Communiqué de presse Codra – février 2020

La Cybersécurité, la clé d'une transformation digitale réussie

Au sein de toutes les entreprises Françaises, une transformation digitale est en marche pour relever les challenges portés par la quatrième révolution industrielle. Secteurs de l'Industrie, de l'Energie ou des Utilités n'échappent pas au phénomène. Pour ces acteurs économiques, un des enjeux est donc de faire évoluer leurs systèmes de production ou d'exploitation (SCADA) d'un mode clôt et isolé à un fonctionnement plus ouvert et interconnecté avec tous les systèmes de l'entreprise. Les objectifs sont variés. Pour certains il s'agit de générer des gains de productivité, compétitivité ou d'apporter un meilleur service à leurs clients. Pour d'autres, améliorer les capacités de production, voire développer de nouveaux services à valeur ajouté.

Le métier de la Supervision vit une véritable révolution

Le métier de la Supervision est en train de vivre une révolution digitale. Traditionnellement, les systèmes SCADA étaient isolés des autres systèmes informatiques. Cet isolement était soit physique, car il s'appuyait généralement sur un réseau informatique dédié, soit géographique (les sites de production étant souvent distants des centres de décision). Les protocoles de communication étaient également très spécifiques, voire propriétaires et très proches des modes de fonctionnement des systèmes de contrôle-commande et d'automatisme.

Or aujourd'hui ce cloisonnement qui pouvait apparaitre comme un premier rempart de protection face à des problématiques « Cyber » est en train de disparaître. Il n'est plus rare de constater que les automates et systèmes communiquant utilisent des protocoles de communication en Ethernet (IP) et s'interfacent avec des systèmes informatiques de gestion d'entreprise : ERP, MES, GMAO, SIG... Cette interconnexion portée par l'émergence des nouvelles technologies, mobiles, objets connectés, Cloud, Big Data… représente un des challenges techniques de la transformation digitale portée par la convergence OT/IT (Informatique Industriel/Entreprise). Fort potentiel de création de valeur, cette convergence présente également une menace pour l'intégrité des systèmes. Les SCADA héritent désormais des nombreuses vulnérabilités issues des systèmes informatiques d'entreprise (IT) qu'il faut désormais traiter. Cela passe à la fois par des règles d'hygiène informatique strictes mais aussi par la mise en service de systèmes SCADA capables intrinsèquement de prendre en compte les enjeux de la Cybersécurité informatique.

Les menaces et enjeux de la Cybersécurité sur les systèmes SCADA

La digitalisation des entreprises est une réalité. Cela passe par le renforcement de la connectivité et de l'interaction des systèmes entre eux. Il est facile de s'imaginer que les enjeux de cybersécurité sont dédiés à quelques fleurons industriels nationaux, mais ce serait une erreur. Selon une étude de Kaspersky*, les vulnérabilités des systèmes d'ICS (Systèmes Industriels de Contrôle) augmentent régulièrement en nombre et en sévérité. Déstabilisation, espionnage, sabotage ou cybercriminalité, les entreprises, qu'elles soient ou non considérées par l'état français comme d'importance vitale (OIV), sont devenues des cibles privilégiées. Toutes se doivent de préserver l'intégrité de leur système d'information afin de maintenir un outil de production fiable et compétitif.

De par son expérience dans des projets de supervision dit « sensibles », Codra a toujours prêté attention à la sécurité informatique. Celle-ci est inscrite dans l'ADN de la société. C'est en 2015 qu'un tournant majeur a été pris en inscrivant la Cybersécurité comme pilier de la stratégie de développement des produits Panorama. C'était donc une évidence pour Codra de travailler en étroite collaboration avec l'ANSSI afin de pouvoir apporter rapidement des solutions concrètes aux enjeux de cybersécurité dans les métiers de la Supervision. *Ce choix stratégique a permis à Panorama E2 de devenir aujourd'hui la première plateforme SCADA à obtenir la Certification de Sécurité de Premier Niveau (CSPN) délivrée par l'ANSSI.*

A quoi sert la certification CSPN ?

En choisissant un produit certifié, une entreprise est assurée que les fonctionnalités offertes disposent d'un niveau de sécurité éprouvé.

La certification répond principalement à 3 objectifs :

- Objectifs **réglementaires** : Répondre aux règlements nationaux ou européens qui imposent l'utilisation de solutions garantissant un niveau de robustesse éprouvé.
- Objectifs **contractuels** : Répondre aux donneurs d'ordres publics ou privés qui exigent que les solutions utilisées aient préalablement obtenu un Visa de sécurité ANSSI.
- Objectifs **commerciaux :** Permettre à un fournisseur de produits ou à un prestataire de services, ainsi qu'aux utilisateurs finaux de ces solutions, de se démarquer de la concurrence par la garantie d'un certain niveau de robustesse.

Utiliser une plateforme certifiée comme support à des applications de supervision dûment implémentées assure donc un niveau de fiabilité éprouvé. L'entreprise qui avance dans une démarche de cybersécurité gagnera un temps précieux lors des phases de tests et de validation de son système de supervision dans le cadre de sa politique de sécurité du ou des systèmes d'information (PSSI).

La Cyber-stratégie de Codra

Dans le cadre du CSPN, des tests de pénétration ont été effectués par un organisme mandaté par l'ANSSI. Les fonctionnalités implémentées permettent de limiter la propagation des attaques et d'assurer une défense en profondeur.

Concrètement, Panorama E2 est doté de mécanismes de cybersécurité permettant aux entreprises d'appliquer aux mieux les bonnes pratiques cyber en termes d'hygiène informatique. Par exemple, identifier les différents rôles utilisateurs et données sensibles à protéger, contrôler l'intégrité et le chiffrement des applications, renforcer la sécurité en matière de communication.
Les menaces étant constantes, des attaques malveillantes peuvent intervenir à tout moment (altération de flux, corruption de configuration, contournement d'identification, etc.). La mise en place d'un PSSI couplé à des mécanismes de cybersécurité éprouvés sont autant d'atouts à la fois pour les opérationnels et les DSI/RSSI qui doivent désormais travailler main dans la main pour assurer un niveau de sécurité optimal.

Afin d'assurer un dialogue constant entre les utilisateurs et les équipes techniques Panorama, Codra a également mis en place un CSIRT produit (Computer Security Incident Response Team). Disponible depuis 2018, il permet de travailler sur le volet prévention notamment avec la publication de bulletins de sécurité et mise à disposition de correctifs de sécurité.

Pour mener à bien cette cyber-stratégie, la certification du produit Panorama fut une étape majeure pour Codra mais pas la seule, ni la dernière ! Ainsi Codra est en route pour la qualification ANSSI. Celle-ci garantit plus largement les compétences et l'engagement de Codra à respecter des critères de confiance approuvés par l'agence nationale.

La Cybersécurité est une course sans fin et chez Codra nous sommes déterminés à ne pas nous laisser distancer. La protection des systèmes SCADA de nos clients étant notre priorité absolue !

Encart aérien :
Cybersécurité dans les transports aérien (source OACI : Organisation Aviation Civile Internationale)
En 2018, 92% des opérateurs aériens avaient ou prévoyaient de mettre en œuvre dans les 3 prochaines années une stratégie de Cybersécurité.

Entre 2017 et 2018, la part du budget pour les technologies de l'information dédiée à la Cybersécurité a augmenté de 2 points, passant de 10 à 12% pour les aéroports, et de 7 à 9% pour les compagnies aériennes selon une étude de la Société internationale de télécommunications aéronautiques (SITA).

Le secteur du transport aérien fait face à des menaces nombreuses et variées :

- Vols de données de passagers,
- Blocage de systèmes opérationnels,
- Modifications des informations,
- Brouillages des communications,
- Prises de commande de logiciels ou d'aéronefs à distance par des acteurs malveillants.
- …

Contact :
Kim CLOUTET
Chargée de Communication Codra
Tel 01 60 92 34 34
k.cloutet@codra.fr