ENSTO

Cybersécurité des IoT connectés

La protection contre les cyber-attaques, au cœur de nos produits et services

Un enjeu mondial, une priorité chez Ensto

Better life.
With electricity.

ensto.com

Cybersécurité des IoT connectés

La protection contre les cyber-attaques, au cœur de nos produits et services

Enjeux

La distribution électrique est nécessaire aujourd'hui pour permettre le fonctionnement des domaines majeurs de notre société.
La disponibilité de l'électricité est donc exigée avec pour certains secteurs, des niveaux très critiques de performances. L'automatisation des ouvrages de distribution connectés, est une des solutions pour satisfaire à ces exigences, permettant de détecter les défauts, les localiser, auto-cicatriser les défaillances, et communiquer à distances sur les bilans de fonctionnement d'un site.

Cependant, les évolutions des technologies informatiques, ont depuis quelques années, fait apparaître les phénomènes de cyber-attaques, qui peuvent instantanément ralentir ou anéantir le fonctionnement normal d'une infrastructure. Il est donc devenu primordial de protéger les installations automatisées de ce type d'agression malveillante.

Risques encourus

L'automatisation d'un système de distribution électrique qui collecte, gère et transfère des données, va augmenter sa surface de vulnérabilité. La corruption du système liée à une faille de cyber sécurité, peut par exemple amener au mauvais fonctionnement d'un capteur, et transmettre des informations erronées.

Outre le fort risque de non électrification d'une zone géographique, ce type de situation peut altérer lourdement le fonctionnement sécurisé des équipements électriques et même dans certains cas, attenter à la vie des personnes.

De même, le ralentissement de calculs, l'effacement de données, peuvent réduire ou suspendre le fonctionnement d'équipements stratégiques et affaiblir une Entreprise ou un Pays.

Solution technique

Ensto, reconnu comme fournisseur dans le domaine de l'automatisation de réseaux Moyenne et Basse Tension (détection de défauts, contrôle commande...), développe désormais des solutions cybersécurisées pour ses équipements connectés. Les compétences mises en oeuvre s'appuient sur des normes de références dans ce domaine (IEC 62 351 et IEC 62 443) ainsi que les bonnes pratiques de conception et de contrôle des logiciels de communication (codage, ...). Particulièrement, l'application de la norme IEC 62 351 est déroulée selon les paragraphes suivants :

- IEC 62 351 - 3 détaillant le chiffrement et les contrôle des données pour les profils TCP/IP (TLS)
- IEC 62 351 - 5 détaillant l'authentification des utilisateurs et l'intégrité de la communication
- IEC 62 351 – 8 détaillant les contrôles d'accès

Le transfert des données de nos équipements vers le système exploitants (SCADA, Système de Management de l'Energie,...) est assuré par l'utilisation d'un "Tunnel VPN" IP Sec.

Par ailleurs, et afin de garantir le maintien en exploitation de ces exigences de cybersécurité, Ensto propose des solutions de mises à jour sécurisée des prestations de services après-vente.

Adaptation de notre organisation

Notre Entreprise a également décidé de s'adapter à l'exigence de sécurité de l'information et va très prochainement solliciter la certification ISO 27001. Ce référentiel permettra notamment de garantir en interne le contrôle des accès, le stockage des données, les échanges de données. Cette certification complètera les garanties apportées à nos clients concernant la protection cyvbersécurisée de nos produits et services.

ENSTO

ensto.com

Ensto Novexia SAS
210, rue Léon Jouhaux - BP 10446
FR - 69656 Villefranche-sur-Saône cedex
Tél : +33 (0)4 74 65 61 61
Fax : +33 (0)4 74 62 96 57
E-mail : infos.novexia@ensto.com