8 EN MATIÈRE DE CYBERSÉCURITÉ,

LES GESTIONNAIRES DE RÉSEAUX ÉLECTRIQUES DOIVENT METTRE EN PLACE DES BONNES PRATIQUES TECHNIQUES ET ORGANISATIONNELLES

Les gestionnaires de réseaux électriques, Opérateurs de Services Essentiels

Les gestionnaires de réseaux électriques sont considérés comme des Opérateurs de Services Essentiels (OSE), c'est-à-dire des opérateurs tributaires des réseaux et systèmes d'information dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie et de la société. Les OSE sont tenus de respecter la directive européenne « *Network and Information Security 2016* » et sa transposition en droit français dont l'application est pilotée par l'Agence Nationale de la Sécurité des Systèmes d'Information ou ANSSI (*arrêté du 14 septembre 2018 fixant les règles de cybersécurité et leurs délais d'application*).

Des spécificités pour la mise en place de mesures de cybersécurité pour les gestionnaires de réseaux de transport et de distribution d'électricité

En plus d'être des OSE, les gestionnaires de réseaux de transport et de distribution d'électricité présentent des spécificités notables pour la mise en place de mesures de cybersécurité :

- **Des systèmes de plus en plus ouverts :** avec l'avènement des réseaux électriques intelligents, les opérations de conduite, de supervision et de maintenance du réseau, nécessitent des échanges importants de données entre les systèmes industriels, auparavant isolés, et les systèmes d'information tertiaires. Ces échanges de données engendrent de nouveaux défis en termes de cybersécurité, à la fois pour des raisons techniques (interfaces entre systèmes hétérogènes complexes) et des raisons organisationnelles (mise en relation d'organisations gérant auparavant séparément les questions de sécurité)
- **De nombreux processus nécessitent d'être effectués en temps réel**, en particulier pour la protection des réseaux électriques. Ces contraintes en temps réel empêchent le déploiement de solutions de cybersécurité trop lourdes (typiquement, cryptage et authentification complexes)
- Enfin, un problème de cybersécurité pour l'un de ces gestionnaires de réseau **risque fort d'entraîner un effet en cascade**,

un événement local pouvant mener à l'écroulement du réseau électrique européen qui est fortement interconnecté.

La nécessaire mise en œuvre de bonnes pratiques

Une bonne cybersécurité des systèmes industriels peut être obtenue en mettant en œuvre les **bonnes pratiques techniques et organisationnelles** suivantes :

- Établir une **connaissance fine de la sécurité informatique du système en fonctionnement** (cartographie du système d'information et de ses interconnections, plan de sauvegarde automatique et de documentation, résultats des analyses de vulnérabilité)
- S'assurer de la **sécurité physique** (accès aux équipements y compris informatiques)
- Maîtriser les **interventions des personnels internes et externes** (formation, habilitation)
- Disposer de **plans actionnables pour le fonctionnement en mode dégradé**, la reprise en cas d'incident et la gestion de crise
- **Prévoir les risques futurs** (par la veille) et **intégrer la cybersécurité dans le cycle de vie complet du système** (des exigences du cahier des charges, à la gestion de l'obsolescence, en passant par la conception du système, son installation, les tests et la gestion des évolutions)

Plus spécifiquement pour les gestionnaires de réseaux de transport et de distribution d'électricité, il convient d'ajouter :

- **Promouvoir l'utilisation de normes de cybersécurité spécifiques** au domaine comme la CEI62351 qui définit la sécurité des protocoles de communication du TC57
- **Être particulièrement vigilant à la ségrégation géographique des systèmes informatiques** afin de garantir la bonne exécution des processus temps réel et de se prémunir contre les effets en cascade
- **Faire réaliser des tests d'intégrité et de sécurité du système** (si possible par des organismes externes de certification)

Pour aller plus loin / références :

1. *La cybersécurité des systèmes industriels, par l'ANSSI*
2. *IEC TC57 WG15: IEC 62351 Security Standards for the Power - System Information Infrastructure*

CONTACTS

Régis HOURDOUILLIE
regis.hourdouillie@yele.fr

Jérémy FLEURY