ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE
DIRECTION GENERALE DE LA SECURITE
DES SYSTEMES D'INFORMATION

GUIDE RELATIF A LA SECURITE DES SYSTEMES D'INFORMATION INDUSTRIELS

INFORMATIONS

AVERTISSEMENT

Les éléments contenus dans ce document ont vocation à être applicables à tous les secteurs. Certains d'entre eux ont des spécificités qui n'ont peut-être pas été détaillées ou prises en compte dans le présent document. En conséquence, une déclinaison sectorielle de ce document pourra être nécessaire dans certains cas afin de préciser les modalités d'application et prendre en compte les contraintes spécifiques.
Il est également possible que dans certaines situations des mesures ne puissent s'appliquer sans adaptation (pour des raisons de compatibilité avec des systèmes industriels existants ou des contraintes métier spécifiques, par exemple). Ces cas particuliers devront être étudiés spécifiquement et les mesures qui en découleront seront soumises pour approbation aux responsables du système d'information industriel.

GESTION DU DOCUMENT

Auteur	Version	Date de la version
DGSSI	**V.1**	**Février 2017**

POUR TOUTE REMARQUE

Contact	**e-mail**
DGSSI	contact@dgssi.gov.ma

SOMMAIRE

INTRODUCTION

Les systèmes industriels utilisent aujourd'hui abondamment les technologies de l'information alors qu'ils n'ont pas été conçus pour faire face aux menaces qu'elles introduisent. Pour cette raison, les systèmes industriels sont de plus en plus concernés, et probablement même davantage, que les autres systèmes d'information par les enjeux de la cybersécurité.

Pour faire face aux enjeux et aux risques croissants qui entourent les systèmes d'informations industriels, la DGSSI a élaboré le présent guide qui a pour principaux objectifs de:

- Sensibiliser les acteurs concernés aux vulnérabilités des systèmes d'information industriels;
- proposer un ensemble de mesures pour améliorer le niveau de cybersécurité de ces systèmes.

Ce document s'adresse à tous les acteurs (entités responsables, chefs de projets, acheteurs, équipementiers, intégrateurs, maîtres d'œuvre, etc.) participant à la conception, la réalisation, l'exploitation et la maintenance des systèmes industriels.

Avis aux lecteurs

Les mesures présentées dans le document sont des mesures de cybersécurité conventionnelles mais adaptées pour les systèmes industriels. L'objectif de ce document n'est en aucun cas de former les lecteurs à la cybersécurité pour les systèmes industriels. Il a donc été supposé que les lecteurs disposaient de connaissances élémentaires en matière de technologies de l'information et de la communication mais aussi de cybersécurité ou qu'ils pouvaient s'appuyer sur des personnes disposant de ces compétences. La bonne application de certaines mesures nécessitera certainement un travail d'équipe entre des « informaticiens » et des « automaticiens ».

I. DEFINITION, CONSTITUANTS

Un Système d'Information Industriel pilote des installations, régule des procédés et traite des données.

Un système d'information industriel est généralement composé des sous-systèmes suivants :

→ une interface homme-machine assurant la visualisation et le commandement du processus industriel;
→ un système de supervision et de contrôle informatique qui est connecté au système de gestion de production de l'entité d'où il reçoit ses commandes. Il est constitué le plus souvent d'éléments issus de l'informatique de

gestion tels que des serveurs ou des postes de travail fonctionnant avec des systèmes d'exploitation ;

→ une unité terminale distante (RTU) convertissant les signaux provenant des capteurs en flux de données numériques et envoyant les données numériques au système de supervision ;

→ des automates programmables industriels utilisés pour leur versatilité et flexibilité due à leur capacité d'être configurables ;

→ une infrastructure de communication connectant le système de supervision et contrôle aux éléments terminaux ;

→ divers instruments permettant l'interaction avec le monde physique : Il s'agit de capteurs (température, ouverture, humidité, lumière…) et d'actionneurs (pompes, vérins, moteurs, voyants…).

II. LES ENJEUX DE LA CYBERSECURITE DES SYSTEMES INDUSTRIELS

1. GENERALITES SUR LES ATTAQUES

Les cyber-attaquants ont des profils divers, notamment le hacker isolé, le salarié mécontent, les réseaux organisés, les cellules de renseignement. Ils ont une multitude des motivations, tels que le défi informatique pour démontrer une capacité technique, le vol de données à des fins lucratives, le hacker-activisme pour des causes idéologiques ou politiques, l'espionnage à des fins économiques ou industrielles, etc.

Les attaques peuvent provenir de :

- l'intérieur de l'entité exploitant le système d'information industriel : menaces internes du fait de comportements inadaptés des personnels à l'usage des nouvelles technologies ou d'une malveillance et du fait d'un défaut de gouvernance augmenté ;
- l'extérieur de l'entité : hacktivisme, virus, campagnes de spam.

2. LES IMPACTS POTENTIELS SUR LES SYSTEMES INDUSTRIELS

Les cyber-attaques ciblant les systèmes d'information industriels sont de plus en plus sophistiquées, comme l'incident de centrale nucléaire au Royaume-Uni lié à Conficker, l'incident lié au ver Slammer aux USA, ou bien la propagation généralisée du virus Stuxnet. Leurs impacts peuvent être analysés et répertoriés selon différents axes, présentés ci-dessous:

Dommages matériels / corporels	La modification des configurations nominales des installations peut provoquer des dégradations physiques avec le plus souvent des conséquences matérielles et humaines considérables.
Perte de chiffre d'affaires	L'arrêt de la production génère des pertes financières importantes. La modification de paramètres de fabrication conduisant à des produits

	non conformes génère des coûts supplémentaires considérables.
Vol de données	Perte de données sensibles (secret de fabrication) offre des avantages pour le concurrent.
Responsabilité civile / pénale - Image et notoriété	L'indisponibilité du système comme la rupture de distribution d'électricité ou d'eau, ainsi que la fourniture de produits défectueux mettent en défaut l'entité devant ses obligations légales et juridiques et peuvent aboutir à des poursuites pour les dommages occasionnés ou simplement dégrader l'image de marque de l'entité (la satisfaction du client et sa confiance).
Impact sur l'environnement	La défaillance du système suite à une prise de contrôle malveillante peut provoquer des catastrophes écologiques et des dégâts sanitaires.

3. LISTE DES CONTRAINTES

Lors du choix des mesures de sécurité à mettre en œuvre, il est primordial de prendre en considération les contraintes énumérées ci-dessous qui peuvent avoir des conséquences graves sur la sécurité du système industriel concerné.

3.1. Gouvernance de sécurité

- Lorsque la direction des systèmes d'information (DSI) se voit attribuer la mission de sécuriser les systèmes industriels, elle n'a pas de lien hiérarchique avec les équipes chargées de l'opération de ces derniers. Ceci complique ou ralentit la mise en œuvre de la cybersécurité.
- Lorsque la sécurisation des systèmes industriels est confiée à une direction métier, la cybersécurité a souvent une priorité basse et la responsabilité de la gestion des interfaces entre les systèmes industriels et les systèmes de gestion est floue.
- Il y a peu de personnel en charge de l'informatique industrielle sur un site industriel.

3.2. Maîtrise des installations

- Multitude d'intervenants sur une installation ce qui rend difficile la maîtrise des actions effectuées sur celle-ci.
- Multitude de sites isolés, notamment dans les secteurs du transport, de la distribution d'eau ou de l'énergie, bénéficiant d'une protection physique limitée.
- La documentation technique de l'installation peut être limitée. Ce qui entraîne une perte du savoir lors des départs de personnels et ne facilite

pas le traitement des incidents.

- Certains fournisseurs font de la télémaintenance depuis l'étranger.
- Sur certaines installations cohabitent deux opérateurs différents, ce qui peut parfois poser des problèmes en cas de modification de l'installation.
- Les installations sont souvent hétérogènes car venant de différents fournisseurs ou parce qu'elles ont évoluées au cours du temps. L'hétérogénéité peut être imposée pour des raisons de sûreté fonctionnelle.

3.3. Contrats

- Les fournisseurs exigent d'avoir accès à leurs équipements en télémaintenance sous peine de ne pas les garantir.
- La modification des systèmes sans accord préalable du fournisseur peut entrainer une perte de garantie.
- Il peut être contractuellement interdit de modifier l'installation existante même pour implémenter des mesures de cybersécurité.

3.4. Gestion des Changements

- Il n'existe pas d'environnement de test permettant de s'assurer de la non- régression des installations.
- Les interventions sur les installations ne peuvent être effectuées que lors des périodes de maintenances.
- Les fournisseurs offrent peu de support pour aider les opérateurs à qualifier les impacts des mesures de sécurité sur les installations.

3.5. Contraintes Economiques

- Les mises à jour des systèmes existants et l'évolution des installations entraînent des coûts importants pour le client.

3.6. Contraintes Techniques

- Les équipements sont déployés pour 15 à 20 ans. L'obsolescence limite leurs possibilités de mise à jour ainsi que l'intégration de fonctions de sécurité.
- Certains équipements (comme les automates) et protocoles offrent des fonctionnalités de sécurité limitées voire inexistantes.
- Les fournisseurs offrent peu de solutions techniques permettant une gestion centralisée des fonctions de sécurité. Par exemple, il n'est souvent pas possible de changer un mot de passe sur plusieurs équipements dispersés géographiquement.

3.7. Culture de la sécurité

- Dans les milieux où la sûreté de fonctionnement est très présente, il y a souvent un sentiment que celle-ci permet également de régler les problèmes de cybersécurité.

- La sécurité des systèmes d'information n'est pas abordée lors des cursus de formation et en particulier ceux des automaticiens.

3.8. Maturité des solutions techniques

- Il existe peu de compétences en matière de cybersécurité des systèmes industriels.
- Peu de fournisseurs intègrent la notion de cycle de développement sécurisé dans la réalisation de leurs produits.

4. CARTOGRAPHIE DES VULNERABILITES LIEES AUX SYSTEMES D'INFORMATION INDUSTRIELS

Parmi les principales vulnérabilités rencontrées dans les systèmes d'information industriels, on pourrait retrouver :

4.1. Absence de veille sur les vulnérabilités

Les entités responsables de système industriel négligent la mise en place d'une veille active sur les vulnérabilités des produits et technologies utilisés. Aucune veille n'est faite sur l'évolution de la menace ou des techniques d'attaque.

4.2. Défaut de la politique de gestion des mots de passe

Les politiques de mots de passe sont souvent insuffisantes ou incomplètes. Ceci peut impliquer les problèmes suivants :

- Automates et composants industriels en production avec des mots de passe par défaut ;
- la faible fréquence de changement des mots de passe (par exemple due au manque d'outil pouvant mettre à jour les mots de passe d'un parc d'automates) ;
- l'utilisation de mots de passe faibles.

4.3. Absence de procédure de gestion des départs et des arrivées

Les entités responsables des systèmes industriels mettent rarement en place des procédures de gestion des départs et des arrivées. En particulier, un ancien employé pourra garder son compte longtemps après son départ.

4.4. Défaut de contrôle des interfaces de connexion

Sur certains systèmes industriels, on constate l'absence de la mise en place d'une politique de gestion des interfaces de connexion. Par exemple, les ports USB ne sont pas désactivés ou les ports Ethernet non exploités sont laissés actifs.

4.5. Manque de contrôle d'intégrité ou d'authenticité

Les entités responsables des systèmes industriels ne prennent pas en considération la nécessité de mise en place des mécanismes de contrôle

d'intégrité ou d'authenticité pour les logiciels, les programmes d'automates et applications SCADA.

4.6. Utilisation d'équipements vulnérables

Les équipements développés pour les systèmes industriels intègrent souvent des contraintes de sûreté de fonctionnement fortes mais rarement des contraintes de cybersécurité. En particulier, les fonctions de sécurité sont souvent limitées voire inexistantes et les techniques de développement employées prévoient rarement la présence d'un attaquant sur le système comme une menace.

4.7. Absence de sauvegarde

Les sauvegardes sont souvent partielles, inexistantes ou disponibles chez le fournisseur seulement. Lorsque des sauvegardes existent, le bon fonctionnement des procédures de restauration en cas d'incident est rarement testé et vérifié.

4.8. Modifications en ligne non maîtrisées

Il est possible de modifier à chaud, sans mécanisme d'authentification ou de journalisation, des programmes d'automates ou des applications SCADA. Cette fonctionnalité très utile lorsque les systèmes fonctionnent en 24/7 présente souvent très peu de mécanismes de cybersécurité.

4.9. Utilisation de protocoles vulnérables

Les systèmes industriels font souvent usage de protocoles réseaux n'intégrant aucun mécanisme de sécurité (chiffrement..). Ces protocoles peuvent être des protocoles classiques ou standards mais peuvent également être des protocoles spécifiques aux systèmes industriels.

4.10. Défaut de contrôle d'accès physique

Selon le domaine d'activité, le système industriel ou ses composants pourraient être situés dans des usines, sur la voie publique ou dans d'autres endroits qui ne permettent pas la mise en place d'un contrôle d'accès physique adéquat et efficace.

4.11. Défaut de cloisonnement

Il est fréquent qu'il n'y ait pas de cloisonnement effectif entre un système industriel et le système d'information de gestion. Cette ouverture des réseaux industriels vers le système d'information de gestion ou un réseau public comme Internet peut être due à des raisons opérationnelles comme des contraintes de planning ou de mutualisation d'outils ou à des raisons de réduction de coûts pour faciliter la remontée d'information du système industriel vers le système d'information de gestion.

Par ailleurs, il est très souvent qu'il n'y ait pas de cloisonnement non plus au sein même des systèmes industriels ; entre ses différents sous-ensembles par

exemple. Ceci peut également être dû à des besoins de réduction de coûts ou à une méconnaissance de la nécessité de cloisonner les systèmes.

4.12. Les solutions de la télémaintenance

L'usage de la télémaintenance et la télégestion est une pratique de plus en plus courante pour les systèmes industriels. Certains sont même connectés sur des réseaux publics comme Internet ou les réseaux de téléphonie mobile. Les solutions techniques utilisées pour la télégestion ou la télémaintenance diminuent considérablement le niveau de sécurité et augmente la surface d'attaque.

4.13. Utilisation de technologies standards

Afin d'assurer l'interopérabilité des systèmes industriels avec les systèmes d'information de gestion, les technologies employées pour les premiers sont de plus en plus standards. Ainsi, en termes de réseau, Ethernet et TCP/IP sont de plus en plus utilisées pour remplacer les technologies propriétaires qui étaient employées auparavant. Les outils de développement ou de maintenance font également de plus en plus appel à des briques génériques.

4.14. Manque de la sensibilisation

Les intervenants sur un système industriel ne sont pas toujours sensibilisés à la cybersécurité des systèmes d'information et méconnaissent souvent la politique de sécurité des systèmes d'information (PSSI), si elle existe, du système sur lequel ils interviennent. De nombreux incidents, provenant d'un manque de sensibilisation, sont régulièrement constatés.

4.15. Supervision insuffisante des événements de cybersécurité

En cas d'incident sur une installation, les opérateurs et mainteneurs n'envisagent pas forcément une action malveillante comme cause possible. La journalisation des événements de sécurité est souvent limitée et peu exploitée. Les dispositifs de détection d'incidents ou de dysfonctionnements sont rares.

Lorsqu'une supervision des événements de cybersécurité est effective, la multitude des paramètres et la complexité de l'environnement peuvent limiter l'analyse de l'incident.

4.16. Absence de plan de continuité d'activité

Les plans de continuité d'activité ou les plans de reprise d'activité ne prennent pas forcément en compte les événements relatifs à la cybersécurité. Les équipes opérationnelles disposent rarement de consignes de réaction à des événements de cybersécurité.

4.17. Non prise en compte de la cybersécurité dans les projets

Lors des phases de spécification et de conception du système industriel, les documents n'intègrent généralement aucune exigence en matière de cybersécurité.

4.18. Absence de tests de cybersécurité

Les tests avant mise en service (FAT et SAT) contiennent rarement des tests portant sur la cybersécurité. Lors des opérations de maintenance, des tests de sûreté ou de conformité du système d'information sont souvent envisagés mais pas d'audits de cybersécurité.

4.19. Mal définition des responsabilités

Les responsabilités en matière de cybersécurité sont souvent mal identifiées entre le fournisseur, l'intégrateur et l'entité responsable du système industriel. De même les responsabilités entre les directions métier et la Direction des Systèmes d'Information ne sont pas forcément claires non plus.

III. MESURES TECHNIQUES ET ORGANISATIONNELLES A IMPLEMENTER POUR RENFORCER LA CYBERSECURITE DES SYSTEMES INDUSTRIELS

De nombreuses mesures énumérées ci-dessous sont similaires à celles de l'informatique de gestion, mais leur mise en œuvre est à adapter aux contraintes du domaine industriel. Il conviendra d'évaluer de manière exhaustive les impacts avant toute implémentation.

1. Définir les rôles et responsabilités

Il est nécessaire de définir clairement les responsabilités relatives à la cybersécurité pour chacune des parties prenantes quel que soit l'aspect concerné (développement, intégration, exploitation, maintenance, etc.).

2. Sensibiliser et former les intervenants

La formation des intervenants en cybersécurité est obligatoire avant toute intervention sur le système industriel. Une charte de sécurité doit être définie et signée par chaque intervenant.

3. Elaborer la politique de sécurité des systèmes d'information industriels

En parallèle à l'action de sensibilisation et de formation des intervenants, l'élaboration de la politique de sécurité des systèmes industriels doit être mise en place en prenant en considération les aspects relatifs à la cybersécurité.

4. Concevoir une cartographie

Une cartographie logique et physique du système industriel doit être établie. La cartographie et la documentation du système industriel doivent être revues régulièrement, à chaque modification touchant le système industriel.

5. Conduire une analyse de risques

Les systèmes industriels doivent faire l'objet d'une analyse de risque rigoureux et continu pour la cybersécurité. Il est recommandé de suivre la méthode proposée par le guide relatif à la gestion des risques élaboré par la DGSSI.

6. Prendre en compte de la sécurité des systèmes d'information lors des achats

Il convient de s'assurer que les dossiers d'appels d'offres contiennent des exigences de sécurité sur le système industriel acheté. Elles concernent le système faisant l'objet de la consultation mais aussi la gestion du projet lui-même (formation voire habilitation des installateurs), en incluant les phases opérationnelles et de maintenance. Il est recommandé de :

- vérifier dans les réponses aux appels d'offres la couverture des exigences sécurité inscrites dans la consultation ;
- établir les clauses concernant la maintenance de l'équipement : demander les plans de maintenance nécessaires pour maintenir l'installation en condition opérationnelle et de sécurité ;
- définir les processus de traitement des incidents et de fourniture de correctifs de sécurité : qui prend l'initiative, qui déploie, sous quels délais, qui fait les tests de bon fonctionnement et comment, etc. ;
- définir les conditions de propriété des codes sources et des paramètres.

7. Prendre en compte de la sécurité des systèmes d'information à l'occasion des opérations de maintenance

Les plans de maintenance des systèmes d'information industriels ne peuvent être dissociés des plans de maintenance des installations qu'ils pilotent .Pour cette raison, la sécurité des systèmes d'information (SSI) des installations industrielles doit être prise en compte lors de la rédaction des plans de maintenance. Ces derniers doivent intégrer les opérations nécessaires pour maintenir le niveau de sécurité des systèmes dans la durée :

- définir les opérations de maintenance propres à la SSI qui sont nécessaires au maintien en conditions opérationnelles (MCO) et au maintien en conditions de sécurité (MCS) ;
- intégrer dans les opérations de maintenance préventive métier (maintenance électrique, mécanique par exemple) les opérations de SSI qu'il n'est pas possible de réaliser lorsque l'installation est en fonctionnement.

8. Concevoir un plan de sauvegarde

Il est primordial de concevoir un plan de sauvegarde des données afin de permettre leur restauration en cas d'incident .Il est recommandé de tester régulièrement le processus de restauration des sauvegardes.

9. Protéger la documentation

Il est nécessaire de garantir la confidentialité de l'ensemble des documents relatifs à la conception, à la configuration ou au fonctionnement du système industriel. Les documents doivent être stockés et manipulés dans un système d'information dont le niveau de sensibilité est adapté aux systèmes industriels.

10. Réaliser des audits et tests de cybersécurité

Il est nécessaire d'effectuer régulièrement des tests ou des audits de cybersécurité. Chaque audit doit être associé à un plan d'action corrective à mettre en œuvre. Pour éviter toute défaillance, Les tests de pénétration doivent être exécutés dans le cadre de maintenance ou avant la mise en production des systèmes.

11. Gérer les interventions

Il est nécessaire de formaliser une procédure de gestion des interventions afin de pouvoir déterminer :

- la personne exécutant le travail et son donneur d'ordre ;
- la date et l'heure de l'intervention ;
- le périmètre de l'intervention ;
- les actions menées ;
- la liste des équipements retirés ou remplacés (y compris, le cas échéant, les numéros d'identification) ;
- les modifications apportées et leur impact.

Chaque intervention doit être autorisée et validée par l'entité responsable.

12. Protéger les accès aux locaux

Une politique de contrôle d'accès physique doit être formalisée. Elle doit prévoir notamment la protection des clés permettant l'accès aux locaux et les codes d'alarme. Les accès aux locaux devraient être mis sous vidéo-protection et être réservé uniquement aux personnes habilitées.

Chaque l'entité responsable du système industriel doit assurer la traçabilité des accès et conserver les enregistrements pour une durée d'au moins trois mois.

13. Protéger les accès aux équipements

Les unités centrales des stations, les équipements réseaux industriels et les automates doivent être placés dans des armoires fermées à clé. Les prises d'accès au système industriel ne doivent pas être accessibles dans les zones sans surveillance.

14. Définir un plan de reprise ou de continuité d'activité

Les plans de reprise et de continuité d'activité doit prendre en compte les incidents de cybersécurité afin de pouvoir reconstruire le système après sinistre. Le PCA /PRA devrait être régulièrement mis à jour, en fonction :

- des évolutions propres de l'infrastructure (maintenance, intégration de nouveaux composants, qui peuvent introduire de nouvelles vulnérabilités) ;
- de l'évolution des menaces.

15. Gérer les incidents

La mise en place d'un processus d'alerte et de gestion d'incident est obligatoire. Il doit être testé régulièrement, et au minimum une fois par an, pour vérifier son efficacité. Il permet de déterminer :

- les actions à mener lors de la détection d'un incident ;
- la personne qui doit alerter ;
- la personne qui doit coordonner les actions en cas d'incident ;
- les premières mesures à appliquer.

La gestion des incidents doit prévoir une phase d'analyse post incident permettant d'en identifier l'origine et d'améliorer la sécurité du système industriel.

16. Gérer l'authentification des intervenants

Les différents composants (équipements et logiciels) ne doivent être accessibles qu'après une authentification avec identifiant et mot de passe. Lorsque cela est possible, la politique de mots de passe doit répondre à minima aux exigences suivantes :

- les mots de passe doivent être robustes;
- les mots de passe par défaut doivent être changés.

Des rôles doivent être définis, documentés et implémentés pour que les comptes des utilisateurs aient des privilèges correspondant exactement à leurs missions.
Il est fortement recommandé de mettre en œuvre une authentification forte (carte à puce, OTP, etc.) sur les postes de travail et serveurs. Cette mesure peut être étendue aux équipements de terrain (automates, entrées/sorties déportées), etc.

17. Assurer le cloisonnement des systèmes industriels

Les systèmes industriels doivent être cloisonnés entre eux à l'aide de pare-feu. L'interconnexion doit être unidirectionnelle vers le système d'information de gestion. Cette unidirectionnalité doit être garantie physiquement (avec une diode, par exemple) ou bien par un pare-feu. Un système industriel ne doit pas être connecté à un réseau public.

18. Protéger l'accès à distance

Les opérations de télémaintenance ou de télégestion sont fortement déconseillées. Le cas échéant, la solution de télémaintenance doit suivre les règles suivantes :

- elle doit assurer la confidentialité, l'intégrité et l'authenticité des communications (exemple : VPN IPsec) ;
- une authentification forte à deux facteurs doit être mise en place ;
- les équipements de connexion doivent être cloisonnés du reste du système

industriel et seuls les flux indispensables à la télémaintenance doivent être autorisés ;
- la journalisation des événements de sécurité doit être activée.

19. Protéger les communications sans fil

L'usage des technologies sans fil n'est est pas recommandé et doit être limité aux cas où il n'existe pas d'autre solution. L'utilisation de technologie sans fil doit être interdite sur toutes les liaisons ayant des besoins critiques de disponibilité. Les événements de sécurité générés par les équipements sans fil doivent être centralisés et supervisés en temps réel.

20. Gérer les vulnérabilités

La mise en œuvre d'un processus de gestion des vulnérabilités est obligatoire afin de:

- rechercher les correctifs disponibles pour corriger et traiter ces vulnérabilités ;
- identifier les vulnérabilités connues et mesurer leurs impacts sur les systèmes ;
- mette en œuvre les correctifs en commençant par les plus importants ;
- recenser les vulnérabilités qui n'ont pas pu être corrigées (soit par manque de correctifs, soit parce que le correctif n'a pas pu être appliqué en raison de contraintes opérationnelles).

Les correctifs de sécurité doivent être appliqués en priorité sur les équipements les plus exposés (postes de travail, PC portables, stations d'ingénierie, consoles de programmation, pare-feu, VPN, etc.). Une vérification de l'application effective des correctifs de sécurité doivent être effectuée.

Un environnement de test représentatif des systèmes en production devrait être mis en œuvre afin de s'assurer de leur non-régression après l'application des correctifs.

21. Gérer les médias amovibles

Définir une politique d'utilisation des médias amovibles (clé USB, disquette, disque dur, etc.) est fortement conseillé. Il convient de mettre à disposition des intervenants des médias amovibles dédiés aux systèmes industriels. L'utilisation de ces médias pour tout autre usage devrait être interdite.

22. Gérer les points d'accès réseau

Il est nécessaire de mette en œuvre un processus permettant l'identification et le recensement des points d'accès réseau disponibles. Les points d'accès réseau non utilisés (commutateurs, hubs, baies de brassage, prises de maintenance sur les bus de terrain, etc.) devraient être désactivés. En cas de tentative de connexion et de déconnexion sur des ports réseau, une alerte doit être remontée et traitée.

23. Gérer l'usage des équipements mobiles

Il est nécessaire de mettre en place une charte d'utilisation des terminaux nomades. L'usage des périphériques personnels quels qu'ils soient (ordiphones, tablettes, clés USB, appareils photos, etc.) devrait être interdit.
Un processus d'attribution des terminaux mobiles devrait être mis en place. Il devrait permettre, à minima :

- de valider l'attribution du terminal par le responsable hiérarchique ;
- d'assurer la traçabilité entre le terminal et ses utilisateurs ;
- de sensibiliser l'utilisateur aux règles d'usage en vigueur.

24. Sécuriser l'environnement de développement

Un environnement de développement devrait être dédié au système industriel. Le niveau de sécurité de l'environnement de développement doit être vérifié par des audits. En cas d'externalisation de l'environnement de développement chez un fournisseur, il convient d'indiquer les exigences attendues dans le cahier des charges.

25. Mettre en place de moyens de surveillance et de détection

Des moyens de détection d'intrusion doivent être déployés en périphérie des systèmes industriels et sur les points identifiés comme critiques qui comprennent notamment :

- les interconnexions avec Internet (y compris la télémaintenance) ;
- les interconnexions avec le système d'information de gestion ;
- les points de connexion spécifiques vers l'extérieur (WiFi industriel par exemple);
- sur les réseaux d'automates jugés sensibles.

26. Désactiver Les protocoles non sécurisés

Les protocoles non sécurisés (http, telnet, ftp, etc.) devraient être désactivés au profit des protocoles sécurisés (https, ssh, sftp, etc.) pour assurer l'intégrité, la confidentialité, l'authenticité des flux.

Pour les protocoles ne pouvant pas être sécurisés pour des raisons techniques et opérationnelles, des mesures compensatoires devraient être mises en place comme :

- mettre en place des protections périmétriques (pare-feu) ;
- encapsuler les flux dans un VPN pour en assurer l'intégrité et l'authenticité.

GLOSSAIRE

Cybersécurité : État recherché pour un système d'information lui permettant de résister à des événements d'origine malveillante susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services rendus par ce système.

Diode : Équipement de cloisonnement visant à permettre la circulation des informations dans un seul sens. L'unidirectionnalité est assurée de manière physique

Disponibilité : Propriété permettant de rendre le service attendu en temps voulu et dans les conditions d'usage prévues.

Impact : Conséquence directe ou indirecte de la non-réalisation des besoins de sécurité sur l'organisme et/ou sur son environnement.
Exemples : sur la mission, sur la sécurité des personnes, financiers, juridiques, sur l'image, sur l'environnement.

Intervenant : Toute personne étant amenée à intervenir sur un système d'information. Ceci comprend le personnel chargé de l'opération du système mais également les intégrateurs, les mainteneurs….

Intrusion : Prise de contrôle, certaine ou probable, d'un système d'information ou de l'un de ses constituants par une ou plusieurs personnes non-autorisées

Intégrité : Propriété de protection de l'exactitude et de la complétude des actifs.

Mesure de sécurité : Moyen de traiter un risque de sécurité de l'information. La nature et le niveau de détail de la description d'une mesure de sécurité peuvent être très variables.

Pare-feu : Équipement permettant d'appliquer la politique de cloisonnement entre plusieurs réseaux en filtrant les flux de données entre ceux-ci.

Surface d'attaque : Ensemble des ressources vulnérables d'un système donné, exposées à des attaques par des sources de menace extérieures via les différentes interfaces entre ce système et son environnement.

Télégestion : Action de prendre le contrôle à distance, sous-entendu depuis l'extérieur des systèmes d'information de l'entité responsables, d'installations techniques géographiquement réparties (lecture/écriture).

Télémaintenance : Action d'effectuer à distance, sous-entendu depuis l'extérieur des systèmes d'information de l'entité responsable, des tâches de maintenance sur des installations techniques. Ceci implique notamment de pouvoir faire des modifications de paramètres ou de programmes (lecture/écriture).

Vulnérabilité : Caractéristique d'un bien support qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information.