

- Alors que les systèmes TIC traditionels privilégiaient l'intégrité des systèmes, les SCI définissent la **disponibilité** comme étant la première priorité (selon les grilles de la « CIA » : Confidentialité, Intégrité, Disponibilité). Cela vient notamment du fait que les SCI sont indispensables pour réaliser des opérations sans solution sur des infrastructures critiques.
- Les principaux acteurs des SCI ne bénéficient pas toujours d'une expertise suffisante dans le domaine de la cybersécurité. De même, les CERT établies ne comprennent pas forcément les aspects techniques spécifiques au secteur concernant les SCI.
- Au vu des dommages significatifs pouvant être potentiellement causés aux SCI, les **procédures de recrutement** des équipes SCI-CERC exigent que le personnel soit inspecté de façon rigoureuse. De nombreux aspects doivent également être pris en compte et les individus doivent par exemple se montrer prêts à accepter de travailler de manière efficace, et ce, malgré la pression et en dehors des horaires de travail.
- L'importance de la coopération aux niveaux national et international doit être mise en avant.

- Les défis exceptionnels touchant les services de cybersécurité des SCI peuvent être relevés en **faisant usage des bonnes pratiques identifiées pour les CERT,** des précédentes expériences mondiales et européennes et d'un **meilleur échange de ces pratiques.**

Le directeur exécutif de l'ENISA, le professeur Udo Helmbrecht, a déclaré : « Jusqu'à il y a quelques décennies, les SCI ont fonctionné dans des environnements très discrets, très isolés, mais elles sont aujourd'hui souvent connectées à Internet. Cela permet de simplifier et d'automatiser les processus industriels, mais augmente par ailleurs les risques d'exposition aux cyberattaques ».
Voir le rapport complet ; https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/ics-cerc/good-practice-guide-for-certs-in-the-area-of-industrial-control-systems/

Contexte : Stratégie de l'UE en matière de cybersécurité. Ce guide se base sur de précédents travaux de l'ENISA dans le domaine des CERT[1]. Ce guide ne désigne pas quelles entités au sein des Etats membres devraient se voir confier les services SCI-CERC.
Pour toute demande d'interview, veuillez consulter Ulf Bergström, porte-parole, ulf.bergstrom@enisa.europa.eu, téléphone portable : + 30 6948 460 143, ou notre experte, Andrea Dufkova, cert-relations [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

[1] *http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities*