Livret de Sécurité
Les 13 bonnes pratiques de l'ANSSI

V1.1 – 04/2023

SOMMAIRE

1 Introduction 3
1.1 Généralités 3
1.2 Symboles du document 3
2 Les 13 bonnes pratiques 4
2.1 Contrôle d'accès physique aux équipements et aux bus de terrain (BP01) 4
2.2 Cloisonnement des réseaux (BP02) 5
2.3 Gestion des médias amovibles (BP03) 6
2.4 Gestion des comptes (accès logique, authentification) (BP04) 7
2.5 Durcissement des configurations (système industriel) (BP05) 8
2.6 Gestion des journaux d'événements et d'alarmes (BP06) 9
2.7 Gestion des configurations (paramétrages) (BP07) 10
2.8 Sauvegardes / restaurations (BP08) 11
2.9 Documentation (BP09) 12
2.10 Protection antivirale (BP10) 13
2.11 Mise à jour des correctifs (planification) (BP11) 14
2.12 Protection des automates (PLC) (BP12) 15
2.13 Stations d'ingénierie, postes de développement (BP13) 16

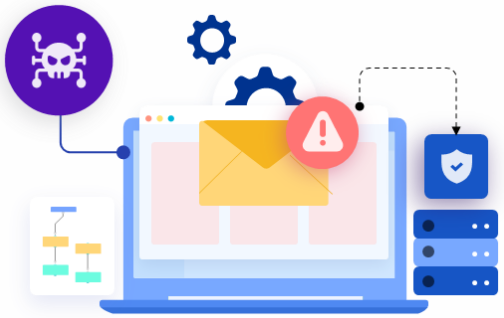
1 Introduction

1.1 Généralités

La sécurité a depuis toujours été un sujet important pour les équipements techniques des bâtiments, et elle l'est d'autant plus ces dernières années. Notre secteur d'activité est exposé, comme d'autres secteurs d'ailleurs, aux risques de cyberattaques. Tous nos clients sont concernés par la cybersécurité selon les enjeux de leurs métiers et les éventuelles contraintes réglementaires auxquelles ils sont soumis.

La cybersécurité pour WIT est un enjeu majeur inscrit dans la stratégie de l'entreprise dans la durée. Nous mettons en œuvre les recommandations de l'ANSSI dans le process industriel de conception, d'assemblage de nos produits et de leur mise en œuvre sur site.

Ce document présente les spécificités de nos solutions répondant aux recommandations et bonnes pratiques de l'ANSSI pour les systèmes industriels.



Qu'est-ce que l'ANSII ?
Service du Premier ministre, rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN), l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique. Acteur majeur de la cyber sécurité, l'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV). Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

1.2 Symboles du document

Ce symbole représente la recommandation de l'expert cybersécurité : l'ANSSI.

Ce symbole représente l'action du gestionnaire du bâtiment, il doit s'assurer de respecter les bonnes pratiques données par l'expert cybersécurité.

Qu'est-ce qu'une ULI ?
Unité Local Intelligente, dans ce document l'ULI représentera l'UC REDY.

2 Les 13 bonnes pratiques

2.1 Contrôle d'accès physique aux équipements et aux bus de terrain (BP01)

Accessibilité physique et Numérique

Ce sujet porte sur la maitrise des points d'accès physique qui permettraient de s'introduire dans le système. Ainsi, la sécurisation des accès physiques à l'Unité Locale Intelligente (ULI) ainsi qu'aux différents postes informatiques pouvant s'y connecter sont à prendre en considération dans la sécurité globale de l'installation.

Cette sécurisation peut être réalisée par des moyens traditionnels (porte à clé) ou par des moyens plus modernes : contrôle d'accès avec identification des personnes (lecteur de badges + ventouse/gâche électrique ou serrure sans-fil). Cette seconde solution offre également l'avantage de pouvoir suivre les accès aux locaux techniques. De plus il sera important d'identifier les contacts ayant accès aux équipements, selon leurs besoins et leurs fréquences d'utilisation du système.

Il est recommandé de sécuriser l'intérieur comme l'extérieur des bâtiments les accès aux appareils communicants, aux câbles réseaux (Ethernet), aux prises de connexion ainsi qu'aux bus terrains (modbus, BACnet, M-BUS,…)

Il est conseillé de mettre en place un système d'accès et d'intrusion aux sites.
Ce système doit prendre en compte les armoires électriques comprenant les automatismes.
Aucun câble et point de terminaison ne doit être accessible à l'extérieur du bâtiment/site.
De maitriser les accès aux terminaisons réseaux et bus terrain a des personnes externes.

2.2 Cloisonnement des réseaux (BP02)

Limiter la propagation des attaques et confiner les vulnérabilités

Afin de limiter la propagation des attaques et confiner les vulnérabilités, il est nécessaire de cloisonner les réseaux des différents services.
La cartographie des Flux : C'est un élément indispensable à un Système d'informations car il permet d'évaluer très rapidement les vulnérabilités du système.

Il est recommandé :

- D'établir une cartographie des flux, c'est un élément indispensable à un Système d'informations car il permet d'évaluer très rapidement les vulnérabilités du système
- De séparer les réseaux par des équipements appropriés (par ex. VLAN).
- D'avoir un Pare-feu qui filtre les flux. Les systèmes de Pare-Feu doivent être inhérent à chaque matériel afin de sécuriser au mieux les installations. Cependant seul un pare-feu général est garant de l'ensemble d'un site industriel.
- De rejeter et d'analyser ces flux, pour cela le protocole Syslog répond de façon standardisée. Syslog est un protocole définissant un service de journaux d'événements d'un système informatique. C'est aussi le nom du format qui permet ces échanges.

Il est nécessaire de s'assurer que :

- La DSI de mon site dispose d'une cartographie de flux à jour de l'ensemble de mon site.
- Cette cartographie démontre que le cloisonnement des équipements et des services est bien pris en compte.
- La configuration du pare-feu inclue les automatismes.

2.3 Gestion des médias amovibles (BP03)

Contrôle et gestion des supports USB

Les supports externes pouvant être connectés aux prises USB de l'ULI, sont des vecteurs majeurs de propagation de virus. La maitrise et le contrôle de ces connexions sont indispensables.

Il est recommandé de m'assurer que chaque périphérique USB connecté aux appareils communicants respecte les contraintes de sécurité minimales exigées par la politique de sécurité du site.

Il est nécessaire de s'assurer :

- Que l'accès physique à l'ULI soit sécurisé. (cf BP1)
- Que les périphériques connectés sont bien exploités dans l'ULI.
- D'éviter les périphériques amovibles sur les appareils communicants.
- Dans le cas d'un usage nécessaire, vérifier les droits d'accès de ces périphériques au système (accès en lecture restrictive).

2.4 Gestion des comptes (accès logique, authentification) (BP04)

Identification et Autorisations

Cette partie traite de la gestion des mots de passe et des autorisations associées. L'identification permet de s'assurer de l'identité utilisateur. Les autorisations permettent une fois l'utilisateur identifié de lui attribuer des droits tels que la lecture et l'écriture sur le système.

Il est recommandé de :

- Définir une politique de gestion des mots de passe et d'autorisations associées.
- Supprimer les comptes avec les identifiants par défaut.
- Privilégier des mots de passe robustes (Mot de passe de 16 caractères dans un alphabet de 36 symboles).
- Changer régulièrement les mots de passe.

Il est nécessaire de s'assurer :

- Que la DSI de mon site dispose d'une politique de gestion de mots de passe définie pour mon site et que celle-ci a été mise en œuvre. Cette politique devra inclure le bannissement des mots de passe par défaut et des mots de passe faibles.
- De définir strictement les personnes autorisées sur les systèmes (Identifications et autorisations) et en réduisant au strict minimum les administrateurs.

2.5 Durcissement des configurations (système industriel) (BP05)

Renforcer la sécurité

Durcissement des configurations pour limiter la surface d'exposition aux attaques.
Mettre en œuvre toutes les actions permettant de mieux sécuriser le système.
Le fait d'ouvrir de nombreux protocoles et d'avoir plusieurs applications sur un système industriel augmente considérablement la vulnérabilité de celui-ci.

Il est recommandé :

- D'activer impérativement le HTTPS pour des accès externes. D'activer le HTTP uniquement sur une configuration sécurisée et maitrisée (Réseau Privé entre un PC et un Système Industriel).
- D'installer et d'activer uniquement les protocoles et services nécessaires.
- Dans le cas d'activation de protocoles ou de services supplémentaires de changer la configuration par défaut notamment au niveau des ports d'accès.
- Idéalement, donner accès au système uniquement et de manière ponctuelle à l'administrateur et dans les autres cas à des utilisateurs sans privilèges et sans accès aux paramètres critiques.

Il est nécessaire de s'assurer :

- De chiffrer les données et sécuriser les communications (Ex VPN).
- Que les protocoles et services vulnérables et non sécurisés ne sont pas activés.
- Que si des services ou des protocoles non sécurisés sont actifs de les répertorier pour mettre en place les mesures.
- De définir une liste Blanche/Noire des accès autorisés par IP ou Adresse Mac.

2.6 Gestion des journaux d'événements et d'alarmes (BP06)

Surveiller les systèmes et détecter les Intrusions

Le but de cette bonne pratique est de vérifier que les échanges de communication au niveau des systèmes soient conformes à la volonté d'exécution des paramétrages et des applicatifs. Pour ce faire il faut mettre en place des systèmes de suivi et de traçabilité pour pouvoir intervenir en cas de communication indésirée. Il faut également mettre en place les stratégies de stockage et de sauvegarde de ces journaux.

Il est recommandé :

- D'activer la journalisation via des protocoles tel que Syslog ou SNMP.
- De centraliser les journaux et en assurer le stockage et la sauvegarde.
- De définir une stratégie de conservation de ces journaux.

Il est nécessaire de s'assurer :

- Que l'ensemble de mes périphériques de mon site profite de la journalisation de type SysLog ou SNMP.
- Que ma DSI a bien mis en place un système de sauvegarde pour ces journaux.
- Que le stockage de ces journaux respectent le principe d'une sauvegarde 1,2,3 soit une dans le système, une dans le site et une autre en dehors du site (sauvegarde distante).

2.7 Gestion des configurations (paramétrages) (BP07)

Intégrité du paramétrage

Ce sujet porte sur les potentielles modifications malveillantes des paramétrages présents dans les systèmes.
Les modifications malveillantes peuvent être de plusieurs types: modification des utilisateurs, modification ou création de fichier par les protocoles FTP/FTPs ou encore l'exécution d'un script d'exécution interne de type Injection SQL ou JavaScript.

Il est recommandé :

- D'avoir une gestion des utilisateurs maitrisée, c'est-à-dire diminuer le plus strictement possible l'élévation des privilèges des utilisateurs ayant accès au paramétrage.(BP04)
- De s'assurer qu'aucune injection de code malveillant ne soit exécutée par les systèmes.
- De sécuriser l'accessibilité aux systèmes, que ce soit en accès physique ou via les réseaux (LAN, Wi-Fi, 3G ou 4G).
- De n'ouvrir les accès FTP et FTPs que lorsque cela est nécessaire (voir BP 05).

Il est nécessaire de s'assurer :

- Que les accès administrateurs et installateurs soient connus et divulgués uniquement aux personnes concernées.
- Que mes systèmes possèdent un contrôle d'intégrité des structures de configuration et des paramétrages.
- Que l'accès physique soit sécurisé.
- Que les accès via réseaux soient connus et maitrisés.
- Que les échanges de fichier via FTP ou FTPs soient réalisés de manière ponctuels et contrôlés.

2.8 Sauvegardes / restaurations (BP08)

Gestion des sauvegardes/restauration des paramétrages et des versions

La sauvegarde de la structure du paramétrage et des données est primordiale. Elle assure la restauration de l'installation conforme au besoin et avec le minimum de perte de données en cas de dysfonctionnements.
Les dysfonctionnements peuvent être de plusieurs types: piratage, défaillance matérielle ou encore une erreur humaine.

Il est recommandé :

- D'effectuer des sauvegardes régulières et automatisées, de la structure des programmes et des données.
- D'avoir un accès simple à ces sauvegardes horodatées, cela permet une restauration de l'installation rapide et fluide.
- Que les ULI bénéficient des dernières versions logicielles, cela permet d'avoir les dernières mises à jour de sécurité.

Il est nécessaire de s'assurer :

- Qu'au minimum les sauvegardes de la structure et des données soient réalisées automatiquement à une fréquence cohérente avec l'usage de paramétrage de l'installation.
- Que l'export et le stockage des fichiers soient réalisés à minima dans deux localisations différentes facilement accessibles et sécurisés.
- D'avoir une sauvegarde compatible avec le système d'exploitation correspondant aux équipements.

2.9 Documentation (BP09)

Existence et gestion des documentations

La maitrise de la documentation pour disposer d'une image exacte des installations permet d'éviter des erreurs d'exploitation.
Il est aussi important de maitriser la diffusion afin que seules les personnes ayant besoin des informations soient les destinataires.
Sensibiliser les utilisateurs aux risques liés à la documentation permet la maitrise de la diffusion de la documentation.
Par exemple: laisser des documents en évidence sur un bureau ou dans le coffre d'une voiture est une mauvaise pratique.

Il est recommandé :

- De disposer de tous les documents de l'installation (schéma d'architecture, schéma de raccordement, analyse fonctionnelle,…). Que leur accès soit sécurisé. (BP01)
- Améliorer l'accessibilité des documentations en les intégrants dans les équipements et sécuriser leur accès par des codes.
- Informer les utilisateurs ayant accès à ces documentations d'effectuer une diffusion uniquement aux personnes habilitées.

Il est nécessaire de s'assurer :

- Que toutes les documentations propres au site sont existantes et stockées à un endroit sécurisé.
- De sensibiliser les utilisateurs des documentations de la diffusion restreinte de celle-ci.

2.10 Protection antivirale (BP10)

Logiciel anti-virus

Protéger en priorité les équipements et applications en contact direct avec l'extérieur et les utilisateurs.
La mise en œuvre d'un logiciel anti-virus, mis à jour régulièrement est un des maillons importants dans la protection des équipements.

Il est recommandé :

- De mettre en œuvre une politique antivirale, qui permet de détecter et d'éviter l'exécution de codes malveillants.
- De Protéger particulièrement les équipements en contact direct avec l'extérieur.

Il est nécessaire de s'assurer :

- Que les antivirus soient bien actifs et que leurs bases de données soient automatiquement mises à jour.
- Si les équipements ne possèdent pas d'antivirus, l'installation peut être protégée en amont par des équipements spécialisés.

2.11 Mise à jour des correctifs (planification) (BP11)

Disposer des derniers correctifs des équipements

Les équipements doivent disposer des derniers correctifs mis à disposition par le fabricant. Il peut s'agir de correctifs liés à la cybersécurité ou au fonctionnement de ces équipements.
Il est recommandé de s'assurer de la provenance de ces correctifs.

Il est recommandé :

- D'appliquer régulièrement les correctifs publiés par les équipementiers.
- D'utiliser la connexion au serveur du fabricant pour les différentes mises à jour applicatives et systèmes.
- Pour les sites sensibles, de profiter des arrêts de maintenance pour effectuer les mises à jour.

Il est nécessaire de s'assurer :

- D'avoir qualifié ces correctifs préalablement à leur déploiement.
- Dans la mesure du possible, que les versions en exploitation sont les dernières versions publiées par le fabricant.

2.12 Protection des automates (PLC) (BP12)

Protéger les programmes automates

Sécurisation des accès logiques et physiques des équipements d'automatisation des sites.

Il est recommandé :

- De protéger l'accès aux équipements par un mot de passe.
- De protéger l'accès au code source des équipements.
- De désactiver la configuration et/ou programmation à distance.

Il est nécessaire de s'assurer :

- De définir strictement les personnes autorisées sur les systèmes (Identifications et autorisations) et en réduisant au strict minimum les administrateurs.
- De protéger l'accès aux fichiers sources par désactivation des protocoles le permettant et de sécuriser leur accès avec un chiffrage asymétrique.
- Pour les sites sensibles, sécuriser l'accès aux équipements en libérant l'accès à distance uniquement sur une plage horaire définie par l'Administrateur Système.
- Mettre en place une détection d'ouverture de l'armoire par contact sec.

2.13 Stations d'ingénierie, postes de développement (BP13)

Securisation des postes de Supervision locaux

Ces éléments constituent des points vulnérables et sont des vecteurs forts de contamination et de prise de contrôle dans un site industriel.

Il est recommandé :

- D'appliquer systématiquement les correctifs.
- D'activer systématiquement les antivirus.
- Utiliser des comptes nominatifs pour leur utilisation.
- Ne pas connecter ces postes sur d'autres réseaux que ceux dédiés aux équipements.
- Eteindre les postes ou les déconnecter du réseau de production.

Il est nécessaire de s'assurer :

- Que ma DSI a pris en compte ces équipements dans sa politique de mises à jour et de mot de passe.
- Que ma DSI a bien séparé ces équipements du réseau OT/IT (Composants Industriels / Systèmes d'Informations).

Pour tout renseignement complémentaire, notre support technique se tient à votre disposition par e-mail à hot-line@wit.fr ou par téléphone au +33 (0)4 93 19 37 30