LA CYBERSÉCURITÉ
ET LES PME MANUFACTURIÈRES

LE GUIDE

cti réseau
COMPÉTITIVITÉ
TECHNOLOGIE
INNOVATION

WWW.RESEAU-CTI.COM

Alliance INDUSTRIE DU FUTUR

Préfaces

Avec la volonté de voir renaître une France Industrielle forte, notre ambition est de profiter des progrès des technologies digitales pour accélérer la modernisation de notre outil productif, revitaliser le tissu industriel français et rendre notre territoire plus attractif à l'activité économique.

L'Alliance Industrie du futur, que j'ai l'honneur de présider depuis sa création au mois de juillet 2015, a pour mission de mettre en œuvre sur le terrain cette volonté. Les systèmes industriels et ce, de manière transversale à toutes les filières industrielles, évoluent profondément avec la diffusion du numérique et l'augmentation des communications qui l'accompagne (présence de capteurs générant des données, communications au sein et en dehors de l'entreprise, etc.).

C'est dans ce cadre que la cybersécurité est un enjeu majeur pour les entreprises industrielles.

Notre mission est de promouvoir d'avantage de continuité numérique mais cela passe par une bonne connaissance et une prévention des risques ! Car la connectivité toujours plus forte des équipements offre désormais une plus grande surface d'attaques.

La médiatisation des cyberattaques de toutes natures doit être vue comme une opportunité pour renforcer la sensibilisation, la formation et l'accompagnement de dirigeants, techniciens aux risques encourus par leurs équipements et surtout les former aux outils et réflexes à adopter dans la construction de l'architecture de son système de production.

C'est dans ce cadre, que la publication du présent guide cybersécurité à destination des PME-ETI industrielles constitue une étape importante. Après avoir décrit six grands enjeux cybersécurité de l'industrie du futur, des fiches pratiques représentent des cas pratiques de situations opérationnelles vécues par les entreprises industrielles.

Le réseau des CTI, soutenus par les experts de l'AIF, ont pris le parti pris de ne pas traiter de tous les enjeux cybersécurité, de nombreux guides didactiques existants déjà, mais de se focaliser sur les réflexes immédiats que tout entrepreneur doit prendre. Ce guide s'est également basé sur les principes et doctrines portés par l'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI) dont le rôle central tant dans la définition de la doctrine nationale mais également dans la certification des produits.

Je vous souhaite une bonne lecture !

Philippe Darmayan
Président de l'Alliance pour l'Industrie du Futur

Pourquoi les CTI se mobilisent sur le sujet de la cybersécurité pour les PME ?

Les Centres techniques Industriels – CTI - ont été créés il y a plus de 60 ans, à la demande des professions industrielles, afin d'apporter aux entreprises des moyens et des compétences pour accroître leur compétitivité, participer à la normalisation, faire le lien entre la recherche scientifique et l'industrie, promouvoir le progrès des techniques, aider à l'amélioration du rendement et à la garantie de la qualité.
Ils participent activement au développement d'une industrie moderne, innovante, du futur.

Dans ce mouvement d'innovation, les usines intègrent des technologies de plus en plus numériques (internet des objets, interconnexion des systèmes industriels, externalisation des données via le cloud ...), et le défi de la sécurité devient majeur pour les entreprises. Même les systèmes non connectés sont désormais concernés (une simple clé USB peut inoculer un virus) et certains systèmes industriels existants depuis plusieurs années s'avèrent vulnérables car développés sans intégrer de concepts de sécurité. La cybersécurité doit donc continuer à se développer dans la culture industrielle, en général, et dans celles des collaborateurs, en particulier, et ce quelles que soient leur fonction dans l'entreprise. On sait aujourd'hui par expérience que 80 % des attaques peuvent être évitées lorsqu'une entreprise a mis en place des actions simples, et la plupart de ces mesures ne nécessite pas une mise en œuvre par des experts des systèmes d'information.

Ce document de sensibilisation à la cybersécurité pour les PME, mis à votre disposition, est construit à partir de l'expérience de terrain des Centres Techniques Industriels (CTI) en contact permanent avec plus de 51 000 entreprises. Les experts de la cybersécurité de l'Alliance pour l'Industrie du Futur sont venus l'enrichir. Ce partenariat original a été coordonné par le Réseau CTI.

Le fruit de nos travaux est présenté dans ce document, qui rassemble des mesures concrètes et pragmatiques pour entrer dans une démarche de cybersécurité et progresser pas à pas.

Les CTI sont prêts à vous accompagner !

Stéphane LE GUIRRIEC
Président du Réseau CTI

Sommaire

PARTIE 1 : DÉFINITIONS, ENJEUX ET ACTIONS INCONTOURNABLES

PARTIE 2 : FICHES PRATIQUES

PARTIE 3 : GLOSSAIRE

Ce document s'inscrit en complément de guides plus techniques, et constitue une première sensibilisation à un domaine, qui peut inquiéter vu la multiplicité et les différentes formes des attaques. A chaque étape de la vie de l'entreprise et de son écosystème, les enjeux, vulnérabilités et risques autour la sécurité numérique sont décrits et des pistes de recommandations sont proposées.
Ce guide est scindé en trois parties :

Partie 1 : définition de la cybersécurité de ses enjeux dans un fonctionnement d'entreprise type et des actions incontournables à réaliser pour l'appréhender.

Partie 2 : des fiches pratiques adossées à des problématiques spécifiques.

Partie 3 : un glossaire pour mettre en lien le vocabulaire « sécurité numérique » avec les pratiques manufacturières.

Ce document s'adresse à des **chefs d'entreprise, décideurs, responsables de sites de production**, et leur permettra de :

- De mesurer les enjeux pour l'entreprise et d'en identifier les vulnérabilités spécifiques
- Sensibiliser les collaborateurs
- Se mettre en mouvement dans une démarche de cybersécurité
- Se familiariser avec le langage propre à la cybersécurité et de comprendre la portée des mots
- De faciliter le dialogue avec des prestataires de services en cybersécurité

Les CTI ont ainsi choisi de partir du fonctionnement d'une PME industrielle en décrivant **six enjeux liés à la sécurité numérique, au sein desquels seront déclinés des fiches pratiques :**

1. **Sensibiliser, former et guider les collaborateurs** (4 fiches)
2. **Garantir le fonctionnement de l'atelier / outil de production** (4 fiches)
3. **Protéger ses données d'entreprise, son patrimoine immatériel** (2 fiches)
4. **Sécuriser la relation avec les fournisseurs et sous-traitants** (1 fiche)
5. **Sécuriser la relation avec les clients** (2 fiches)
6. **Fournir des produits connectés et / ou services associés sécurisés** (1 fiche)

Ces fiches pratiques permettent au lecteur de mener une réflexion propre au fonctionnement de son entreprise, notamment dans un contexte d'intégration des nouvelles technologies IOT et numériques. Elles sont indépendantes les unes des autres et couvrent les items suivants :

- Description du thème et de ses éventuels impacts cybersécurité dans une usine
- Focus sur les principales vulnérabilités et risques associés
- Identification des risques liés au cas spécifique du lecteur par le biais de questions orientées
- Présentation de recommandations et bonnes pratiques pour aider à la mise en place d'actions pragmatiques dans l'entreprise
- Evaluation de la facilité de mise en œuvre et l'échelle de déploiement dans l'entreprise du thème traité.

Définitions enjeux et actions incontournables

Qu'est-ce que la cybersécurité pour une usine ?

La **cybersécurité** consiste à assurer que les ressources numériques d'une entreprise, qu'elles soient matérielles (ex : puce, calculateur, PC, robot, machine à commande numérique...), logicielles (ex : programmes et données), ou de communication (ex : Wifi, internet) sont préservées de toutes attaques, qui les détourneraient de leur fonctionnement initialement prévu.

Elle vise à obtenir pour les outils, les services et les données:

- **La disponibilité** (ex : l'opérateur a accès à sa machine au moment où il en a besoin, y compris quand son fonctionnement et/ou les conditions d'utilisation sont dégradés)
- **L'intégrité, c'est-à-dire la conformité** des caractéristiques par rapport à ce qui est attendu. (ex : la machine réalise l'action demandée et uniquement celle-là, y compris avec un fonctionnement dégradé
- **La confidentialité des accès** (ex : en toutes circonstances, les données clients restent confidentielles)

Le respect de ces trois items augmente le niveau de sécurité des collaborateurs/partenaires/clients des biens/outils /moyens de production et optimise la bonne marche de l'entreprise.

La cybersécurité s'intègre dans une réflexion plus globale de l'entreprise sur la sécurité, et porte plus particulièrement sur :

- Les **systèmes industriels** (ateliers, machines, plateformes, SCADA, locaux...)
- Les **systèmes d'information** (logiciels, serveurs, moyens de communication...)
- Les **produits et services** proposés aux clients

Les interfaces numériques nécessaires à la communication entre ces différents systèmes constitutifs de l'entreprise sont autant de risques supplémentaires.

La mise en pratique de mesures très simples permet d'éviter la majorité des problèmes.

Plus les entreprises numérisent leurs processus et plus les vulnérabilités augmentent. La digitalisation et la connexion des usines renforcées dans la démarche de « Industrie du Futur » imposent d'autant plus la mise en œuvre d'actions spécifiques de cybersécurité.

Pour entrer dans le sujet de la cybersécurité, il convient de distinguer les notions de :

- **Vulnérabilité** : faiblesse au niveau d'un élément d'un système industriel ou d'information. La vulnérabilité peut toucher la conception, la réalisation, l'installation, la configuration et l'utilisation. (ex : machine non protégée par mot de passe, obsolescence des systèmes)
- **Risque** : possibilité qu'une vulnérabilité conduise à un préjudice sur le fonctionnement de l'entreprise, (ex : un attaquant (menace) utilise un canal non protégé. (vulnérabilité) prend le contrôle à distance et modifie les consignes de fonctionnement)
- **Menace** : cause potentielle d'un incident, à des fins malveillantes
- **Attaque** : concrétisation d'une menace, qui nécessite l'exploitation d'une vulnérabilité. On distingue l'attaque ciblée des attaques générales (grande majorité des cas)

Les six enjeux
Cybersécurité pour des PME

Appréhender les enjeux de la cybersécurité dans une entreprise est obligatoirement une démarche globale liée au fonctionnement complet de l'entreprise et de son écosystème, et on ne peut se contenter de séparer les sujets. Pour ce faire, une approche possible est de se focaliser les six enjeux suivants, choisis par les CTI car correspondants au fonctionnement classique d'une PME.
Les six enjeux ci-dessous structurent la suite de ce document :

1 Sensibiliser, former et guider les collaborateurs

Le facteur humain est la source essentielle du risque de cybersécurité. Les menaces exploitent souvent les comportements individuels (utilisation de clé USB, liens internet et/ouverture d'emails de provenance inconnue ...), plutôt que les failles logicielles pour installer des programmes malveillants, dérober des informations confidentielles, transférer des fonds... Les risques de se faire duper par des messages malveillants sont d'autant plus forts que ceux-ci imitent de façon très fidèle des messages authentiques.

La méconnaissance par les collaborateurs des bonnes pratiques et « règles de sécurité informatique » est donc à l'origine de nombreux incidents et permet l'exploitation de vulnérabilités. **La vigilance et la sensibilisation régulière du personnel à certaines règles de base est donc indispensable.** Elle peut être complétée par des formations et la mise en place d'outils d'assistance à la mise en œuvre des bonnes pratiques.

Ce risque est amplifié avec la généralisation des outils nomades. Les frontières entre les espaces personnels et professionnels deviennent de moins en moins marquées, augmentant considérablement les vulnérabilités. Même utilisés dans un cadre strictement professionnel, ces outils engendrent de nouvelles problématiques de sécurité et nécessitent donc la mise en place de mesures adaptées.

De façon similaire, les réseaux sociaux et les messageries sont à présent largement utilisés en milieu industriel. Avec internet, ces moyens de communication exposent les entreprises à divers types d'attaques informatiques dont la pluralité et la complexité ne cessent de croître.

Le risque porté par le facteur humain concerne tous les collaborateurs dans l'entreprise (informaticiens, automaticiens, personnel administratif, personnel d'ateliers...). Il est donc nécessaire d'adapter sa campagne de sensibilisation et formation aux différents métiers de l'entreprise et de faire travailler ensemble et de manière décloisonnée les équipes autour des problématiques de sécurité.

Les règles de base doivent également être présentées et appliquées par le personnel extérieur (prestataires, intérimaire ...).

FICHES PRATIQUES ASSOCIÉES :

1 SENSIBILISER SES COLLABORATEURS

2 UTILISER DES OUTILS NOMADES, ACCES A DISTANCE

3 COMMUNIQUER VIA LES RESEAUX SOCIAUX, MESSAGERIE, INTERNET

4 BRISER LES FRONTIERES ENTRE LES DIFFERENTS SERVICES (NOTAMMENT ENTRE LES SYSTEMES INFORMATIQUES ET LES SYSTEMES INDUSTRIELS

2 Garantir le fonctionnement de l'atelier et de l'outil de production

Les outils de la transformation numérique de l'atelier et de son outil de production (IOT, Cloud, machines intelligentes, communications M2M, robots...) sont autant de sources de risques cyber, car ils créent de nouvelles vulnérabilités et de nouvelles menaces. Pour autant, même les ateliers non connectés à internet sont exposés aux menaces numériques (ex : clé USB contaminée branchée sur un équipement de production, pour sa maintenance ou le transfert de données).

Quant aux usines qui démarrent la modernisation de leurs équipements par l'intégration d'outils numérisés (ex : Retrofit de machine avec intégration du digital), elles sont sans doute les plus vulnérables car utilisatrices de systèmes et moyens développés sans intégrer de concept de sécurité.

La nécessité de disposer d'une traçabilité des données, notamment de production, implique une stratégie sécurisée de conservation et de traitement de ces informations. La donnée constitue aujourd'hui un des enjeux principaux des cyberattaques.

Enfin l'utilisation généralisée de logiciels (ERP, CAO, bureautique ...) nécessitent de mettre en place **une démarche de gestion** (sélection, mise à jour, configuration) formalisée et conforme à la politique de sécurité.

La sécurisation des accès physiques ne suffit plus à se prémunir des risques numériques dans l'usine et vices-versa.

FICHES PRATIQUES ASSOCIÉES :

- 5 GARANTIR LE FONCTIONNEMENT DES MACHINES
- 6 CONTROLER LES ACCES
- 7 MAITRISER LA GESTION ET L'ECHANGE DES DONNEES NUMERIQUES INTERNES
- 8 ASSURER LA TRAÇABILITE DE LA PRODUCTION

3 Protéger ses données d'entreprise, son patrimoine immatériel

Avec l'avènement de la dématérialisation, les savoir-faire, données d'entreprises (données de production, données sociales...), secrets industriels et expertises des entreprises se retrouvent fortement exposés aux cyberattaques et aux négligences. Il est nécessaire de préserver le caractère confidentiel de ces données sensibles qui contribuent à la valeur et à la compétitivité d'une entreprise.

La tendance à l'hébergement mutualisé des données et logiciels dans l'informatique cloud public offre de nouvelles possibilités aux PME. Les solutions ouvertes au public sont souvent des solutions de qualité (en général plus sûres que des développements « maison ») mais nécessitent une certaine vigilance. Il convient de choisir le type d'hébergement en tenant compte de son besoin en disponibilité, intégrité et confidentialité.

FICHES PRATIQUES ASSOCIÉES :

- 9 SAUVEGARDER ET PROTEGER LES DONNEES ET LOGICIELS
- 10 SERVICES EN LIGNE ET HEBERGEMENT CLOUD

4 Sécuriser la relation avec fournisseurs et sous-traitants

Le fonctionnement d'une PME nécessite dans la très grande majorité des cas le recours à des fournisseurs et sous-traitants, avec qui des données numériques seront inévitablement échangées (plans, bibliothèques de données, programmes...). Ils constituent une brèche dans la chaine de confiance numérique entre partenaires d'autant plus qu'il est difficile de connaître leur niveau véritable de cybersécurité. En effet, il peut être plus aisé pour un attaquant d'arriver à ses fins en passant par les sous-traitants, potentiellement moins protégés que l'entreprise-cible.

Toutes les données et savoir-faire de l'entreprise (programmes, données machines et/ou produits, gammes de fabrication ...) peuvent être :

- Utilisées/divulguées à mauvais escient (concurrence, ventes...)
- Modifiées et / ou détruites

Afin de conserver le niveau de sécurité informatique choisi, il est donc nécessaire pour une PME de s'assurer que ses sous-traitants répondent à des exigences de cybersécurité acceptables par rapport à celles qu'elle s'impose.

FICHE PRATIQUE ASSOCIÉE :

11 SECURISER LES DONNEES NUMERIQUES AVEC L'EXTERIEUR

5 Sécuriser la relation avec les clients

La relation avec les clients comprend à la fois :

- Les échanges financiers dématérialisés
- L'authentification du donneur d'ordre et/ou du tiers de confiance...
- La gestion numérique des documents contractuels
- Les services d'e-commerce (ex : catalogues et ventes en ligne)

La dématérialisation des paiements réduit les risques d'erreur et simplifie les procédures comptables : elle est donc devenue incontournable. Dans ce contexte, les tentatives de fraudes par « ingénierie sociale » s'intensifient dans les entreprises. A titre d'exemple, les collaborateurs sont contactés par un fraudeur se faisant passer pour l'un de leurs responsables hiérarchiques (« fraude au président »), aisément identifiable grâce aux informations mises en ligne par l'entreprise elle-même, et qui demande un ordre de virement outrepassant les procédures usuelles de vérification et autorisations.

La dématérialisation des contractualisations requiert également des moyens adéquats tels que les signatures électroniques à valeur légale. L'archivage des documents comptables et financiers dématérialisés doit par ailleurs répondre aux normes en vigueur (NF Z 42-013 ou ISO 14641-1).

Le recourt au commerce en ligne n'est plus réservé aux particuliers. Les plateformes de ventes de pièces et équipements manufacturés gérées en direct par les entreprises sont de plus en plus courantes. Toutes les informations contenues dans les catalogues mis en ligne peuvent être modifiées et/ou détournées.

FICHES PRATIQUES ASSOCIÉES :

12 SECURISER LES DOCUMENTS OFFICIELS ET ENGAGEMENTS CONTRACTUELS

13 MAITRISER LES FLUX FINANCIERS ET COMMANDES DEMATERIALISEES

6 Fournir des produits connectés et/ou services connectés sécurisés

Les objets connectés sont devenus omniprésents et sont par nature exposés aux risques liés à la cybersécurité. Ces risques sont variés et concernent aussi bien le vol de données sensibles et l'espionnage industriel que le sabotage d'objets physiques La vente de produits connectés (ex : chaudière, domotique) ou de services associés (suivi à distance du bon fonctionnement d'une pompe par exemple) nécessite donc la mise en place de mesures de sécurité permettant de protéger les clients, les tiers et l'entreprise qui a mis ces produits sur le marché.

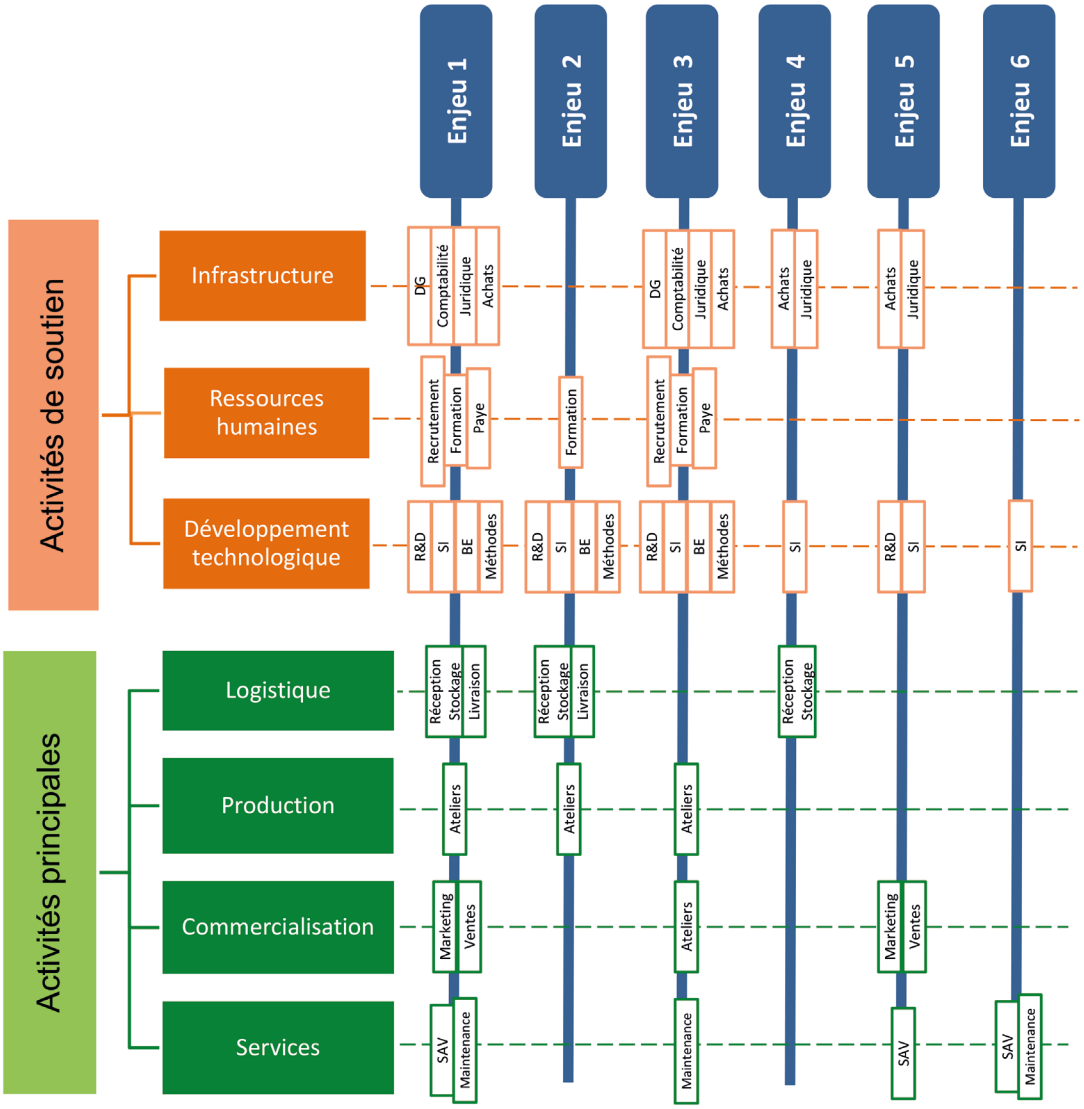
La mise en œuvre de ces mesures est en particulier compliquée par la diversité des protocoles d'échange utilisés. Les problèmes d'interopérabilité ne doivent pas amener à diminuer les exigences de cybersécurité. La mise sur le marché d'objets connectés doit faire l'objet d'une vigilance particulière sur l'intégration d'un certain degré de cyber sécurité sur la conception du produit en vue de son utilisation. Ex. : dispositifs de surveillance médicale.

FICHES PRATIQUES ASSOCIÉES :

14 SECURISER LES PRODUITS ET SERVICES CONNECTES

La cybersécurité : tous concernés !

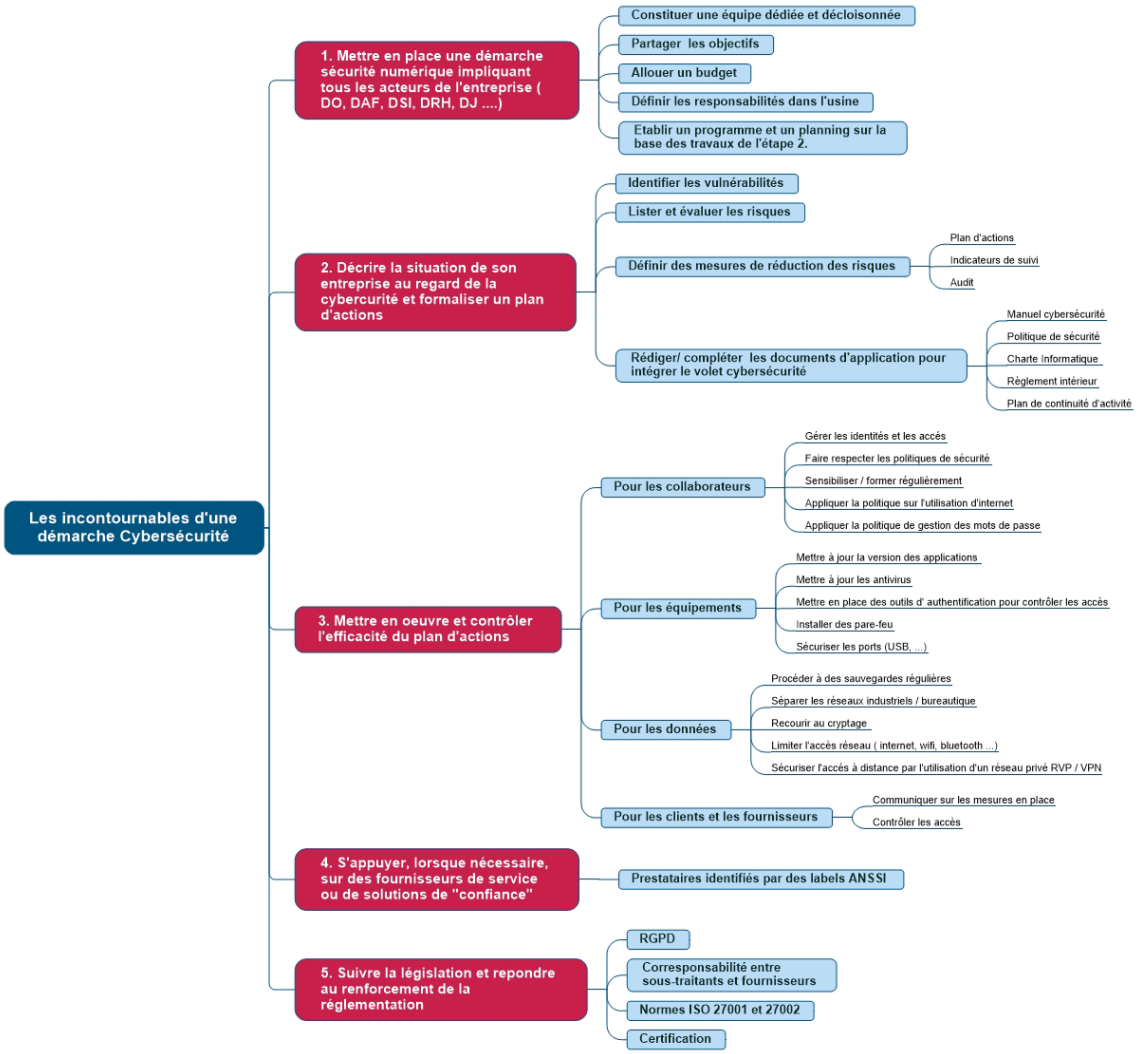
Ces six enjeux impactent le fonctionnement de l'entreprise à tous les niveaux et dans les différents services. Le schéma ci-dessous liste les principales équipes impactées :



Les actions incontournables pour appréhender la cybersécurité dans son entreprise

Afin d'être en mesure de protéger son entreprise (collaborateurs, système de production, systèmes d'informations, ...) de tous types d'attaques, il est primordial, quelle que soit sa taille et son degré d'intégration des outils digitaux et d'exposition à internet, d'établir une **politique de sécurité adaptée à son environnement et à son contexte industriel.**

Les cinq items incontournables pour intégrer la cybersécurité dans son entreprise sont décrits ci dessous. Des recommandations d'actions concrètes sont listées pour chacun d'eux. Elles devront être complétées par l'application des fiches pratiques de la partie 2, en fonction des spécificités et besoins de chaque entreprise.



Pour le deuxième item de cette démarche, il est nécessaire de décrire la situation actuelle de l'entreprise au regard de la cybersécurité, et pour ce faire une phase de diagnostic est indispensable.

L'Alliance Industrie du Futur travaille sur le développement d'un outil spécifique de diagnostic dédié à la cybersécurité des usines dans leur globalité. Il devrait être disponible en 2018.

Il existe néanmoins un outil qui permet de tester son niveau global de sécurité DIESE, disponible sur le site du Ministère de l'Economie (Direction Générale des Entreprises).

DIESE (Diagnostic d'intelligence économique et de sécurité des entreprises) est un outil gratuit. Il ne requiert que vingt minutes pour être rempli, et son utilisation à intervalle de temps régulier permet de noter les progrès apportés. Conçu sous Excel (acceptant les macros), il s'utilise hors connexion pour une meilleure sécurité et se compose d'un questionnaire de 83 items. Il fournit une évaluation sous une forme graphique.

Le lien d'accès à cet autodiagnostic est le suivant :

http://www.entreprises.gouv.fr/information-strategique-sisse/outils.

Enfin, comme pour d'autres démarches globales dans l'entreprise, il revient à chaque entreprise de définir le bon niveau entre les contraintes liées à la sécurité et sa productivité.

Responsabilité de l'entreprise

De manière générale, les entreprises sont soumises à deux régimes de responsabilité :

- **Une responsabilité civile** (article 1384 alinéa 5 du code civil): l'employeur est civilement responsable du fait de l'activité de ses collaborateurs, notamment en cas d'utilisation malveillante des moyens informatiques et de communications électroniques.
- **Une responsabilité pénale** (article L. 121-2 du code pénal) : l'employeur peut être pénalement responsable du fait de ses collaborateurs dès lors qu'ils commettent des infractions susceptibles d'engager la responsabilité pénale des personnes morales (ex : atteinte aux systèmes de traitement automatisé de données, contrefaçon...) et qu'elles ont été commises pour le compte de l'entreprise par ses « organes ou représentants ».

Dans le cadre de l'évolution réglementaire, il devient nécessaire de mettre en place des mesures de protection.

En particulier, Le Règlement Général sur la Protection des Données **(RGPD)** ou General Data Protection Regulation **(GDPR)**, qui en France se substitue à la loi informatique et liberté, implique que le chef d'entreprise doit respecter des exigences de protection des données à caractère personnel manipulées au titre de l'activité d'entreprise (ex : données clients, données sociales...). Ce règlement européen entrera en vigueur le 25 mai 2018.

L'aspect réglementaire autour de la cybersécurité est en pleine évolution, et il conviendra de se tenir régulièrement informé.

Sources d'informations

La cybersécurité étant devenue un sujet clef, de nombreuses sources sont disponibles pour s'informer et effectuer des actions de veille. Nous citons ci-après les acteurs de référence :

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est le référent national de l'Etat. Elle gère en particulier l'élaboration des procédés et des règles nécessaires à la protection des systèmes d'information de l'État et contrôle l'application des mesures adoptées au préalable. Elle a également un rôle de conseil et de soutien envers différents organismes avec notamment la publication de guides de bonnes pratiques. Deux publications de l'ANSSI sont particulièrement intéressantes en complément de ce document : la cybersécurité des systèmes industriels et le guide de l'hygiène informatique. Site internet :

http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/

Le CERT-FR (Computer Emergency Response Team) est une équipe constituée pour réagir aux incidents informatiques. Il existe plusieurs CERT en France et chaque CERT a son domaine d'application. Les CERTS centralisent les demandes d'assistance suite aux incidents de sécurité sur les réseaux et systèmes d'information, et jouent un rôle de prévention par diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident. Il a par exemple publié « Les bons réflexes en cas d'intrusion sur un système d'information », avec des mises à jour annuelles depuis 2002. Site internet :

https://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/les-cert-francais/

L'AFNOR (Association Française de NORmalisation) est l'organisation française représentant la France auprès de l'Organisation Internationale de Normalisation (ISO) et du Comité Européen de Normalisation (CEN). Cette association, sous l'égide de la DIRECCTE Centre, a coordonné une action collective qui a abouti à la rédaction d'un *« Guide de bonnes pratiques pour l'élaboration d'un Plan de Continuité d'Activité (PCA) »*. Ce guide a pour cible les PME et ETI, encore peu nombreuses à élaborer une stratégie de sécurisation de leurs systèmes informatiques notamment en cas de sinistre ou d'une cyberattaque. Elle a également rédigé un *« Guide de protection des données personnelles : l'apport des normes volontaires »* afin d'éviter les problèmes de fichier perdus et d'anticiper la nouvelle réglementation européenne sur la protection des données personnelles et des outils qui entrera en application en mai 2018.
Site internet :

http://www.afnor.org/dossiers-thematiques/numerique/

La Commission Nationale de l'Informatique et des Libertés (CNIL) conseille et renseigne les organismes qui souhaitent mettre en œuvre des fichiers informatiques. La CNIL apporte des réponses aux questions des professionnels grâce à son service d'orientation et de renseignement. Elle publie également des guides et fiches pratiques, comme le guide *« La sécurité des données personnelles ».*
Site internet :

https://www.cnil.fr/fr/thematique/internet-technologies

Le CLUSIF est une association de professionnels de la sécurité qui a pour mission principale la favorisation des échanges d'idées et des retours d'expériences dans le but de mettre en place la cybersécurité la plus efficace et opérationnelle possible pour les entreprises et des collectivités locales.
Site internet :

https://clusif.fr/publications/

Fiches pratiques

Sensibiliser ses collaborateurs

Les aspects numériques sont prépondérants dans l'Industrie du Futur, mais la numérisation et la connectivité des machines font naître de nouveaux dangers dont il faut se prémunir.

Une grande partie des incidents liés à la cybersécurité provient de la méconnaissance des collaborateurs concernant les risques sur les installations. Leur sensibilisation aux bonnes pratiques contribue donc à la réduction des vulnérabilités et des opportunités d'attaques.
Les risques évoluant en permanence, cette sensibilisation doit être effectuée de manière régulière.

Vulnérabilités et risques associés

La gamme de services en ligne qu'une PME peut solliciter est très vaste. Il est possible de façon simplifiée de les regrouper comme suit :

- Négligences internes, à cause d'un manque de formation et/ou d'informations
- Demande de rançon
- Usurpation d'identité (Fraude au président)
- Propagation de virus (ou vers)
- Déni de service (voir lexique
- Paralysie de tout ou partie de l'outil de production, et des services de l'entreprise
- Mise sur le marché de produits défectueux
- Mauvaise communication entre les collaborateurs
- Le manque de mise à jour d'un utilitaire anti-virus crée une vulnérabilité faisant courir une multitude de risques potentiels.

Les questions à se poser pour identifier les risques

- Peut-on identifier rapidement un problème de connexion à une machine de l'atelier ?
- Peut-on identifier un comportement anormal d'une machine ?
- Peut-on savoir si des fichiers ont disparu ? ou si un système de fichiers est endommagé ?
- Comment savoir si des connexions ou activités inhabituelles ont lieu ?
- Comment vérifier s'il y a eu création ou destruction de comptes ?
- Gère-t-on bien les messages d'alerte des pare-feu et applications antivirus ?

FICHE PRATIQUE

Sensibiliser ses collaborateurs

N°01

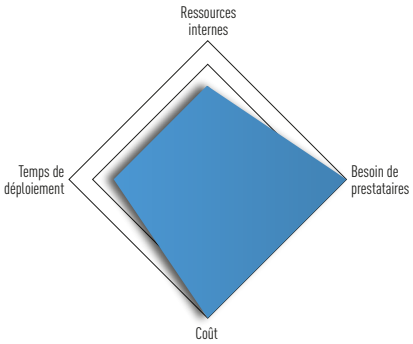
Recommandations, bonnes pratiques

- Former un ou plusieurs référents internes en cybersécurité
- Mettre en place une charte de bonne conduite et la faire appliquer dans l'entreprise
- Mettre en place un calendrier de formation et de sensibilisation pour l'ensemble du personnel (cybersécurité et sécurité du site)
- Ne jamais faire confiance à un tiers inconnu, sans vérifier la réalité de son identité par des justifications complémentaires, notamment pour la messagerie, le téléphone et la maintenance du réseau informatique
- En particulier, ne pas ouvrir les pièces jointes quand l'expéditeur n'est pas connu ou quand le sujet n'est pas cohérent avec l'expéditeur
- Bien gérer les identifiants d'accès en les renouvelant fréquemment, notamment pour les accès nomades
- Interdire les installations de logiciels sans autorisation préalable et supprimer toutes les applications non utiles à l'activité de chaque poste
- Désactiver ou enlever les comptes par défaut, les ports physiques (USB...) inutilisés, les supports amovibles non utiles, les services web non indispensables
- Maîtriser les outils de programmation, développement et débogage des systèmes de production
- Éviter d'utiliser les systèmes de supervision de terrain de l'outil de production comme terminal bureautique ou lecteur PDF
- Mettre en place un processus de veille pour rester informé de l'évolution des menaces, des techniques d'attaque et des mécanismes de protection
- Faire une sauvegarde régulière des données et logiciels sur des supports séparés
- Mettre à jour les systèmes d'exploitation et applications de sécurité à chaque évolution

Les sources d'informations utiles sont :

- **« Maîtriser la SSI pour les systèmes industriels - ANSSI »,** https://www.ssi.gouv.fr/uploads/ IMG/pdf/ Guide_securite_industrielle_ Version_ finale-2.pdf
- **« Bâtir une politique de sécurité – Fiche 1, MEDEF »,** https://repo.zenk-security.com/Guide SSI/ Guide SSI Batir une politique de securite.pdf
- **« Sensibilisation du personnel – Fiche 4, MEDEF »,** https://repo.zenk-security.com/Guide SSI/ Guide SSI Sensibilisation du personnel.pdf

Facilité de mise en œuvre



Utiliser des outils nomades, accès à distance

L'Industrie du Futur repose sur une mise à disposition et une utilisation en temps réel de l'information, pour décider, voire pour agir sur le système d'information ou sur un composant de l'outil de production. L'accès à distance, que ce soit pour gérer des opérations de production ou pour la télémaintenance repose sur des outils dits nomades tels que les smartphones, les ordinateurs portables ou les tablettes. Ces moyens sont généralement mis à disposition par les entreprises, mais l'on commence à voir apparaître des usages professionnels d'outils nomades personnels.

Vulnérabilités et risques associés

Les risques importants d'intrusion et de malveillances reposent principalement sur deux vulnérabilités potentielles qui sont **la connexion et la perte / ou le vol :**

- La prise en main d'une machine par un tiers malveillant dans un but de sabotage, de rançonnage ou d'autres malveillances
- Le contrôle d'accès à distance avec authentification insuffisamment protégée permettant une intrusion dans le système informatique de l'entreprise
- Le vol ou la perte d'informations pouvant retarder la sortie d'un nouveau produit/-service ou renseigner un concurrent
- La prise de commande à distance d'un moyen de production pouvant conduire à l'arrêt de l'atelier
- Les négligences dans la gestion et l'utilisation des moyens nomades par manque de formation et de formalisation de procédures
- L'absence de responsabilité identifiée, une sous-traitance de la gestion de parc informatique mal maîtrisée
- La possibilité de mise en danger de la population et/ou de l'environnement si le stockage et/ou l'utilisation de produits dangereux sont à la maîtrise à distance d'un tiers malveillant

Les questions à se poser pour identifier les risques

- Y-a-t-il une bonne identification de tous les outils nomades qui sont déployés dans l'entreprise ?
- Suis-je assuré que ces outils nomades sont liés à un meilleur niveau de sécurité ? (comme le fait de chiffrer le contenu des téléphones portables, d'utiliser une double authentification pour accéder aux systèmes de l'entreprise, d'assurer la mise à jour du parc nomade malgré des connexions intermittentes, ...) ?
- L'entreprise est-elle à même de révoquer efficacement les autorisations données à un équipement (en cas de vol par exemple) ou à une personne (en cas de départ de l'entreprise par exemple) ?
- Mes services des protections et gestionnaires de mots de passe sont-ils à jour ?
- Le personnel connait-il les risques encourus lors de la perte ou du vol d'un outil nomade ?
- Est que je connais exactement les informations qui sont sur les téléphones ou les tablettes et qui sont critiques pour l'entreprise ?
- Ai-je bien évité d'enregistrer mes codes d'accès sur l'ensemble de mes outils nomades ?
- Ai-je paramétré complètement l'effacement de mon historique de navigation, y compris pour les mots de passe ?
- Comment être sûr qu'un collaborateur n'utilise pas ses propres outils ?

FICHE PRATIQUE

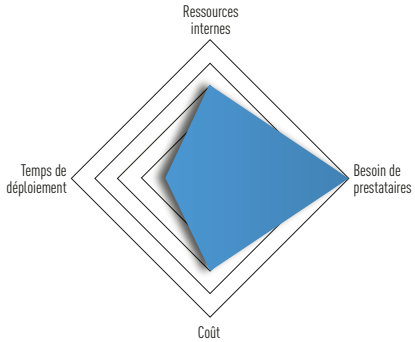
Utiliser des outils nomades, accès à distance

N°02

Recommandations, bonnes pratiques

- Faire superviser la gestion du parc des outils nomades e par un responsable gestionnaire et rédiger une procédure en cas de perte ou de vol
- Envisager de mettre en place un gestionnaire de mots de passe
- Paramétrer complètement l'effacement de l'historique de navigation
- Gérer les portes d'entrée des outils nomades, accès uniquement à des VPN (Virtual Private Network) utilisant des technologies TLS (Transport Layer Security) ou IPSec (Internet Protocol Security)
- Mettre en place des outils et services permettant le verrouillage à distance et en-cas extrêmes de l'effacement à distance des données
- Sécuriser les points d'accès, les clients Wi-Fi et le compte administrateur et utiliser une liste d'accès d'appareil autorisés
- Etendre et compléter les services de sécurité déjà déployés sur le réseau filaire (exemple par VPN, firewall...)
- Informer et former spécifiquement les utilisateurs sur les points suivants : pour les appareils en mobilité, les fonctions de liaison sans fil Wi-Fi doivent être désactivées par défaut et réactivées pour un usage ponctuel
- Surveiller le réseau : surveillance de l'IP avec un système de détection d'intrusions classique et surveillance au niveau physique (sans fil) avec des outils dédiés
- L'usage des périphériques personnels quels qu'ils soient (téléphones, tablettes, clés USB, appareils photos, etc.) devrait être interdits ou en tous cas, une politique d'usage doit être formulée
- Ne faire des opérations de télémaintenance qu'à l'aide de protocoles sécurisés assurant notamment l'intégrité et l'authenticité des échanges
- Dans le cas d'une connexion par modem n'offrant pas de système d'authentification robuste, a minima un système de rappel (call-back) pour valider le numéro de téléphone appelant

Facilité de mise en œuvre



Communiquer via les réseaux sociaux, messagerie, internet

La visibilité, le développement économique des entreprises et leur attractivité en matière de méthodes de travail, notamment pour les « digital natives » reposent sur une utilisation massive d'internet, des messageries et des réseaux sociaux, tant mondiaux (Facebook, Twitter) que privés, circonscrits au périmètre de l'entreprise. Cette multiplication des outils numériques de communication au bureau et dans l'usine, conjuguée à l'utilisation croissante des messageries professionnelles à des fins personnelles font exploser les risques cyber sur le lieu de travail.

Vulnérabilités et risques associés

- Le « Spoofing » ou usurpation d'identité, consiste à se faire passer pour quelqu'un d'autre via des sites miroirs contrefaits semblables à des portails de renom.
- L'usurpation d'identité peut conduire à ruiner votre image de marque sur les réseaux sociaux, à enclencher des ordres financiers (fraude au président).
- L'absence de sensibilisation des employés aux dangers liés à l'utilisation de l'Internet en général est préjudiciable. La question n'est pas de savoir si une attaque va avoir lieu, mais quand.
- L'absence de règles sur l'utilisation de la messagerie, l'absence de charte informatique avec des points clairs et documentés laisse la porte ouverte à tous les abus.

Les questions à se poser pour identifier les risques

- Ai-je organisé des séances d'information auprès des collaborateurs, et ma campagne de communication sur la cybersécurité est-elle efficace ?
- Ai-je besoin d'une aide extérieure pour auditer et améliorer les bonnes pratiques et la politique RH en matière de cyber sécurité de mon entreprise ?
- Comment puis-je inciter les collaborateurs à moins (ne pas) utiliser les outils de communication de l'entreprise à des fins personnelles, en conformité avec les règlements de protection des données personnelles et la Loi Travail (2017) ?

FICHE PRATIQUE

Communiquer via les réseaux sociaux, messagerie, internet

N°03

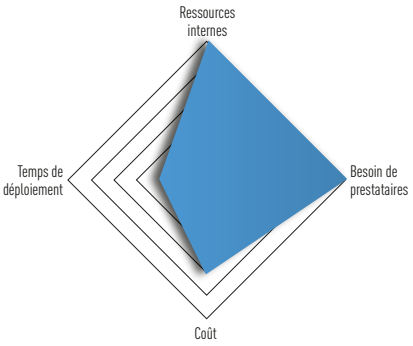
Recommandations, bonnes pratiques

- Ne jamais ouvrir un fichier attaché d'un mail de provenance inconnue
- Faire en sorte que les accès ne se fassent qu'avec des VPN (Virtual Private Network) utilisant des technologies TLS (Transport Layer Security) ou IPSec (Internet Protocol Security)
- Couper physiquement les moyens connectés s'ils ne sont pas utilisés
- Pour toute information sensible, adopter le cryptage des données dans la messagerie ou utiliser des services de messagerie sécurisés, associés à des certificats de signature électronique
- S'assurer des identifications, authentifications et autorisations
- Former les collaborateurs à définir des mots de passe complexes
- Interdire la mémorisation des mots de passe dans les moyens connectés
- Définir une procédure sécurisée de réinitialisation des mots de passe en cas de perte
- Interdire le téléchargement de logiciels non répertoriés par l'entreprise
- Limiter le nombre de personnes pouvant publier sur les comptes des réseaux sociaux de l'entreprise
- Sensibiliser les collaborateurs aux impacts de leurs communications personnelles relatives à l'entreprise (photos et informations)

Les sources d'informations utiles sont :

- **« Mettre en œuvre des moyens appropriés à la confidentialité des données – Fiche 3, MEDEF »,** https://repo.zenk-security.com/Guide SSI/Guide SSI Mettre en oeuvre des moyens appropries a la confidentialite des donnees.pdf
- **« Mesures de prévention relatives à la messagerie »,** https://www.cert.ssi.gouv.fr/information/CERTA-2000-INF-002/
- **« Les mots de passe »,** https://www.cert.ssi.gouv.fr/information/CERTA-2005-INF-001/

Facilité de mise en œuvre



Briser les frontières entre les différents services (notamment entre les systèmes informatiques et les systèmes industriels)

Nous avons vu que pour faire face aux nouveaux cyber-risques, la sensibilisation des collaborateurs est obligatoire. Mais il n'est pas rare, en PME, de voir cohabiter des mondes différents liés d'une part à **l'informatique de gestion, d'autre part à l'informatique industrielle, voire à l'automatique.** Pour réussir une campagne de communication sur la cybersécurité, il va être nécessaire de construire un langage commun. Pour ce faire, les différents mondes du digital doivent se décloisonner.

Vulnérabilités et risques associés

Les vulnérabilités proviennent essentiellement des passerelles entre l'informatique de gestion et l'informatique industrielle, ainsi que l'absence d'une vision totale du cycle de vie des informations, de la gestion à la machine de production, sans oublier la destruction au bout d'un certain temps (suivant le produit/-service et/ou la législation).

- En cas d'attaque, l'informatique de gestion pourrait prendre la décision de couper les flux d'informations conduisant certaines parties de l'outil de production à avoir des comportements inadaptés, voire dangereux
- La pluralité des automates, concentrateurs et autres terminaux d'atelier contribue à augmenter les vulnérabilités
- L'absence d'une maîtrise commune de l'ensemble des langages numériques peut entraîner des vulnérabilités (langage à contacts, grafcet, technologies web, etc...)
- Le cloisonnement entre les services techniques (ordonnancement, production, maintenance, approvisionnement, ...) et les services de gestion (planification, commercial, comptabilité,...) ne peut conduire qu'à un manque de compréhension des vulnérabilités de chacun et surtout une réaction désorganisée de type panique en cas d'attaque
- Une campagne de sensibilisation mal préparée, c'est-à-dire qui ne tient pas compte des spécificités de chaque métier interne de l'entreprise, peut conduire à des comportements contraires à ceux attendus et avoir des conséquences négatives pour l'entreprise

Les questions à se poser pour identifier les risques

- Mon organisation n'est-elle pas trop cloisonnée ?
- Est-ce que je connais la disparité de mon parc numérique (tous appareils confondus) ?
- Ma charte informatique est-elle cohérente avec la pluralité des métiers internes à mon entreprise ?
- Est-ce que chacun sait quoi faire en cas d'attaque ?

FICHE PRATIQUE

Briser les frontières entre les différents services

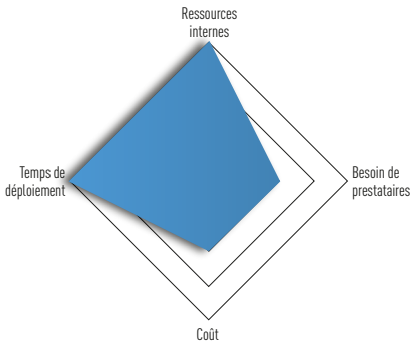
(notamment entre les systèmes informatiques et les systèmes industriels)

N°04

Recommandations, bonnes pratiques

- Pour réussir la sensibilisation à la cybersécurité :
  - Faire un état des lieux des différents composants numériques de l'entreprise
  - Faire un état des lieux des connaissances de chacun sur l'utilisation, la programmation, la communication, les faiblesses et accès de chacun des composants
  - Construire un plan de formation avec des intervenants extérieurs en fonction des résultats obtenus, et de l'utilité pour chacun d'obtenir tel ou tel état de connaissances (utilité métier)
- Créer un groupe de travail multi-métiers, avec par exemple, un automaticien, un informaticien, des utilisateurs (gestion, production, maintenance, ...) et mettre en œuvre les actions incontournables cybersécurité telles que décrites dans la partie 1 de ce guide. Un intervenant externe est recommandé
- Faire construire au groupe de travail un plan minimum de continuité d'activité en cas d'attaque sur la base d'une analyse de risques. Un intervenant extérieur est souhaitable
- Former les personnes directement impactées par le plan de continuité
- Réunir le personnel (par groupes, suivant le nombre) pour procéder à la présentation du plan de communication et du plan de continuité. Distribuer les documents
- Introduire les plans dans le règlement intérieur
- Introduire les plans dans le livret d'accueil des nouveaux arrivants (embauche, intérimaires, ...)
- Introduire les consignes minimales dans le document contractuel d'intervention de toutes sociétés extérieures pouvant intervenir dans les locaux de l'entreprise

Facilité de mise en œuvre



FICHE PRATIQUE

Garantir le fonctionnement des machines

Un atelier de production est composé d'une multitude de moyens de transformation, de manutention et de périphériques. Ces machines sont de plus en plus :

- à commande numérique (ex : programmation via des interfaces homme/machine, ..),
- instrumentées (par ex : capteurs permettant de mesurer et exploiter des données recueillies à des fins de maintenance prédictives),
- connectées et communicantes, au travers soit de réseaux M2M (Machine to Machine), soit par IOT.

Toutes les machines et robots sont directement ou indirectement connectés à des réseaux et en particulier à l'internet. Ces équipements peuvent souvent accueillir des clés USB ou des consoles de maintenance. Il est donc nécessaire de protéger ses machines. La sécurité de celles-ci ne peut se résumer à des parades logicielles et matérielles visant à repérer et à éradiquer des codes malveillants. Elle doit garantir également la fiabilité du transfert d'informations intégrées entre les différents équipements.

Vulnérabilités et risques associés

- Pour les **fonctionnalités de premier niveau (systèmes de production simples)** : vulnérabilités des capteurs/actionneurs, entrées/sorties déportées, automates, pupitres, systèmes embarqués, analyseurs, ... Les risques sont de bloquer tout ou partie d'une machine, de modifier son comportement par la modification d'informations, etc...
- Pour les **fonctionnalités de second niveau (systèmes de production complexes)** : vulnérabilités des stations de supervision, serveurs d'historique local, bases de données locales, ... Les risques les plus importants sont de perdre toutes les informations relatives à un groupe de machines, provoquant l'arrêt de l'unité de fabrication.
- Pour les **fonctionnalités de troisième niveau (systèmes de production très complexes) :** vulnérabilités des systèmes intégrant des consoles de programmation, des stations d'ingénierie connectées en permanence, des systèmes connectés à d'autres dédiés à l'exécution des fabrications, des bases de données centralisées, ... Les risques vont de la prise en main à distance par un tiers malfaisant pouvant amener à la destruction d'une partie de l'atelier, à modifier la planification de fabrication, à faire accepter des pièces non conformes, jusqu'à la perte complète des bases de données ou leur cryptage en vue d'obtenir une rançon.

La vulnérabilité des composants IOT qui intègrent la mécatronique ou des composants électroniques dans les sous-ensembles ou machines peut être due à quelques failles classiques de type :

- Mises à jour non sécurisées
  → Téléchargement de mises à jour sans signature authentifiée de l'émetteur
- Utilisation des clés par défaut
  → Dans les protocoles de communication, on garde les valeurs par défaut connues de tous
- Pas de chiffrement des communications
  → Les fournisseurs de réseaux de communication de l'internet des objets ne proposent pas de chiffrement dans l'offre de base
- Stockage de données non sécurisé
  → De nombreux composants conservent des données personnelles non prévues dans l'application d'origine

Les risques associés principaux sont :

- Possibilités de propagation de virus, de « vers »
- Possibilités d'attaques distribuées
- Possibilités d'accès à distance
- Livraison de pièces non conformes
- Une attaque grave d'un atelier de production peut conduire à l'arrêt de l'activité et nuire à l'économie de l'entreprise et plus largement de son écosystème.
- Si l'atelier utilise ou produit des substances nocives pour les hommes et l'environnement, les conséquences sanitaires et écologiques d'une attaque peuvent être désastreuses.

FICHE PRATIQUE

Garantir le fonctionnement des machines

N°05

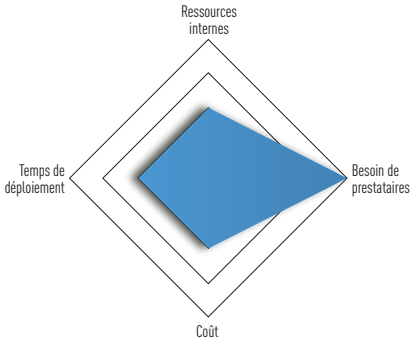
Les questions à se poser pour identifier les risques

- Est-ce que l'architecture physique et numérique de mon site de production est connue, formalisée ?
- Est-ce qu'une analyse de risque a été pratiquée (ou un audit avec un intervenant extérieur possible) pour chaque niveau de fonctionnalité et chaque point d'interconnexion (USB, réseaux, ...) ?
- Est-ce que ma politique de sécurité est à jour (le danger évoluant sans cesse) et intègre bien l'atelier de production?

Les sources d'informations utiles sont :

- **« Méthode de classification et mesures principales, ANSSI »,** https://www.ssi.gouv.fr/uploads/2014/01/securite_industrielle_GT_methode_classification-principales_mesures.pdf
- **« La cybersécurité des systèmes industriels, ANSSI »,** https://www.ssi.gouv.fr/uploads/IMG/pdf/Guide_securite_industrielle_Version_finale.pdf

Facilité de mise en œuvre



Recommandations, bonnes pratiques

- **Contrôler les accès :**
  - Remplacer systématiquement les mots de passe par défaut par des mots de passe personnalisés. Des matériels offrent la possibilité de configurer un accès en lecture seule pour les interventions de maintenance de premier niveau
  - Protéger les accès physiques et numériques aux stations de développ ement SCADA, consoles de programmation automate, terminaux portables (PDA, Pocket PC par exemple), écrans tactiles, capteurs et actionneurs dits intelligents
  - Établir une cartographie des flux d'information, filtrer les flux au moyen de pare-feu, tracer et analyser les échecs de connexion

- **Séparer les réseaux**
  - Vérifier que les réseaux sont bien séparés (bureautique, ateliers, etc...)
  - Séparer autant que possible les connexions entre les îlots de production.
  - Effectuer une coupure physique totale des équipements non utilisés

- **Prêter attention aux configurations par défaut ou fonctionnalités inutilisées :**
  - Désactiver les modes de configuration et/ou de programmation à distance lorsque la fonctionnalité existe
  - Éviter les choix proposés par défaut, incluant les mots de passe.
  - Désactiver systématiquement les protocoles et fonctionnalités vulnérables et non sécurisés (serveur Web, NetBios, FTP,...)
  - Désactiver les modes de configuration et de programmation à distance sur les installations critiques. Sur les automates, ce mode se configure parfois par un commutateur physique sur le CPU
  - N'installer que les logiciels nécessaires. Pas d'outils de développement sur des serveurs de production ou stations opérateur
  - N'installer ou n'activer que les protocoles et services nécessaires. Les uniformiser

- Appliquer systématiquement tous les correctifs et mises à jour des logiciels

Contrôler les accès

La connexion à internet n'est malheureusement pas le seul vecteur de malveillance potentielle ou même de négligence. Un simple port USB accessible facilement peut devenir la porte d'entrée d'une cyberattaque.
De très nombreux intervenants ont cependant besoin de pouvoir accéder physiquement aux installations. Des mesures adaptées permettant de maîtriser les points d'accès physiques, qui permettraient de s'introduire dans le système, doivent donc être mises en place. Elles concernent en particulier tous les équipements informatiques, les ateliers ou parties d'atelier sensibles, les salles d'archivage, etc...

Vulnérabilités et risques associés

- Deux points essentiels liés au contrôle des accès sont :
  - → Les accès physique aux infrastructures, qui peuvent déjouer toutes les préventions cybersécurité.
  - → Des équipements d'apparence anodine notamment USB (clé USB, clavier USB, souris USB...) peuvent être des vecteurs d'intrusion souvent insoupçonnés.
- Chaque accès physique non sécurisé est une vulnérabilité pouvant entraîner tous les types de risques possibles. Par exemple, un accès sur un port de communication (comme USB) effectué par une personne non compétente peut engendrer des mauvaises configurations de l'outil de production et créer d'autres vulnérabilités. Ce même accès effectué à des fins malveillantes peut amener à l'injection de virus, l'espionnage d'informations comme la configuration des machines, la modification des configurations pour réduire le rendement, voire détruire le système de production. Un accès direct aux machines permet d'imaginer toute sorte de manipulation, comme le vol des disques durs ou la machine elle-même, la destruction de la machine.
- Chaque possibilité d'accéder en direct au système d'information forme une vulnérabilité conduisant à des risques majeurs pour l'entreprise. Ces risques sont les mêmes que ceux décrits dans la fiche pratique n°2 concernant l'accès à distance.
- En cas de permissivité non contrôlée d'accès aux différents points névralgiques de l'entreprise, celle-ci se trouve en grand danger car elle peut ne plus être en mesure d'assurer le volume de production pour son équilibre économique. Les conséquences financières peuvent amener la société à disparaître.
- Une stratégie sans gestion des accès peut entraîner un manque de confiance des utilisateurs dans l'utilisation des outils de production, la perte de responsabilisation des utilisateurs compétents en charge de garantir le bon fonctionnement.
- Les accès non sécurisés peuvent mettre en danger la survie de l'entreprise mais peuvent conduire aussi à des conséquences humaines et écologiques désastreuses.
- Le manque de politique de gestion des accès peut impacter la sécurité des personnes et des bâtiments et ne plus être en règle

Les questions à se poser pour identifier les risques

- Quels sont les accès physiques qui peuvent mettre en danger mon entreprise (SI, atelier, produits, matières, ...) ?
- Est-ce que mon niveau de protection, comme le contrôle d'accès et le monitoring est adapté ?
- Est-ce que mes procédures et ma politique de sécurité sont adaptés lorsqu'une intervention extérieure est nécessaire : dépannage d'une machine, nettoyage des locaux, etc... ?

FICHE PRATIQUE

Contrôler les accès

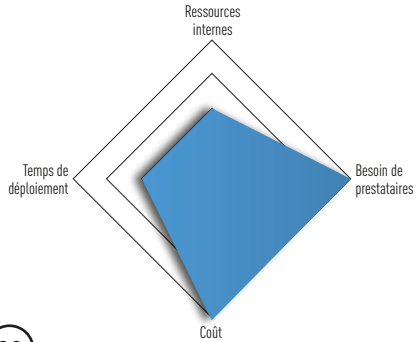
N°06

- **Protection des locaux :**
- Définir les règles d'accès aux locaux, avec le nom des personnes habilitées et leur période d'accès
- Réserver strictement l'accès aux équipements à des personnes habilitées
- Effectuer un suivi des accès aux locaux permettant leur analyse
- Récupérer les clés et badges d'un employé à son départ
- Changer régulièrement les codes de l'alarme de l'entreprise (en installer une s'il n'y en a pas)
- Les prestataires extérieurs ne doivent jamais recevoir de clé ou de code d'alarme sauf s'il est possible de tracer les accès et de les restreindre à des plages horaires prédéfinies
- Rendre les contrôles d'accès robustes (cryptage des badges, biométrie, ...)
- Mettre en place un système de vidéosurveillance des accès
- Mettre en place un système de détection d'intrusion pour les zones vitales, particulièrement celles non-occupées 24h/24
- Placer les unités centrales des stations, les équipements réseaux industriels et les automates dans des armoires fermées à clé
- Eviter le placement de prises d'accès au système industriel et câbles réseaux dans des endroits ouverts au public
- Eviter le placement de prises d'accès au système industriel dans des zones sans surveillance
- Protéger l'intégrité physique des câbles par un capotage par exemple
- Obstruer les prises dédiées à la maintenance lorsqu'elles ne sont pas utilisées (bouchons, plaques d'occultation...). Une autorisation préalable et une procédure bien définie sont nécessaires avant le retrait de l'obturateur
- Doter les armoires contenant des équipements sensibles d'un dispositif de détection d'ouverture avec alarme, ou au minimum d'un moyen de contrôle visuel (scellé). Une autorisation préalable et une procédure bien définie sont nécessaires avant leur retrait

- **Protection des équipements et des câblages :**
- Définir les règles d'accès aux équipements, avec la définition des droits concernant l'utilisation des ports de communications locaux (USB, UART, port de test...)
- Disposer d'un système de monitoring d'accès aux équipements
- Installer les serveurs dans des locaux fermés sous contrôle d'accès, si possible dans des salles informatiques

- **Les médias amovibles (disques externes, clés USB, DVD, ...) :**
- Définir une politique pour l'utilisation de ce type de média
- Activer les politiques de restrictions logicielles
- Désactiver l'utilisation de ces médias et utiliser des systèmes dédiés aux transferts (SAS) pour échanger des données entre les réseaux si besoin
- Désactiver les ports USB sur les systèmes, restreindre les fonctionnalités

Facilité de mise en œuvre



Maîtriser la gestion et l'échange des données numériques internes

Classiquement, la gestion et l'échange des données numériques internes **concernent l'informatique de gestion** à tous les niveaux de l'entreprise. Avec l'avènement de l'internet de l'industrie et des objets (numérisation et connexion des machines et organes de production), les données « internes » s'élargissent naturellement à **des sources situées sur la chaîne de production**, dont par exemple les infrastructures. L'objectif de cette numérisation est une intégration « verticale numérique » de tout l'écosystème des produits & services avec deux finalités en vue.

D'une part, un gain de productivité, d'efficience, de maintenance prédictive et d'amélioration permanente de processus est visé.

D'autre part, il s'agit de profiter des effets « d'externalités » par l'implication des usagers et clients, sous forme d'une boucle de retour numérique sur l'expérience et les KPI des livrables de l'entreprise. Autant la frontière entre systèmes de gestion et systèmes industriels est claire, au moins dans la nature « structurelle » des dispositifs qui les composent, autant les périmètres entre données « internes » et « externes » deviennent parfois floutés, rendant complexe l'anticipation des risques associés et parfois artificielle la séparation entre les deux démarches cybersécurité qui les ciblent. Nous avons opté malgré tout pour des fiches séparées dans la mesure où les « destinataires » des données numériques concernés dans la présente fiche sont strictement internes à l'entreprise qu'il s'agisse de personnes ou de machines.

Vulnérabilités et risques associés

- Les liaisons sans fil mal protégées constituent une porte d'entrée majeure vers les données internes.
- Si le réseau ne comporte aucun cloisonnement, la prise de contrôle d'un poste de travail par un attaquant lui permet généralement d'étendre son intrusion aux autres postes de travail pour, in fine, accéder aux documents des utilisateurs.
- Les médias amovibles sont des vecteurs majeurs de propagation de virus. Ils sont principalement utilisés lors de l'échange de données entre les réseaux qui ne sont pas interconnectés.
- Les négligences telles que l'oubli d'un verrouillage du poste de travail représentent une vulnérabilité des données internes évidente, pouvant mettre en danger l'entreprise et sa notoriété.

Les questions à se poser pour identifier les risques

- L'entreprise dispose-t-elle d'un inventaire des équipements autorisés à accéder aux données internes ?
- Le réseau Wifi est-il le même pour toutes les catégories d'intervenants ?
- Quel est le niveau de sécurité des mots de passes en vigueur ?
- Quelle est l'architecture du réseau de l'entreprise ?

FICHE PRATIQUE

Maîtriser la gestion et l'échange des données numériques internes

N°07

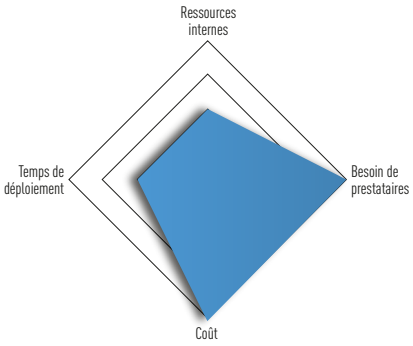
Recommandations, bonnes pratiques

- Verrouiller les postes de travail lorsqu'ils ne sont pas occupés
- Autoriser la connexion au réseau de l'entreprise aux seuls équipements maîtrisés
- S'assurer de la sécurité des réseaux d'accès Wi-Fi et de la séparation des usages : mettre à disposition des visiteurs et des terminaux à usage personnel un réseau Wi-Fi avec SSID dédié
- Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur :
  - Utiliser des comptes d'accès nominatifs (éviter les comptes génériques de type « admin »
  - Les comptes d'administration doivent comporter des identifiants et secrets d'identification différents des comptes utilisateurs (p ar exemple, pmartin comme identifiant utilisateur mais adm-martin comme identifiant administrateur)
- Assurer la traçabilité des connexions et des échanges réussis et échoués
- Changer les éléments d'authentification par défaut sur les équipements et services
- Si nécessaire, employer la double authentification, c'est-à-dire fournir un mot de passe supplémentaire lors de l'authentification, généré aléatoirement par un service tiers avec une génération unique, et réinitialisé à chaque utilisation
- Proscrire le branchement de tout périphérique inconnu (ex. clé USB) ou non maîtrisées (provenance connue mais intégrité non évaluée)
- Activer et configurer le pare-feu local des postes de travail
- Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques
- Se protéger des vulnérabilités en effectuant régulièrement des mises à jour (correctifs)
- Identifier les données sensibles, les sauvegarder et intégrer cette procédure dans le Plan de Continuité d'Activité

Les sources d'informations utiles sont :

- **« Guide d'hygiène informatique, renforcer la sécurité de son système d'information en 42 mesures, ANSSI »,** https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

Facilité de mise en œuvre



Assurer la traçabilité de la production

Les systèmes industriels utilisent de plus en plus de moyens numériques embarqués pour assurer la traçabilité de la production, soit pour en garder l'historique, soit pour connaître à n'importe quel moment l'état de transformation du produit. Ces moyens de traçage peuvent être positionnés sur des supports (ou palettes) ou directement sur le produit. Les plus utilisés sont la reconnaissance optique de caractères ou de code à barres. L'étiquette RFID est maintenant bien répandue pour l'échange d'informations avec le produit. C'est une étiquette constituée d'un circuit électronique et d'une antenne qui peut communiquer, pour certaines, jusqu'à 100 mètres. Une version à beaucoup plus courte portée commence à se généraliser, même dans le public : la technologie NFC qui permet, par exemple, le paiement par carte bancaire sans contact.

Vulnérabilités et risques associés

- Un traçage passif (sans étiquette et protocole radio RFID ou NFC) est naturellement vulnérable car facilement copiable.
- La possibilité de lecture de l'étiquette RFID (aussi appelée tag) ou NFC pose aussi des problèmes de sécurité. Les vulnérabilités sont à deux niveaux : celui de la communication avec le lecteur et celui de l'accès direct (physique) à l'étiquette. Les transactions avec les lecteurs peuvent en effet être captées et réutilisées d'une façon illégale. Il existe aussi des attaques physiques comme la rétroconception et l'observation de l'activité du RFID de façon à récupérer la structure et le contenu du RFID. Les vulnérabilités sont décrites en détail ci-dessous.
- **Le clonage ou contrefaçon :** il s'agit de dupliquer les étiquettes RFID, en ayant effectué préalablement sa rétro-conception, et en créer des copies conformes, permettant ainsi l'accès à une zone restreinte, l'introduction de pièces contrefaites, la modification du prix d'un produit, etc, ...)
- **Le rejeu :** il s'agit d'enregistrer une communication avec le tag RFID et de la rejouer pour valider des produits de natures différentes, voire contrefaites. L'attaquant utilise un dispositif malveillant qui sert de relai de communication entre les deux composants. L'information envoyée par l'étiquette est interceptée et est renvoyée au lecteur. Le lecteur a donc l'impression que l'information provient directement de l'étiquette. Cette attaque peut s'effectuer à distance et est difficile à contrer. Elle contourne les protocoles de sécurité et est même capable de contourner le cryptage en faisant usage de clés privées.
- **L'attaque de « l'homme du milieu » ou « Man-in-the-middle »**, tout comme l'attaque par rejeu, consiste à intercepter la communication entre une étiquette et le lecteur et sans qu'aucune anomalie ne soit détectée. En plus de l'attaque par rejeu, l'attaquant modifie les données de façon illégale de façon à ce que lecteur valide un produit de nature différente ou contrefait.
- **L'attaque par injection de code** est basée sur l'attaque man-in-the-middle. il s'agit de manipuler des étiquettes RFID afin d'y inclure un code malveillant ou un virus affectant le bon fonctionnement du système de gestion et de traitement des données. Les systèmes touchés par ce genre d'attaque deviennent inutilisables ou hors-service. Plus particulièrement, ces attaques sont des injections de type SQL qui peuvent être utilisées pour altérer n'importe quel enregistrement dans une base de données SQL.
- **L'attaque conduisant à un déni de service** ou corruption de données : la majorité des composants d'un système RFID sont des cibles potentielles pour les attaques par déni de service, que ce soit l'étiquette, le lecteur, le système de gestion ou le serveur. L'attaquant n'a pas besoin d'avoir accès aux données transmises. L'attaque consiste à transmettre un signal radio brouillant les échanges RFID, rendant le système indisponible et bloquant potentiellement la production.
- **L'attaque par canaux cachés** consiste à déterminer les paramètres de chiffrement (cryptographie) en analysant la consommation électrique, le temps d'exécution, etc... C'est une attaque simple par analyse de courant utilisée pour craquer un protocole de chiffrement de type RSA (du nom des inventeurs Rivest Shamir Adleman). La consommation de courant est directement liée au paramètre de déchiffrement.

FICHE PRATIQUE

Assurer la traçabilité de la production

- Les vulnérabilités des systèmes RFID ou NFC utilisés en logistique peuvent engendrer des pertes économiques élevées, en cas d'arrêt d'une chaîne de production notamment
- La gestion des étiquettes radio nécessite un système complet de traçage : des serveurs de confiance, un système d'information sécurisé, un parc de lecteur...
- Des produits contrefaits peuvent être intégrés dans la chaine de production si le système de traçage a été corrompu par une attaque du type « man-in-the-middle ». Les produits contrefaits sont alors indétectables car possédant une authentification valide
- Une cyber-attaque effectuée sur un système de traçabilité cause des problèmes de confidentialité. En effet, un attaquant peut tracer la localisation d'un produit expédié et avoir accès aux informations relatives aux stocks d'un entrepôt. Il peut s'en suivre une cascade d'attaques et causer préjudice à une filière
- Une chaîne de production avec un système de traçabilité défaillant s'expose à des poursuites judiciaires. Il s'agit en effet d'une exigence règlementaire que d'apporter la preuve de la traçabilité des opérations réalisées, ou encore des matières utilisées et de leur origine

N°08

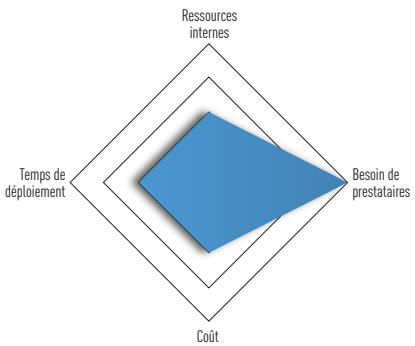
Les questions à se poser pour identifier les risques

- Est-ce qu'un système passif (sans émission radio) peut être utilisé sur mes produits sensibles ?
- Est-ce que je maîtrise parfaitement les possibilités de la RFID et la NFC ? Leurs caractéristiques sont-elles proportionnelles à mes besoins ?
- Est-ce que je connais toutes les raisons qui arrêtent ma production ?
- Est-ce que j'ai des pertes de données de traçabilité ?
- Est-ce que j'ai des défauts d'inventaire, des variations de prix constatés chez mes revendeurs ?

Recommandations, bonnes pratiques

- Munir les étiquettes RFID d'une clé d'indentification privée non effaçable
- Changer régulièrement l'identifiant de la puce RFID de l'étiquette (Il est également possible de changer de manière aléatoire l'identifiant de la puce)
- Utiliser le système informatique afin de détecter des anomalies ou incohérences concernant le statut d'une étiquette. Il est en effet possible de croiser les informations de l'étiquette RFID avec celles provenant d'une autre source.
- Crypter les étiquettes. Cette solution ne résout pas le problème du pistage
- Utiliser si nécessaire, la commande KILL qui permet de désactiver l'étiquette de manière permanente, la rendant inutilisable dans la suite du procédé de fabrication ou de distribution

Facilité de mise en œuvre



Sauvegarder et protéger les données et logiciels

De nombreuses informations existent de plus en plus sous format électronique et contribuent grandement à la valeur d'une entreprise. Elles doivent donc impérativement être sauvegardées et protégées contre toutes formes de pertes de données ou d'attaques possibles, pour préserver les données de l'entreprise, leur intégrité et confidentialité. La sauvegarde nécessite des précautions particulières, d'une part pour ne pas induire des fuites d'informations confidentielles, d'autre part pour garantir la disponibilité des données même en cas de défaillance, ce qui implique un processus d'archivage fréquent et sécurisé.

Vulnérabilités et risques associés

- L'absence de protection des données technologiques (informations sur les produits, les gammes, les conditions de fabrication, les données matériaux, les résultats de contrôle, etc..) peut conduire à leur disparition et/ou leur piratage.
- Les logiciels et outils pour créer ou numériser les documents, s'ils sont piratés peuvent altérer les données et/ou les rendre disponibles à l'extérieur.
- L'absence de sécurisation, non seulement au niveau des données et fichiers mais aussi au niveau du processus d'archivage et d'accès aux données par le système d'information constitue une vulnérabilité importante
- La gestion de l'archivage nécessite une organisation adéquate au sein de l'entreprise. Elle doit permettre de définir les personnes habilitées pour la création de documents, leurs modifications, leur sauvegarde régulière, leur restauration, ...
- La perte ou le piratage de données peut conduire à la faillite de l'entreprise, amenant des conséquences économiques graves pour la région et/ou la nation.
- L'absence de protection de données contractuelles entraîne la responsabilité de l'entreprise et des décideurs en cas de malveillance constatée.

Les questions à se poser pour identifier les risques

- Est-ce que je connais l'intégralité des données et logiciels de mon entreprise, nécessaires à mon activité ?
- Ai-je un plan de sauvegarde et de protection robuste de mes données et versions de logiciels ?
- Quelles sont les personnes habilitées à gérer le processus d'archivage/restauration

FICHE PRATIQUE

Sauvegarder et protéger les données et logiciels

N°09

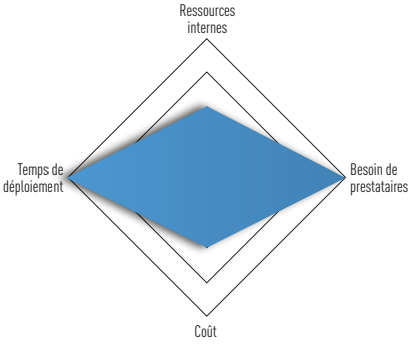
Recommandations, bonnes pratiques

- Identifier les documents à archiver et définir les conditions d'archivage selon la nature de ces documents. En effet, la nature des documents détermine le mode d'archivage, qui peut être simple ou légal à valeur probante
- Protéger les données jugées sensibles avant archivage, avec des moyens cryptographiques pour préserver leur confidentialité et intégrité, et permettre aux personnes autorisées à gérer le processus d'archivage et mise à jour
- Etudier un processus d'archivage et restauration des données puis le mettre en œuvre. Il comprend au moins ces trois volets : établissement d'une cartographie avec les type de données à archiver, le choix des logiciels et des outils numériques pour créer/numériser les documents et la définition de la sécurité du processus d'archivage/ restauration
- Les informations devraient être sauvegardées avant et après toute modifications, y compris lorsque celles-ci ont été apportées « à chaud »
- Tester régulièrement le processus de restauration des sauvegardes. Il peut, par exemple être testé sur un échantillon limité mais représentatif du système dans son ensemble
- S'assurer que les sauvegardes soient déconnectées du système d'information et, avoir plusieurs supports physiques de sauvegarde. Conserver plusieurs sauvegardes à des dates différentes.

Les sources d'informations utiles sont :

- **« L'archivage numérique des documents »,** https://www.entreprises.gouv.fr/files/files/directions_services/numerique/guides/fiches-praTIC/fiche03.pdf

Facilité de mise en œuvre



Services en ligne et cloud

L'utilisation de services en ligne (parfois appelés « sur/dans le cloud ») consiste à exploiter de façon distante, généralement par internet, des fonctionnalités de stockage, de calcul ou de service en général (mail, partage de document, gestion de projet...). Elle est devenue chose courante dans la sphère personnelle et professionnelle. Ces services permettent de tirer pleinement partie des avantages de la révolution numérique (accès à des services pour tout à chacun qui nécessitaient auparavant un investissement conséquent). Ils constituent un levier puissant de compétitivité en coût et fonctionnalités souvent négligés. Il convient cependant d'observer certaines précautions afin d'exploiter pleinement ce potentiel sans fragiliser la sécurité de son installation.
La part de services en ligne peut être internalisée sur des serveurs hébergés et exploitées par l'entreprise ou externalisée sur des serveurs appartenant et exploités par une autre entreprise. Cela dépend de ses contraintes et de sa stratégie propre.

Vulnérabilités et risques associés

La gamme de services en ligne qu'une PME peut solliciter est très vaste. Il est possible de façon simplifiée de les classer en deux catégories :

- **Les services en ligne utilisés par l'entreprise pour elle-même** sans lien avec ses équipements ou son écosystème client/fournisseurs (ex : mail professionnel, système de gestion de projet, service de partage de documents en ligne) dont l'usage est à sa discrétion ;
- **Les services en ligne utilisés par son écosystème** (ex : service de sauvegardes automatiques des paramètres d'une machine-outil sur le cloud proposée par le fabricant de machine, plateforme d'échange de spécifications imposée par un client) que l'entreprise peut ou doit dans certains cas utiliser.

Les vulnérabilités principales résident :

- **Dans la façon dont ses services sont hébergés :**

  → les serveurs doivent être hébergés et exploités selon des pratiques de sécurité compatible avec le service demandé. Il est ainsi souvent plus prudent de confier à un tiers dont c'est le cœur de métie, cette activité, plutôt que de vouloir internaliser des serveurs dans son entreprise (mal déployés/exploités, ils constitueraient un facteur de risque supplémentaire. Habituellement les services en ligne proposent une gamme de certifications permettant d'apprécier le sérieux de leur hébergement (PCI-DSS, ISO/IEC 27001, SOC1-2, ...) ;

- **Dans la façon dont les services sont exploités :**

  → Les données qui transiteront par ces services, notamment s'ils sont hébergés par un tiers, doivent être considérées suivant leur confidentialité (contractuelle ou non).Il convient de s'assurer que le service en ligne possède les fonctionnalités ou agrémentations requises (par exemple possibilité de cryptage coté client, c'est-à-dire avant que les données soient transférées sur le serveur, ou habilitation à héberger des données d'un certain type) afin d'éviter les risques associés à l'exposition, la falsification ou la fuite de ces données.

  → L'utilisation de ces services doit observer un ensemble de bonnes pratiques incontournables en matière de cybersécurité, notamment pour ce qui est de l'authentification (utiliser un compte unique par rôle / utilisateur, utiliser un mot de passe différent par service en ligne, et le cas échéant utiliser un gestionnaire de mot de passe pour pallier à la multiplication des services en ligne) afin de limiter le risque de compromission lié à l'authentification sur un service donné.

FICHE PRATIQUE

Services en ligne et clo

N°10

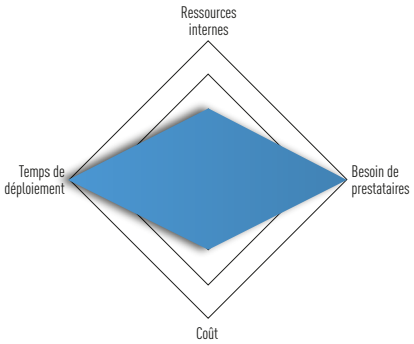
Les questions à se poser pour identifier les risques

- Quels sont les services en ligne qui me sont proposés ou imposés par mon écosystème (partenaire, fournisseur, client, ...). Quel sont les avantages / risques associés ?
- Quelles sont les données qui sont traitées par le service en ligne et quelles sont leurs particularités (confidentialité contractuelle ou stratégique, données personnelles, etc.) ? Faut-il les crypter avant l'usage par ces services ?
- Quelles sont les caractéristiques d'hébergement et d'exploitation des services en ligne utilisés ? En particulier, est-il plus judicieux de confier cette activité à un tiers ou de l'internaliser ? Où les données sont-elles hébergées en cas d'externalisation (les législations du lieu d'hébergement peuvent avoir un impact sur le type de données hébergées) ?
- Quels sont les utilisateurs de ces services en ligne et comment est gérée l'identification (nom d'utilisateur) et l'authentification ?

Recommandations, bonnes pratiques

- Observer les bonnes pratiques générales quant à l'usage des identifiants / mot de passe, notamment utiliser un mot de passe unique par service en ligne (quitte à utiliser un gestionnaire de mot de passe)
- Séparer l'espace professionnel et l'espace personnel (ne pas utiliser les mêmes comptes pour un usage professionnel et un usage personnel)
- S'assurer de la qualité de l'hébergement du service (qu'il soit effectué en interne ou confié à un tiers) et rester objectif quant aux avantages/inconvénients respectifs
- Identifier l'offre de service en ligne disponible et l'évaluer selon les critères de certifications, d'utilisation, de réputation et de lieu d'hébergement – pour les législations en vigueur en 2017, les hébergements situés sur le territoire européen offrent plus de garanties légales de protection de la vie privée et d'exploitation des données à des fins connexes au service proposé)

Facilité de mise en œuvre



Sécuriser les données numériques avec l'extérieur

L'accélération des échanges commerciaux, l'obligation de répondre au plus vite aux fluctuations de la demande, l'augmentation de la complexité des produits incluant toujours plus de fonctionnalités font que les entreprises, leurs sous-traitants et partenaires doivent communiquer en temps réel et donc, de façon numérique. Chaque échange peut être considéré comme un point de vulnérabilité qu'il faut sécuriser.

Vulnérabilités et risques associés

Plusieurs vulnérabilités peuvent être mises en évidence, autour de la divulgation d'informations à des tiers non autorisés, ou de l'accès aux informations par des personnels autorisés.

- **Externalisation :** l'externalisation des services informatiques (par exemple la gestion commerciale avec une société) facilite les opérations de l'entreprise mais les données commerciales sont conservées à l'extérieur, dans des environnements non maitrisés par l'entreprise.
  - → Les mécanismes d'accès doivent être correctement sécurisés. Il convient en particulier de se méfier des services gratuits qui fusionnent de manière informelle services grands public et données professionnelles, et qui sont régulièrement attaqués.
  - → Il convient de s'assurer que les données ainsi exportées peuvent être réimportées (et sous quel format) à tout moment, et ce de manière utilisable.

- **Données commerciales et financières.** Le cadre réglementaire implique la fourniture régulière de données financières à l'extérieur. Les appels d'offre peuvent également requérir l'échange de données commerciales. Ces données sont particulièrement sensibles, tant en termes de contenu que d'échéance. Il convient donc de vérifier l'intégrité des données et la disponibilité des échanges.

- **Données de production et gestion de l'équipement de production.** Les équipements de production peuvent être connectés à l'extérieur pour réaliser des opérations de maintenance. Ces opérations peuvent inclure la transmission au fournisseur de données de production. Elles peuvent également amener à des mises à jour des matériels, pour lesquelles il est nécessaire de vérifier leur innocuité et leur acceptabilité dans les processus de l'entreprise.
  - → Les environnements de développement sont rarement dédiés, il y a donc des risques de confusion en multipliant les activités de chaque poste.

- **Continuité de service.** En cas de fin de contrat d'externalisation mal maitrisé, l'entreprise peut perdre l'accès à ses données. Il convient donc de préparer la continuité de service, notamment en cas de ré-internalisation ou de changement de fournisseur.

- **Sécurisation des échanges :** les données échangées par des moyens « ouverts » de type messagerie peuvent être divulgués à des tiers non autorisés.
  - → Les solutions de sécurisation parfois disponibles pour des PC portables sont souvent inopérantes pour les smartphones.
  - → Il est souvent difficile de convenir de moyens de sécurisation d'échanges (chiffrement de messages et/ou de documents en pièce jointe) avec des grandes entreprises.

FICHE PRATIQUE

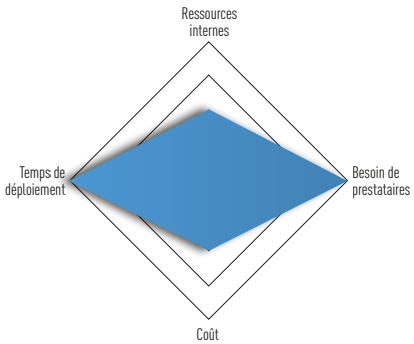
Sécuriser les données numériques avec l'extérieur

N°11

Les questions à se poser pour identifier les risques

- Quel est le degré de confidentialité des informations à transmettre vers l'extérieur ?
  - →Quel moyen a été sélectionné pour la transmission de ces données ?
  - →Quel est le niveau de cybersécurité associé ? Les données sont-elles chiffrées ?
  - →Quel est le niveau de cybersécurité du destinataire des données ?
- De quelle nature est l'accès à distance offert pour la télémaintenance ?
  - →Les machines de l'entreprise ont-elles une connexion Internet et si oui comment l'utilisent-elles ?
  - →Transmettent-elles périodiquement des données à l'extérieur ?
- Quels services externes sont utilisés par l'entreprise ?
  - →Ais-je essayé de récupérer mes données ?

Facilité de mise en œuvre



Recommandations, bonnes pratiques

- Bannir les accès anonymes ou génériques (accès nominatif obligatoire) et fournir aux utilisateurs des certificats (par exemple des cartes à puce)
- Crypter les informations échangées (notamment par messagerie)
- Crypter les supports de stockage des données (disques durs, clés USB, ...)
- Mettre en place une architecture intégrant un réseau tampon (DMZ - Demilitarized Zone), c'est-à-dire un sous réseau se positionnant entre le réseau interne de confiance et l'internet public. Elle est généralement créée par l'emploi d'un pare-feu
- Installer un réseau privé virtuel (VPN) permettant une protection du réseau, si possible utilisant des certificats plutôt que des login/mot de passe :
  - →Intégrées comme service du pare-feu (IPSec) en cas de liaison permanente entre deux sites
  - →Intégrées dans les applications (TLS) de messagerie (SMTPS, IMAPS) ou de navigation (HTTPS) pour les échanges applicatifs
  - →Intégrées dans un terminal (SSH) pour les connexions en mode commande (notamment pour les machines)
- Mettre en place des mécanismes forts d'authentification et de récupération de mots de passe. A l'heure actuelle, une double authentification par calculette (SecurID, etc) ou SMS est opérationnelle pour de nombreux services
- Lors de l'achat en ligne, privilégier les plateformes sécurisées (https:/.....) et être vigilant aux messages d'alerte de votre navigateur concernant les certificats de sécurité

Sécuriser les documents officiels et engagements contractuels

La dématérialisation des contractualisations requiert des moyens adéquats de sécurisation tels que les signatures électroniques à valeur légale. L'archivage des documents comptables et financiers dématérialisés doit par ailleurs répondre aux normes en vigueur (NF Z 42-013 ou ISO 14641-1).

Vulnérabilités et risques associés

- L'utilisation de signatures électroniques non labellisées par l'ANSSI peut se révéler dangereux
- La valeur d'un contrat peut être jugée nulle si le document numérique le contenant ne respecte pas le cadre réglementaire imposé, entraînant ainsi des pertes économiques pour l'entreprise
- L'absence de formation des collaborateurs concernant les pratiques et règles d'archivage numériques pour les documents à valeur probante peuvent engendrer des problèmes juridiques si les documents ne respectent pas le cadre réglementaire défini concernant leur archivage
- L'utilisation d'outils non sécurisés favorise l'usurpation d'identité et la falsification de documents
- Il peut être nécessaire de tracer des événements, des actions ou des informations, de manière à en retrouver la description exacte, l'enchaînement chronologique et l'utilisation afin de répondre à un cadre réglementaire. Toutes les traces doivent être enregistrées et conservées de manière à garantir leur exhaustivité et leur intégrité : toute modification ou suppression de traces doit être détectable. Elles sont certifiées conformes et peuvent être produites devant la justice en tant que preuves. L'absence de moyen adapté d'archivage rend cette traçabilité impossible ou à valeur juridique nulle

Les questions à se poser pour identifier les risques

- Quels sont les moyens d'archivage électronique mis en place ?
- Répondent-ils aux normes requises et obligations légales ?
- Les outils de signature électroniques utilisés sont-ils labellisés par l'ANSSI ?

FICHE PRATIQUE

Sécuriser les documents officiels et engagements contractuels

N°12

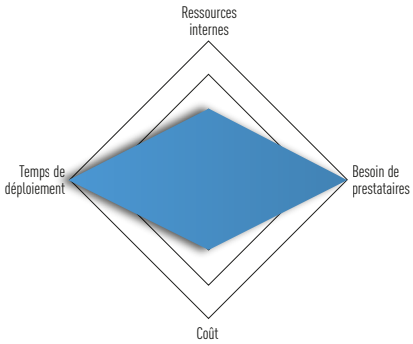
Recommandations, bonnes pratiques

- Assurer la traçabilité de toutes les opérations concernant les archives versées (communication, migration, éventuelle élimination...)
- Les documents officiels et engagements contractuels doivent être à valeur probante, c'est-à-dire que l'intégrité de leur contenu doit être garantie légalement via des mécanismes de sécurité, parmi lesquels une signature électronique sécurisée. Celle-ci devrait utiliser un certificat accrédité par l'ANSSI ou une instance européenne équivalente
- **Différentier les notions de GED (Gestion Electronique de Documents) et SAE (Système d'Archivage Electronique).** Une GED ne fait que gérer, contrôler, indexer et stocker des documents numériques. En supplément de de ces fonctions, un SAE répond à une logique de conservation et de conformité légale/réglementaire. Un SAE garantit donc le maintien de l'intégrité des documents en empêchant leur modification durant leur conservation. Un SAE maintient la valeur probatoire des documents, ce qui n'est pas le cas d'une GED
- Choisir un système d'archivage électronique conforme à la norme NF Z 42-013 si le projet est exclusivement français, ou ISO 14641-1 s'il est international
- Les documents fiscaux et contractuels (bons de commande, états comptables, tickets de caisse, etc.) doivent être hébergés en France ou dans un pays de l'Union Européenne, de préférence par une société de nationalité européenne
- Connaître les engagements pris par le prestataire d'hébergement du SAE (le prestataire s'engage t'il sur la non perte et l'intégrité des documents ou seulement sur la disponibilité du logiciel ?)
- Si le SAE est en mode SAAS, s'assurer qu'il répond à la norme ISO/IEC 27001 ou dispose du label France Cybersecurity
- S'assurer que le prestataire de SAE est en mesure de fournir le document archivé ainsi que les éléments de traçabilité (horodatage d'archivage, empreintes, journal du cycle de vie de l'archive, journal des événements, journal des accès) en cas de rupture du contrat

Les sources d'informations utiles sont :

- **« 6 critères fondamentaux pour choisir une solution d'archivage électronique à valeur probante »,** https://www.globalsecuritymag.fr/6-criteres-fondamentaux-pour,20170321,69781.html

Facilité de mise en œuvre



Maitriser les flux financiers et commandes dématérialisées

Accélérant la gestion financière, réduisant les risques d'erreur et simplifiant les procédures comptables, la dématérialisation des paiements est devenue incontournable. Dans ce contexte, les tentatives de fraudes, en particulier par ingénierie sociale s'intensifient dans le milieu des entreprises.

Vulnérabilités et risques associés

- Contrefaçon aisée des virements papier ou fax.
- La mise en ligne d'informations publiques concernant les collaborateurs pouvant être utilisées à des fins de fraude utilisant l'ingénierie sociale constitue une vulnérabilité
- Les défaillances de cybersécurité concernant en particulier l'authentification permettent l'usurpation d'identité (fraudes liées à l'ingénierie sociale) ou l'accès direct aux comptes de l'entreprise.
- Les impacts économiques d'une fraude touchant les comptes de l'entreprise peuvent s'avérer élevés.

La plupart des fraudes liées aux flux bancaires sont de l'ordre de l'ingénierie sociale *(voir fiche 1).* Les trois techniques malveillantes les plus répandues sont :

- **La fraude aux coordonnées bancaires :** le fraudeur se fait passer pour un fournisseur et signale un changement d'IBAN, accompagné de la dernière facture non-réglée. Celle-ci a été au préalable obtenue en usurpant l'identité de l'entreprise cible. L'entreprise ciblée effectue donc un virement au fraudeur et non au fournisseur.
- **La « fraude au président » :** les collaborateurs sont contactés par un fraudeur se faisant passer pour l'un de leurs responsables hiérarchiques et réclamant un transfert d'argent sur la base d'une urgence ne permettant pas d'activer sereinement les mécanismes de contrôle inhérents à ce type d'opérations.
- **La fraude du test bancaire :** le fraudeur se fait passer pour le service télématique d'une banque et prétexte des tests de compatibilité avec l'entreprise cliente pour demander un virement bancaire, supposé fictif.

Les questions à se poser pour identifier les risques

- Est-ce que les transactions effectuées par la banque correspondent à mes journaux d'événement ?
- Quel est le niveau d'information mis en ligne publiquement concernant les collaborateurs ?
- Les collaborateurs ont-ils connaissance des types de fraudes les plus courantes utilisant l'ingénierie sociale ?
- Qui est autorisé à effectuer des transactions et quelles sont les méthodes d'identification employées ?

FICHE PRATIQUE

Maitriser les flux financiers et commandes dématérialisées

N°13

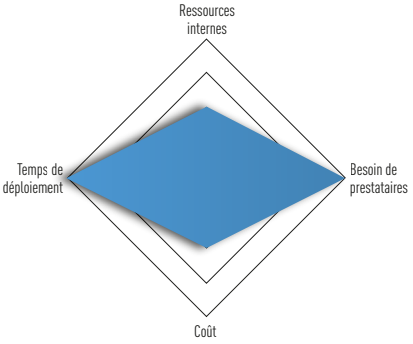
Recommandations, bonnes pratiques

- Identifier toute personne se connectant ou signant des ordres sur un portail de banque en ligne ou sur des protocoles de télétransmission, notamment à l'aide de l'un des moyens suivants :
  - →Identifiant et clavier virtuel
  - →Identifiant et certificat personnel sur support physique
- Signer des ordres pour garantir que le fichier n'a pas été corrompu entre son envoi et sa réception (certificat SWIFT 3SKey, Secure Access...)
- Chiffrer les fichiers d'ordres et le canal (formats CMS, S/MIME, PGP)
- Vérifier l'identité de la personne émettant des ordres pour que les personnes recevant les ordres ne soient pas remises en cause (accusé de réception envoyé aux clients, signature par certificat SWIFT 3SKey...)
- S'informer auprès de sa banque du plan d'action à appliquer en cas de cyber-attaque
- Limiter les virements papier ou fax, faciles à contrefaire
- Privilégier la dématérialisation par le biais de la banque électronique et respecter les consignes de sécurité afférentes à ces outils
- Mettre en place des procédures internes sécurisées (double administration, double signature au-delà d'un seuil, plafonds...)
- Sensibiliser les personnes exposées (trésoriers, comptables, ...)
- Limiter les informations disponibles sur internet (réseau sociaux, professionnels et personnels ou autre) afin de ne pas faciliter les fraudes utilisant l'ingénierie sociale
- Porter un regard critique sur les coordonnées de l'expéditeur d'un mail ou d'un appel téléphonique
- Les outils devraient être utilisés par leurs responsables seulement. Par exemple, les logiciels de comptabilité devraient être accessibles aux comptables uniquement. De même, les logiciels de communication bancaire devraient être réservés aux trésoriers. Cela limite les possibilités de fraude aux coordonnées bancaires
- Crypter les données-client échangées avec un tiers pour leur transmission et leur stockage
- Avoir un code PIN utilisé pour l'application mobile de plus de 6 caractères
- Rendre la double identification obligatoire
- Eteindre automatiquement les applications au bout de 15min d'inactivité
- Mettre en place une surveillance en temps réel des applications
- Vérifier la correspondance entre l'utilisation des cartes bancaires et leurs journaux d'utilisation. Si des dépenses excèdent ce que le journal indique, avertir directement la banque

Les sources d'informations utiles sont :

- **« Sécurisation des paiements : Le contrôle des RIB »,** https://www.voxfi.fr/securisation-paiements-controle-rib/
- **« Sécurité des flux dématérialisés »,** http://cashmanagement.societegenerale.com/dossier/securite-des-flux-dematerialises

Facilité de mise en œuvre



Sécuriser les produits et services connectés

Les objets connectés sont devenus omniprésents et deviennent de plus en plus exposés aux risques liés à la cyber-sécurité. Vendre des produits connectés ou des services associés nécessite donc la mise en place de mesures de sécurité permettant de protéger l'entreprise, les clients et les tiers. La mise en œuvre de ces mesures est rendue complexe par la diversité des protocoles utilisés. L'harmonisation et la normalisation de ces protocoles constitue donc un réel enjeu. Afin de définir un cadre pour la sécurité des objets connectés, certains critères et certifications ont récemment été mis en place au niveau français.

Vulnérabilités et risques associés

Les vulnérabilités associées aux services connectés consistent tout d'abord en la possibilité de voler et/ou de détourner des données, voire de les altérer. L'exploitation de vulnérabilités logicielles peut amener à une perte de contrôle des objets déployés. Les vulnérabilités peuvent concerner soit l'objet lui-même, soit l'objet associé à une infrastructure de commande et de contrôle. Les risques suivants peuvent être mis en évidence :

- **Prise de contrôle des équipements.** Les objets connectés sont souvent fondés sur des technologies ouvertes (Linux, OpenSSL, etc.), dans lesquelles des vulnérabilités sont régulièrement découvertes, soit de mise en œuvre, soit de fonctionnement. On peut citer plusieurs exemples de situations de prise de contrôle malveillantes :
  - → Détournement de capteurs intégrés comme les caméras, micros, et accès au réseau
  - → Intrusion dans la logique de contrôle/commande/régulation du produit, pouvant conduire à des dysfonctionnements et aller jusqu'au blocage de son fonctionnement
  - → Le détournement d'un capteur ou la modification d'un système de contrôle/commande/régulation pouvant mettre en danger la sécurité physique d'une installation et des utilisateurs

Les logiciels développés spécifiquement le sont de manière ad-hoc, sans préoccupation spécifique pour la cyber-sécurité, ou en arbitrant lors de la conception du logiciel en faveur de la fonctionnalité. Dans un environnement informatique, les mises à jour permettent de résoudre le problème. Dans le monde des objets connectés, les mises à jour sont peu fréquentes (voire inexistantes), et peu sécurisées *(voir plus haut).* Il en résulte une capacité pour un attaquant de compromettre un large réseau d'objets connectés et de l'utiliser à son profit.

- **Vol de données.** Le vol de données est la menace la plus évidente, dans la mesure ou les protocoles utilisés dans le contexte IoT, ou les équipements terminaux, sont de faible capacité. Ils ne sont donc pas capables de réaliser des opérations de chiffrement complexes. Les données sont donc souvent transmises en clair, ou avec des mécanismes de chiffrement facilement déchiffrables, sur des réseaux faiblement ou pas protégés. L'évolution récente des réseaux IoT vers des protocoles radio très économes en énergie induit un accroissement de ces risques.

- **Altération de données.** Pour la même raison, les équipements impliqués ne sont pas capables de sceller les données pour assurer leur intégrité, ni d'authentifier les différents intervenants de la communication. Un attaquant peut donc s'insérer dans une communication en se faisant passer pour l'un des intervenants, et modifier les messages échangés. Cela peut amener à une modification des données traitées par l'infrastructure (avec un impact direct sur la qualité de service), ou à une modification de la configuration de l'objet connecté.

FICHE PRATIQUE

Sécuriser les produits et services connectés

N°14

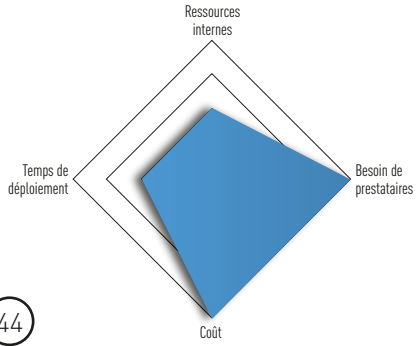
Les questions à se poser pour identifier les risques

- Quel est le type de protocole utilisé par l'objet connecté ? Est-il standard et éprouvé ?
- Quelles sont les dispositions visant à mettre à jour l'objet connecté ? Comment sont effectuées les mises à jour ?
- Le produit comporte-t-il des vulnérabilités physiques permettant d'en extraire de l'information ou d'intervenir sur son fonctionnement ?
- Comment et par qui la qualité du système de protection du produit est-elle contrôlée ?
- Puis-je utiliser des briques de développement (matériel et logiciel) standardisées et bien maitrisées ?
- Comment puis-je assurer la surveillance de l'infrastructure associée aux objets ?

Les sources d'informations utiles sont :

- **« Cybersécurité des objets connectés - Risques, bonnes pratiques et opportunités, ANSSI »,** http://cedric.cnam.fr/workshops/iot-cybersecurite-cyberdefense/Presentation_ANSSI.pdf
- **« Certificat National de Premier Niveau »,** https://www.ssi.gouv.fr/administration/produits-certifies/cspn/

Facilité de mise en œuvre



Recommandations, bonnes pratiques

- **Développement de l'objet**
  - → Utiliser des composants logiciels et matériels standards autant que possible
  - → Prévoir des mécanismes de mise à jour robustes, et proactifs, capables de diffusion à l'échelle du déploiement des objets
  - → Limiter les besoins de communication au strict nécessaire (filtrage d'adresses, utilisation de relais, etc.)
  - → Prévoir des mécanismes de chiffrement adaptés et à l'état de l'art (par exemple recommandations de l'ANSSI ou du NIST) : clés, certificats, ..., et prévoir leur renouvellement (voir mécanismes de mise à jour)
  - → Prendre en compte les vulnérabilités physiques du produit (vibrations et chaleur dégagée pouvant donner une signature des modes de communication voire de leur contenu informationnel, protection électromagnétique, etc.)
- **Usage de l'objet et infrastructure**
  - → Utiliser des composants logiciels et des processus de développement standards pour l'infrastructure (serveurs web, protocole HTTPS, communication MQTT, etc.)
  - → Maintenir l'infrastructure à jour (correction des vulnérabilités du système d'exploitation, des services, etc.), notamment en effectuant une veille appropriée (CERT, etc.)
  - → Valider et surveiller les processus de communication support (radio, DHCP, DNS, routage, ...)
  - → Assurer des mécanismes de remontée et de traitement des alertes entre objets et infrastructure et de réaction en cas de détection d'un incident (SOC, alertes, plan de continuité et/ou de reprise d'activité, ...)
- Faire certifier / auditer la conformité des produits et services par un tiers (certificat de sécurité informatique à l'état de l'art, utilisation de protocoles standards et éprouvés), par exemple par un CESTI
  - → Eventuellement, rechercher une CSPN (Certification de Sécurité de Premier Niveau) malgré un coût parfois élevé
- Mettre en place des dispositifs de contrôle des fournisseurs et sous-traitants de systèmes critiques qui interviennent dans la fabrication des produits ou pouvant entrer dans la composition du produit

Glossaire

A

Adresse IP — La communication sur internet est fondée sur un protocole appelé IP (Internet Protocol) qui permet aux ordinateurs de communiquer entre eux. Ce protocole utilise des adresses numériques pour distinguer ces machines et tronçonne la communication en paquets comportant chacun une adresse de source et une adresse de destination. La version la plus couramment employée du protocole est la version IPv4 dans laquelle les adresses sont composées de 4 nombres, par exemple 213.56.176.2. La version 6 (IPv6) a été développée en prévision de la pénurie d'adressage possible par IPv4, due au développement très rapide d'internet.

Architecture logicielle — L'architecture logicielle décrit d'une manière symbolique et schématique les différents éléments d'un ou de plusieurs applications logicielles, leurs interrelations et leurs interactions.

Architecture matérielle — L'architecture matérielle décrit l'agencement de composants électroniques ainsi que leurs interactions.

Attaque — Concrétisation d'une menace, qui nécessite l'exploitation d'une vulnérabilité.

Authentification — Apporter la preuve de son identité

B

Bitcoin — Monnaie virtuelle cryptée, caractérisée par l'anonymat, la décentralisation et l'absence de réglementation. Cette nouvelle forme de paiement n'a pas besoin d'intermédiaires.

Bluetooth — Technologie de communication sans fil qui équipe la plupart des appareils mobiles (smartphones, tablettes, PDA, netbooks, laptops..) mais aussi les équipements informatiques (clavier, souris ...). Les failles de la technologie Bluetooth sont réelles et il est recommandé de désactiver le Bluetooth lorsqu'il n'est pas utile.

Botnets — Un botnet est un ensemble de systèmes contrôlables par un attaquant via des serveurs de commande. Les propriétaires de ces systèmes ne savent pas que le PC participe à un botnet (leur PC a été compromis au préalable et à leur insu via l'exploitation d'une vulnérabilité).

Buffer overflows — Débordement de mémoire hors allocation

Bug — Défaut de conception d'un programme informatique à l'origine d'un dysfonctionnement.

C

Captation de données Vol de données, soit par extraction de fichier, soit par capture de trafic réseau.

Capteur clavier Logiciel ou matériel employé pour capturer ce qu'une personne tape au clavier.

Cassage de mot de passe Procédé de recouvrement de mots de passe d'un système informatique. Ce procédé permet ponctuellement d'aider un utilisateur du système à retrouver un mot de passe perdu ou d'obtenir le mot de passe d'une tierce personne. On se sert aussi de ce procédé pour obtenir des statistiques de fiabilité et de robustesse des mots de passe utilisés lors d'audits de sécurité.

Dans une démarche d'un professionnel de la sécurité, ce procédé est une mesure préventive permettant de vérifier le niveau de sécurité réel des mots de passe, celui-ci pouvant être comparé avec le niveau demandé par la politique des mots de passe existante.

Certificat Donnée électronique permettant de lier l'identité d'un utilisateur ou d'un système et un ensemble de clés pouvant être utilisées par des algorithmes de chiffrement. Par exemple, TLS (Transport Layer Security, norme de chiffrement de l'information) nécessite l'installation sur le serveur web d'un certificat liant le nom de domaine et une clé publique. Les certificats sont délivrés par une autorité de certification, qui les signe (Verisign, Lets encrypt, ANSSI, ...). Cela permet de vérifier la validité et la qualité d'un certificat pour décider ou non de poursuivre la connexion.

Chantage Forme d'extorsion imposée par un code malveillant sur un utilisateur du système. Si ce dernier refuse de payer ou d'effectuer une tâche imposée, le service auquel il veut accéder lui est refusé par le code malveillant.

Cheval de Troie Programme donnant l'impression d'avoir une fonction utile, mais qui possède par ailleurs une fonction cachée et potentiellement malveillante.

Clé de chiffrement Une clé est un paramètre utilisé en entrée d'une opération cryptographique (chiffrement, déchiffrement, scellement, signature numérique, vérification de signature).

Une clé de chiffrement peut être symétrique (cryptographie symétrique) ou asymétrique (cryptographie asymétrique) : dans le premier cas, la même clé sert à chiffrer et à déchiffrer ; dans le second cas on utilise deux clés différentes, la clé de chiffrement est publique alors que celle servant au déchiffrement est gardée secrète (la clé secrète, ou clé privée, ne peut pas se déduire de la clé publique).

Une clé peut se présenter sous plusieurs formes : mots ou phrases, procédure pour préparer une machine de chiffrement (connexions, câblage, etc. Voir machine Enigma), données codées sous une forme binaire (cryptologie moderne).

Clonage de serveur Activité malveillante visant à modifier un serveur DNS (serveur de noms de domaine), dans le but de rediriger un nom de domaine vers une adresse IP différente de l'adresse légitime.
En croyant aller sur un site connu, l'internaute navigue en réalité sur un site factice.

Cloud Utilisation de la puissance de calcul ou de stockage de serveurs distants par l'intermédiaire d'un réseau, le plus souvent internet. Le Cloud computing est aussi appelé "informatique en nuage".

Code d'exploitation	Tout ou partie d'un programme permettant d'utiliser une vulnérabilité ou un ensemble de vulnérabilités d'un logiciel (du système ou d'une application) à des fins malveillantes.
Code embarqué	Programme chargé en mémoire non volatile dans un objet.
Code source	Texte comprenant des instructions de programmation écrit dans une syntaxe interprétable par un système informatique (soit lu par un programme d'interprétation, soit directement par le système après compilation). Exemples: C, Python, Java, ...
Codecs	Logiciel ou matériel permettant de compresser ou de décompresser un signal numérique (vidéo ou audio), en respectant une certaine norme.
Contrefaçon	La contrefaçon est l'exploitation non autorisée d'une marque déposée, d'un dessin ou d'un modèle enregistré, d'une invention brevetée ou d'une création originale protégée par des droits d'auteur. Exemple de cyber-contrefaçon : imitation de nom de domaine, usurpation de nom d'entreprises
Contrôle d'accés à distance	L'accès à distance, la commande à distance ou encore le contrôle à distance sont des méthodes qui permettent, depuis un dispositif informatique éloigné (ordinateur, tablette, ..) et sans limite théorique de distance, de prendre le contrôle d'un autre système.
Convergence IT/OT	Transition, convergence entre systèmes d'information industriels (SII) / Operation Technology « OT » et systèmes d'information d'entreprise (SIE) / Information Technology (IT). Il s'agit d'un rapprochement entre le monde industriel et le monde informatique, convergeant autour d'un socle technologique commun et confrontés aux mêmes défis de cyber-sécurité, de pilotage du patrimoine matériel et logiciel et de valorisation des données issues des équipements.
Cookie	Un cookie est une suite d'informations envoyée par un serveur HTTP à un client HTTP à chaque fois que le serveur est interrogé. C'est un fichier texte à en-tête HTTP. Il peut être utilisé pour une authentification, une session ou pour stocker une information spécifique sur l'utilisateur. Ils ne sont ni des logiciels espions ni des virus. Néanmoins, un grand nombre de courriels considérés comme "spams" provient de l'information glanée par les cookies de pistage.
CPU	Central Processing Unit ou Unité Centrale de Traitement (uct) qui correspond au processeur d'un dispositif informatique.
Cross Site Scripting	Dépôt de code malveillant (en général javascript) par un attaquant, activé lors de la visite d'un site.
Cryptologie	La cryptologie réunit la cryptographie (« écriture secrète ») et la cryptanalyse (étude des attaques contre les mécanismes de cryptographie). La cryptologie ne se limite plus aujourd'hui à assurer la confidentialité des secrets. Elle s'est élargie au fait d'assurer mathématiquement d'autres notions : assurer l'authenticité d'un message (qui a envoyé ce message ?) ou encore assurer son intégrité (est-ce qu'il a été modifié ?). Pour assurer ces usages, la cryptologie regroupe quatre principales fonctions : le hachage avec ou sans clé, la signature numérique et le chiffrement.
Cyberattaque	Une cyberattaque est un acte malveillant contre un dispositif informatique.
Cybersécurité	La cybersécurité consiste à assurer que les ressources numériques d'une entreprise (qu'elles soient matérielles, logicielles ou de communication) sont uniquement utilisées dans le cadre prévu.

D

Débogueur — Outil de programmation permettant à un développeur d'observer et de contrôler l'exécution d'un programme, afin d'en comprendre le fonctionnement et/ou d'en trouver les dysfonctionnements.

Defacing / defacement — Altération du contenu d'un site web.

Déni de service (Dos) — Action ayant pour effet d'empêcher ou de limiter la capacité d'un système à fournir le service attendu, en sur sollicitant le service au délà de ses capacités (ex : saturer un site web de requêtes pour le mettre hors service).

Digitalisation — Terme synonyme de numérisation qui s'apparente, dans son acceptation moderne à la transformation digitale des entreprises. Numérisation de l'entreprise à tous les niveaux du système de production élargi : chaîne de fournisseurs, sites industriels, lignes de fabrication, SI, ressources, interfaces...

Disponibilité — Assurer l'accès et l'utilisation lorsque c'est nécessaire.

DMZ — Demilitarized Zone: espace réseau (plage d'adresses) spécifiquement configurée pour permettre l'échange entre Internet et un réseau sécurisé de confiance. Une DMZ est construite à partir d'un pare-feu à 3 ports, ou de deux pare-feu.

DPA — Differential Power Analysis. Méthode d'attaque physique d'un composant électronique qui, en utilisant la manipulation de l'alimentation de ce composant, permet d'obtenir des informations, typiquement des clés ou algorithmes de chiffrement.

E

ERP — L'Enterprise Resource Planning correspond au PGI francophone, c'est-à-dire à un Progiciel de Gestion Intégré.

Erreurs de configuration — La configuration d'un logiciel ou d'un matériel est le choix d'un certain nombre de caractéristiques par le futur utilisateur, dans le but d'adapter le logiciel ou le matériel à l'utilisation spécifique attendue. Une erreur de configuration peut conduire à une vulnérabilité ou à un mauvais fonctionnement du système.

Erreurs d'usage — Mauvaise utilisation d'un logiciel ou d'un équipement, utilisation par erreur d'un logiciel ou d'un équipement non prévu pour les résultats attendus.

Exfiltration — Sortie de données de l'entreprise, de manière non autorisée.

Exigences de conformité — Caractéristiques réelles prouvant l'identité d'un tiers et/ou du respect normatif et législatif en vigueur.

F

Failles logicielles — Vulnérabilité d'un programme dans lequel un attaquant peut, en fournissant des données non attendues, obtenir un comportement utile pour lui.

Firewall — Pare feu. Dispositif informatique, positionné en coupure entre deux réseaux, permettant de contrôler les échanges être ces deux réseaux.

G

Fuite d'informations — Voir exfiltration.

GED — Gestionnaire Electronique de Documents.

H

Hachage — Transformation d'une chaîne de caractères en valeurs ou en clés de longueur fixe, plus courtes que la chaîne principale. Le hachage peut être utilisé dans les bases de données et dans des algorithmes pour le cryptage ou la signature numérique de documents.

Hameçonnage — L'hameçonnage (anglais : phishing) - Vol d'identité ou d' informations confidentielles (coordonnées bancaires par exemple) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant comme s'il s'agissait d'un système légitime . Les emails d'hameçonnage sont de plus en plus répandus dans les entreprises (faux email de facture, faux email de rappel, de scan de photocopieuse ...).

Hebergement mutualisé — L'hébergement mutualisé est un mode d'hébergement Internet destiné principalement à des sites web, dans un environnement technique dont la caractéristique principale est d'être partagé par plusieurs utilisateurs. Cette architecture est adaptée pour des sites d'importance et d'audience faibles ou moyennes, ne sollicitant que ponctuellement les ressources du ou des serveurs informatiques assurant l'hébergement (processeur, mémoire vive, espace disque, débit). L'administration de ces derniers est assurée par un intervenant tiers (et non par le titulaire de l'hébergement). Cette mutualisation impose la subdivision d'une partie de l'espace disque du serveur d'hébergement en autant de sites hébergés.

HTTPS — HTTP sécurisé, protocole par lequel un navigateur va tout d'abord construire un tunnel TLS (Transport Layer Security) pour protéger les informations échangées avec le serveur. Cela permet notamment de protéger l'identification et l'authentification d'un utilisateur.

Identification — Communiquer son identité à un système. Une identité peut être un nom, et de plus en plus souvent une adresse mail. Il convient donc d'être extrêmement vigilant dans la protection des comptes de messagerie (mail) utilisés comme mécanisme d'identification.

I

IDS — Intrusion Detection System. Outil logiciel ou matériel capable de surveiller l'activité d'un système d'information ou d'un réseau, et de détecter les attaques.

Infrastructure clés publiques — Infrastructure de gestion de certificats, permettant à un groupe d'utilisateurs d'obtenir et d'échanger de manière sécurisée des informations d'identification et d'authentification.

Ingénierie sociale — Stratégie d'un attaquant par laquelle il va essayer d'obtenir des informations de la part d'un utilisateur légitime en le trompant. Un exemple classique est "la fraude au président", ou l'attaquant se fait passer pour un supérieur hiérarchique et fait pression pour obtenir une information ou une action compromettante.

Intégrité — Conservation des qualités et caractéristiques originelles d'une donnée ou d'un système, sans altération.

Internet Protocol Security — Ensemble de protocoles utilisant des algorithmes cryptographiques, permettant l'échange sécurisé de données sur internet.

Interoperabilité — Capacité de deux équipements informatiques ou systèmes d'information à communiquer.

Intrusion — Attaque réussie.

L

Label — Un label est une étiquette attachée à des données, qui peut servir à traiter cette donnée de façon sécurisée, en certifiant son intégrité.

Loi informatique — Est concerné par la loi informatique (Loi informatique et libertés) tout traitement ou mémorisation d'un fichier à caractère personnel, dont le responsable et/ou le créateur est établit sur le territoire français, ou qui recourt à des moyens de traitement situés sur ledit territoire.

M

M2M — Machine to Machine. Communication entre deux objets, entre un objet et une infrastructure informatique.

Maintien en condition opérationnel (MCO) Définition d'un plan d'action permettant le maintien d'activité d'un équipement. Cela fait souvent partie d'un PCA (Plan de Continuité d'Activité).

Malveillance Acte ayant pour but de nuire ou dont la conséquence est une nuisance.

Malware Programme malveillant (virus, ransomware, etc.)

Menace Cause potentielle d'un accident, à fin malveillante, s'appuyant sur une ou plusieurs vulnérabilités.

Modem Système permettant la communication, par l'intermédiaire d'un réseau analogique, de deux ou plusieurs équipements numériques par modulation/démodulation du signal.

Mouchard Logiciel ou marque espion intégré dans une page web, permettant de tracer la navigation d'un utilisateur entre sites web.

N

Navigateur Logiciel client permettant d'obtenir des pages web depuis Internet et de les afficher sur un terminal. Les plus connus sont Chrome (Google), Edge et Internet Explorer (Microsoft), Firefox (Mozilla), Safari (Apple). Ces logiciels sont complexes et incluent beaucoup de composants, parfois externes (lecteur flash, lecteur pdf, interpréteur javascript, etc.).

NetBios Protocole de communication réseau utilisé dans les environnements Windows, souvent vecteur de vulnérabilités et d'attaques.

O

Obsolescence Système ou protocole vieillissant, périmé, désuet.

P

Pair à pair Mode de fonctionnement d'un réseau dans lequel tout équipement connecté au réseau possède les mêmes capacités de communication, et aucun ne dispose de privilèges particuliers. Cela revient à dire que chaque équipement est capable de transmettre non seulement ses propres informations mais également celle des autres, pour assurer une communication de bout en bout, sans infrastructure particulière. Cela implique souvent que chaque équipement est capable de joindre n'importe quel autre.

Pare feu Un pare feu est un outil permettant de protéger un ordinateur ou un réseau connecté à un autre réseau ou à internet. Il protège des attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant). Le pare feu est souvent installé sur une machine dédiée dans une architecture réseau conçue pour cela.

Patrimoine immateriel Ensemble des informations, données, connaissances et brevets détenus par une organisation.

Plan de continuité d'activité (PCA) Définition d'un plan d'action permettant de continuer l'activité de l'entreprise, éventuellement de manière réduite, lorsqu'elle subit des pannes ou des attaques. Voir résilience.

Plan de reprise d'activité (PRA) Définition d'un plan d'action permettant à l'entreprise, après panne ou attaque, de revenir à un niveau normal attendu de production.

Politique de sécurité Définition de la stratégie de protection de l'entreprise, mise en place suite à une analyse de risque. La politique de sécurité inclut des moyens techniques (pare-feu, anti-virus, annuaire d'entreprise), leur configuration, et les règles de bon comportement des utilisateurs, particulièrement en cas d'incident.

Port — Un port a plusieurs acceptions. Pour une communication TCP/IP, le port est un nombre qui identifie un service particulier (coté serveur) ou l'origine d'une demande de connexion à ce service (coté client). Pour un équipement réseau, le port est un numéro de prise sur cet équipement (ex. prise RJ45).

Port physique — Connecteur qui permet de relier des équipements informatiques (périphériques, ...).

Porte dérobée — Une porte dérobée est un accès secret à un logiciel, permettant à l'éditeur ou au mainteneur informatique d'y accéder plus rapidement. L'introduction malveillante d'une porte dérobée peut transformer le logiciel en "Cheval de Troie".

PRNG — Pseudo Random Number Generator, générateur de nombres pseudo-aléatoires. Les algorithmes de chiffrement et de signature, ainsi que les protocoles associés, impliquent la capacité de générer des nombres aléatoires de manière fiable. Si un attaquant est capable de deviner tout ou partie du processus de génération, il lui est facile de casser la protection.

Produits connectés — Produits pour lesquels le fonctionnement nécessite une connectivité réseau, continue ou intermittente. Par exemple, les mécanismes de reconnaissance vocale sur téléphones demandent une capacité de calcul que ceux-ci ne possèdent pas. L'appel à un service distant permet de réaliser les calculs les plus couteux. Cette externalisation implique souvent que le fournisseur de service obtient tout ou partie des données de l'utilisateur, ce qui conduit au minimum à des problématiques de protection des données personnelles.

Protocole — Ensemble de règles et de contraintes permettant d'établir et de maintenir une communication entre deux ou plusieurs systèmes.

R

Renifleur — Voir sniffing.

Résilience — Capacité à faire face à une situation perturbante telle qu'une panne ou une attaque informatique et de continuer à fonctionner.

Restauration — Remise en état d'un système informatique, d'un système industriel, ou de l'un de leurs composants.

RGPD — Règlement général sur la protection des données. Règlement européen concernant les données personnelles.

Risque — Possibilité qu'une vulnérabilité conduise à un préjudice sur le fonctionnement de l'entreprise.

Robustesse — Niveau de sécurité d'un système informatique face à un éventuel attaquant.

Rootserver — Dans l'infrastructure de nommage des domaines (DNS, Domain Name System), il existe 13 serveurs racines répartis dans le monde, les root server, qui permettent d'accéder à tous les domaines.

S

SAAS — Software as a service. L'application n'est pas dite "propriétaire", c'est-à-dire qu'elle n'existe pas en tant que telle dans un des ordinateurs de l'entreprise. Le logiciel est situé dans le Cloud et son utilisation est apparentée à un service.

SAE — Système d'archivage électronique. Dans le SAE, le mot « archivage » doit être compris comme la dernière étape du cycle de vie du document, et pas dans le sens simpliste de "stockage de fichiers".

Sauvegarde	Copie des documents d'un système d'information, permettant de le remettre dans un état antérieur "sain", ou en tout cas utilisable. Il est important de protéger les sauvegardes, de manière à éviter le vol d'information ou leur destruction par un attaquant.
SCADA	Système d'acquisition et de contrôle de données, permettant la supervision totale d'un système de production, jusqu'à la télégestion en temps réel d'un grand nombre de mesures. Permet de contrôler à distance des installations industrielles.
Sécurité numérique	Cybersécurité.
Security Operating Center (SOC)	Centre de contrôle informatique en charge de traiter les alertes en provenance de mécanismes de détection, et de bloquer les attaques.
Serveurs	Système informatique hébergeant des services, donc capable de recevoir des demandes de connexion d'un logiciel client. Il en existe de nombreux types : web, messagerie, nommage (DNS), ftp, etc. Dans les réseaux IP, les services sont identifiés par un numéro de port inférieur à 1024: 80 pour le web/http, 25 pour la messagerie/SMTP, etc.
SI	Voir système d'information.
Signature électronique	Algorithme et données certifiant l'intégrité et l'authenticité d'un message ou d'un document.
Sniffing / sniffeur	Un sniffeur est un logiciel écoutant le réseau. Les deux plus connus sont tcpdump et wireshark.
SNMP	Simple Network Management Protocol. Outil de gestion de réseau, connu pour ne pas avoir de mécanisme de sécurité.
Spam	Message non sollicité. Ce vecteur est souvent utilisé pour attirer un utilisateur vers un site web malveillant.
Spoofing	Usurpation. En termes de cybersécurité, l'usurpation peut toucher l'identité d'un utilisateur (par exemple vol de son adresse mail et de son mot de passe) ou l'adresse réseau d'un équipement.
Spyware	Logiciel espion, dont l'objectif est d'analyser l'activité d'un utilisateur et/ou de lui voler des données.
SQL Injection	Méthode d'attaque d'un site web dynamique interagissant avec une base de données. L'attaquant détourne les requêtes de la base en ajoutant des informations susceptibles de compromettre la sécurité du système.
Supervision	Surveillance de l'activité d'un système d'information, incluant la collecte de trace et leur analyse, à des fins de détection d'attaques et d'analyse.
Système d'exploitation	Logiciel fondamental d'un ordinateur, d'un téléphone portable ou d'un équipement informatique, intermédiaire entre les capacités du matériel et les services dont ont besoin les applications (affichage, communication, calcul, ...). Un système d'exploitation inclut souvent des fonctions de sécurité comme le contrôle d'accès aux fichiers, ou le filtrage réseau par un pare-feu. Il est souvent protégé par un mécanisme d'identification-authentification. Les plus connus sont Android, Windows, iOS, Linux.
Système d'information	Ensemble de matériels et logiciels fournissant les services numériques d'une entreprise.

Systèmes industriels Système technique de production, souvent constitué d'automates programmable associé à des capteurs et des actionneurs, pilotés par une console (PLC, HMI, SCADA, ICS). Les spécificités des protocoles utilisés les rendent souvent vulnérables, et les contraintes techniques qu'ils doivent satisfaire les rendent plus difficiles à sécuriser.

T

Transport Layer Security TLS Protocole de réseau privé virtuel (VPN) applicatif, permettant de sécuriser les communications d'une session (web, messagerie). Dans un navigateur, l'usage de TLS (HTTPS) se matérialise par un cadenas, et la viabilité du certificat utilisé par une couleur verte dans la barre de navigation. TLS permet majoritairement de garantir l'identité du serveur web auquel l'utilisateur se connecte. Il est possible de réaliser une authentification mutuelle par échange de certificats au préalable.

V

Ver Un ver (ou worm) est un logiciel malveillant indépendant, cherchant à propager son code au plus grand nombre de cibles connectées à un même réseau local, puis de l'exécuter sur ces mêmes cibles. Il perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs.

Violation d'accés Accès non autorisé aux données ou aux services.

Virtual Private Natwork Voir VPN.

Virus Un virus est un programme ou morceau de programme malveillant dont le but est de survivre sur un système informatique (ordinateur, serveur, appareil mobile ...) afin d'en parasiter les ressources (données, mémoire, réseau ...). Les principaux vecteurs d'infection sont les messages avec pièces jointes, les supports amovibles (clé USB..), les sites Web malveillants ou piratés, ...

VLAN Virtual Local Area Network. Réseau local privé "virtuel"; la protection est assurée par l'association de labels aux trames Ethernet. Un équipement non autorisé à utiliser un label ne devrait pas accéder aux trames labellisées. Cependant, l'information circule en clair et un attaquant peut tout à fait écouter le réseau. Il peut arriver, en cas de problème réseau, que l'isolation de VLANs ne fonctionne pas.

VPN Virtual Private Network. Mécanisme d'isolation d'un réseau par rapport aux autres. Certains mécanismes d'isolation reposent sur l'utilisation de protocoles crytographiques comme IPSec (pour sécuriser les datagrammes IP) ou TLS (pour sécuriser un flux applicatif comme du web, de la messagerie, etc.). Ces VPN peuvent être considérés comme forts. Il existe d'autres mécanismes comme MPLS, dans lesquels l'information circule en clair. Dans ce cas, un équipement compromis pourrait donner accès à l'information circulant dans le réseau.

Vulnérabilité Faiblesse au niveau d'un élément d'un système industriel ou d'information. La vulnérabilité peut toucher la conception, la réalisation, l'installation, la configuration et l'utilisation.

Le Réseau CTI remercie les CTI qui ont participé activement à la rédaction de ce document de sensibilisation, sous l'animation de Marie-Sabine GAVOIS, déléguée générale du Réseau CTI :

- **CERIB :** Stéphane LE GUIRRIEC
- **CETIAT :** François DURIER
- **CETIM :** Hélène DETERME et Dominique ROUCKHAUT
- **CTICM :** Claire FILLATRE
- **FCBA :** Robert GOLJA
- **IPC :** Yves SCHMITT

Le Réseau CTI remercie vivement les membres du groupe de travail sur la cybersécurité de l'AIF :

- Patrick DUVAUT de l'**Institut Mines Telecom**
- Valentin HUEBER de **Syntec Numérique**
- Jean SRENG du **CEA List**
- Hervé DEBAR de l'**Institut Mines Telecom**

cti réseau

COMPÉTITIVITÉ
TECHNOLOGIE
INNOVATION

WWW.RESEAU-CTI.COM

8, rue Boudreau • 75009 Paris
01 53 43 82 16
secretariatcti@reseau-cti.com

Made in Kalankaa - 02 38 55 90 44