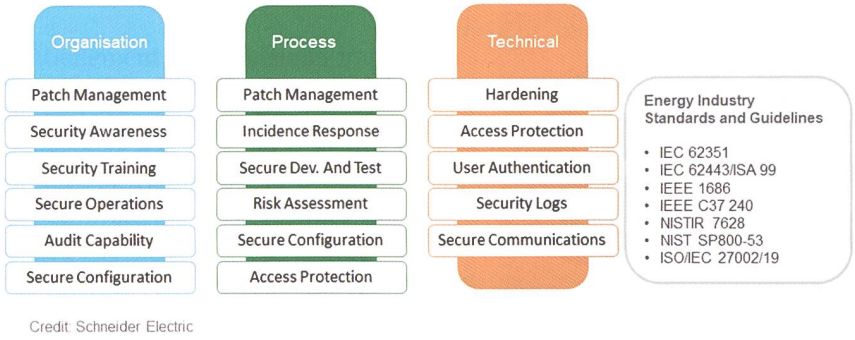
Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2019)
Heft: 1

Artikel: Cybersécurité pour réseaux de distribution électrique modernes
Autor: Giarratano, Didier
DOI: https://doi.org/10.5169/seals-867925



Credit: Schneider Electric

Les trois axes de la cyber sécurité. Toutes les illustrations via l'auteur.
Cet article est paru en langue anglaise dans la revue de l'IEC. Il est reproduit ici avec l'autorisation de son rédacteur en chef.

Protection des infrastructures critiques

Cybersécurité pour réseaux de distribution électrique modernes

Didier Giarratano
Responsable de la plateforme cybersécurité de Schneider Electric

Les réseaux de distribution électrique font partie des infrastructures critiques les plus vulnérables aux cyberattaques.

Défis émergents

Le besoin pressant d'améliorer la disponibilité de l'infrastructure de distribution d'énergie contraint à un changement exigeant un réseau de distribution électrique moderne automatisé. Alors que la demande d'activités numérisées, connectées et intégrées augmente dans tous les secteurs, le défi des services publics est de fournir de manière fiable une énergie reposant sur l'efficacité et la durabilité des sources. Cependant, à mesure que les réseaux de distribution électrique fusionnent et deviennent plus intelligents, les avantages d'une connectivité améliorée entraînent également des risques croissants en matière de cybersécurité, menaçant ainsi de ralentir le progrès. En Europe, les systèmes de distribution électrique ont été conçus à l'origine pour une production centralisée d'énergie et des demandes relativement statiques – et non pas pour gérer des niveaux de consommation ou une complexité en constante évolution. Nous entrons maintenant dans un nouveau modèle énergétique, avec une production plus décentralisée, des sources renouvelables intermittentes (d'origine solaire ou éolienne), un flux d'énergie décarbonisée bidirectionnel et un engagement croissant des consommateurs du côté de la demande.

Modèle décentralisé

Le réseau de distribution électrique est en train de passer à un modèle plus décentralisé offrant davantage de possibilités aux consommateurs et aux entreprises pour intégrer davantage des énergies renouvelables et d'autres sources d'énergie. Par conséquent, les prochaines décennies verront un nouveau type de consommateur d'énergie, capable de gérer production et consommation de manière à réduire les coûts, renforcer la fiabilité et la pérennité selon leurs besoins spécifiques.

L'augmentation de l'énergie distribuée augmente la complexité du réseau. Elle fait évoluer le secteur d'une chaîne de valeur de type traditionnel vers un environnement plus collaboratif dans lequel les clients se connectent de manière dynamique au réseau de distribution, aux fournisseurs d'énergie et au marché de l'énergie. Les technologies et les modèles commerciaux devront évoluer pour que le secteur de l'énergie puisse survivre et prospérer.

La nouvelle grille sera considérablement plus numérisée, flexible et dynamique. Elle sera de plus en plus connectée, avec de plus grandes exigences de performance dans un monde où l'électricité occupe une place plus importante dans l'offre énergétique globale. De nouveaux acteurs seront impliqués dans l'écosystème de l'énergie, tels les gestionnaires de réseaux de transport et de réseaux de distribution, les opérateurs de production décentralisée, les agrégateurs et les prosommateurs.

Régulation et conformité

Le déploiement de la cybersécurité vise à respecter les normes et à se conformer à la réglementation. Cette approche profite à l'industrie en sensibilisant davantage aux risques et aux défis associés aux cyberattaques. Au fur et à mesure que le réseau électrique évolue en complexité, avec l'intégration des ressources distribuées et l'automatisation, une nouvelle approche s'impose, axée sur la gestion des risques.

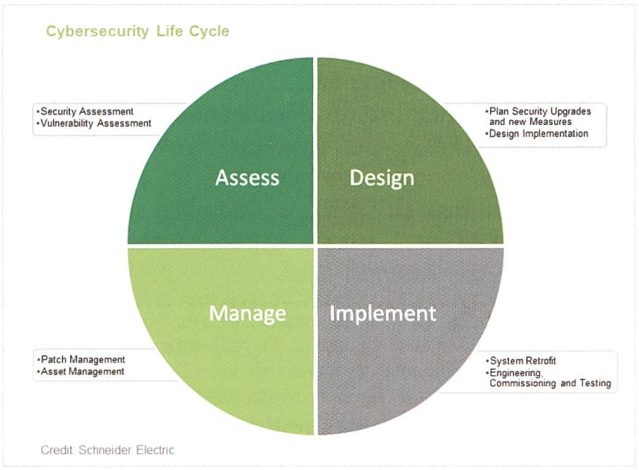
A l'heure actuelle, les parties prenantes des services publics appliquent des processus de cybersécurité appris de leurs homologues des technologies de l'information (IT), ce qui accroît les risques. Dans l'environnement de la sous-station, les dispositifs propriétaires autrefois dédiés à des applications spécialisées sont désormais vulnérables. Les informations sensibles disponibles

en ligne décrivant le fonctionnement de ces dispositifs périphériques sont accessibles à tous, y compris à des acteurs malintentionnés. Ceux-ci, possédant les compétences nécessaires, peuvent pirater un service public et détériorer les réseaux de distribution électrique. Ce faisant, ils mettent également en péril l'économie et la sécurité d'un pays ou d'une région desservis par ces réseaux.

Les régulateurs ont anticipé le besoin d'une approche structurée de la cybersécurité. Aux Etats-Unis, les exigences relatives à la protection des infrastructures critiques de la North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) définissent les éléments nécessaires à la protection du système électrique. Le programme européen de protection des infrastructures critiques (EPCIP) fait à peu près la même chose en Europe. Chaque jour, nous faisons face à de nouvelles attaques complexes, dont certaines sont organisées par des acteurs étatiques, ce qui conduit à une réévaluation de celles-ci et de l'approche de sécurité globale du secteur.

Intégration IT – OT

En raison de la transition vers des technologies et protocoles de communication informatiques ouverts, tels



Ethernet et IP (Internet Protocol), les systèmes gérant les infrastructures critiques sont devenus de plus en plus vulnérables. Lorsque les exploitants d'infrastructures critiques cherchent à sécuriser leurs systèmes, ils se tournent souvent vers des pratiques de cybersécurité plus matures. Cependant, l'approche informatique en matière de cybersécurité n'est pas toujours appropriée, compte tenu des contraintes opérationnelles auxquelles les entités de services publiques sont confrontées.

Didier Giarratano : Responsable de la plateforme cybersécurité de Schneider Electric. M. Giarratino est également membre du Certification Management Committee (CMC) du Système d'évaluation de la conformité pour équipements et composants électrotechniques (IECEE), et membre du Groupe de travail (WG 17) sur la cybersécurité de l'IEC Conformity Assessment Board.

Ces différences d'approche impliquent que les solutions de cybersécurité et l'expertise reposant sur le domaine informatique soient souvent inadaptées pour les applications de technologie opérationnelle (OT). Les attaques sophistiquées réussissent aujourd'hui à tirer parti de services associés tels informatique et télécommunications. A mesure que les services publics font face à la convergence IT-OT, il devient nécessaire de former des équipes multidisciplinaires afin de relever les défis uniques liés à la sécurisation d'une technologie couvrant IT et OT. La protection contre les cybermenaces nécessite désormais une activité plus étendue couvrant plusieurs domaines – les ingénieurs, les spécialistes en informatique et les responsables de la sécurité étant tenus de partager leur expertise pour identifier les problèmes et les attaques pouvant affecter leurs systèmes.

Une approche en quatre points

Les experts en cybersécurité conviennent que les normes en elles-mêmes n'apportent pas le niveau de sécurité approprié. Il ne s'agit pas d'atteindre un état de cybersécurité. Une protection adéquate contre les cybermenaces nécessite un ensemble complet de mesures, de processus et de moyens techniques, ainsi qu'une organisation adaptée. Il est important que les services publics réfléchissent à la manière dont les stratégies de cybersécurité des organisations évolueront avec le temps. Il s'agit de rester au courant des menaces connues de manière organisée et itérative. Assurer une défense efficace contre les cyberattaques est un processus continu qui nécessite des efforts soutenus et un investissement annuel récurrent. La cybersécurité concerne les personnes, les processus et la technologie. Les services publics doivent mettre en place un programme complet comprenant une organisation, des processus et des procédures appropriés pour tirer pleinement parti des technologies de protection de la cybersécurité.

Pour établir et gérer des systèmes cybersécurisés, les services publics peuvent suivre une approche en quatre points. Le Comité consultatif de l'IEC (Commission électrotechnique internationale) sur la sécurité de l'information et la confidentialité des données (ACSEC) travaille sur les mêmes questions, qui sont intégrées dans le Guide IEC 120, Aspects liés à la sécurité – Lignes directrices pour leur inclusion dans les publications.

1. Effectuer une évaluation des risques

La première étape consiste à procéder à une évaluation complète des risques en fonction des menaces internes et externes. Ce faisant, les spécialistes en technologie opérationnelle (OT) et les autres parties prenantes des services publics peuvent comprendre où se trouvent les plus grandes vulnérabilités et être en mesure de documenter la création d'une politique de sécurité et la réduction des risques.

2. Concevoir une politique et des processus de sécurité

La stratégie de cybersécurité des entreprises de service public fournit un ensemble formel de règles à suivre. Celles-ci devraient suivre la série de normes internationales ISO/IEC 27000 sur les techniques de sécurité informatique, qui fournit des recommandations de meilleures pratiques à adopter en matière de gestion de la sécurité de l'information. Cette série de normes est développée par un sous-comité du Comité technique commun créé par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (IEC), ISO/IEC JTC 1/SC 27 : Techniques de sécurité informatique.

La politique d'une entreprise de service public a pour objet d'informer les employés, les fournisseurs et utilisateurs autorisés sur leurs obligations en matière de protection des actifs technologiques et informatiques. Il décrit la liste des actifs à protéger, identifie les menaces qui pèsent sur eux et décrit les responsabilités des utilisateurs autorisés et les privilèges d'accès associés, ainsi que les actions non autorisées et la responsabilité qui en résulte en cas de violation de la politique de sécurité. Des processus de sécurité bien conçus sont également importants. A mesure que les fondements de la sécurité des systèmes changent pour faire face aux vulnérabilités émergentes, les processus du système de cybersécurité doivent être examinés et actualisés régulièrement. Un élément clé pour maintenir une base de sécurité efficace consiste à effectuer une évaluation une ou deux fois par an.

3. Mettre en œuvre le plan de mitigation des risques

Il est nécessaire de choisir une technologie de cybersécurité basée sur les normes internationales afin de garantir la mise en place d'une politique de sécurité appropriée et les mesures d'atténuation des risques adaptées. Une approche sécurisée dès la conception, basée sur les normes internationales. Celles-ci peuvent aider à réduire davantage les risques lors de la sécurisation des composants du système. Elles comprennent, entre autres, la série de publications IEC 62443 sur la sécurité pour les réseaux de communication industriels et les systèmes de contrôle et d'automatisation industriels (IACS), la série de normes internationales IEC 62351 sur la gestion des systèmes d'énergie et les échanges d'informations associées et la norme IEEE 1686 pour les fonctions de cybersécurité des dispositifs électroniques intelligents,

développée par l'Institut des ingénieurs électriciens et électroniciens (IEEE).

4. Gérer le programme de cybersécurité

La gestion efficace des programmes de cybersécurité nécessite non seulement de prendre en compte les trois points précédents, mais également de gérer les cycles de vie des actifs d'information et de communication. Pour ce faire, il est important de conserver une documentation vivante et précise sur les micrologiciels, les systèmes d'exploitation et les configurations. Cela nécessite également une compréhension approfondie des calendriers de mise à niveau technologique et d'obsolescence, ainsi qu'une connaissance approfondie des vulnérabilités connues et des correctifs existants. La gestion de la cybersécurité exige également que certains événements provoquent des évaluations, telles que des points particuliers du cycle de vie des actifs ou des menaces détectées.

Pour les services publics, la sécurité est l'affaire de tous. Les politiciens et le public sont de plus en plus conscients que la sécurité nationale dépend également de la robustesse des services publics locaux. Atténuer les risques et anticiper les vulnérabilités des attaques sur les réseaux et les systèmes de distribution ne consiste pas uniquement à installer des technologies. Les services publics doivent également mettre en œuvre des processus organisationnels pour faire face aux défis d'un réseau décentralisé. Cela signifie une évaluation régulière et une amélioration continue de leur processus de cybersécurité et de sécurité physique afin de protéger notre nouveau monde énergétique.

D. G.

Liens :

Commission électrotechnique internationale (IEC) : https://www.iec.ch/

Organisation internationale de normalisation (ISO) : https://www.iso.org/

ISO/IEC JTC 1/SC 27 : Techniques de sécurité informatique : https://www.iso.org/committee/45306.html

IEC CAB WG 17 – Groupe de travail 17, cybersécurité, du Conformity Assessment Board de l'IEC https://tinyurl.com/y7e7pnyk

IECEE CMC WG 31 – Groupe de travail 31, cybersécurité, du Certification Management Committee du Système d'évaluation de la conformité de l'IEC pour les équipements et composants électrotechniques (IECEE) https://tinyurl.com/y98o3vwm

IEC Advisory Committee on Information security and data privacy (ACSEC) https://www.iec.ch/acsec

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) https://tinyurl.com/y96mlp95

Programme européen de protection des infrastructures critiques (EPCIP) https://tinyurl.com/y9rbqnwy

Normes :

IEC 62443 : Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes (Industrial communication networks – Network and system security) https://tinyurl.com/ya9kd238

IEC 62351 : Gestion des systèmes de puissance et échanges d'informations associés (Power systems management and associated information exchange) https://tinyurl.com/y9rn5fvj

IEEE 1686 : Norme IEEE pour les fonctions de cybersécurité des dispositifs électroniques intelligents, https://tinyurl.com/ycftrj7k