FICHE 17

CYBERSÉCURITÉ

► DESCRIPTIF/DÉFINITION

La cybersécurité consiste à assurer que les ressources numériques d'une entreprise, qu'elles soient matérielles (ex : puce, calculateur, PC, robots, machines à commandes numériques), logicielles (ex : programmes et données) ou de communication (ex : wifi, Internet), soient préservées de toute attaque, qui les détournerait 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 conformes à ce qui est attendu. (ex : la machine réalise l'action demandée et uniquement celle-là, y compris avec un fonctionnement dégradé en cas d'attaque) ;
- 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.

► ENJEUX (AVANTAGES)

Sur le plan économique

- Protéger ses données d'entreprise, son patrimoine immatériel.
- Sécuriser la relation avec fournisseurs et sous-traitants.
- Fournir des produits connectés et/ou services connectés sécurisés.

Sur le plan technologique

- Garantir le fonctionnement de l'atelier et 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 : rétrofit 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.

Sur le plan de la transformation de l'entreprise

- 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, 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

FICHE 17

CYBERSÉCURITÉ

plus forts que ceux-ci imitent de façon très fidèle des messages authentiques. 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. Le risque porté par le facteur humain concerne tous les collaborateurs dans l'entreprise (informaticiens, automaticiens, personnels administratifs, personnel d'ateliers).

► LES CLÉS DE LA RÉUSSITE

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. Sont ainsi décrits ci-dessous les cinq items incontournables pour intégrer la cybersécurité dans son entreprise :

- mettre en place une démarche sécurité numérique impliquant tous les acteurs de l'entreprise ;
- décrire la cybersécurité de son entreprise au regard de la cybersécurité générale et formaliser un plan d'actions ;
- mettre en œuvre et contrôler l'efficacité du plan d'actions ;
- s'appuyer lorsque nécessaire sur des fournisseurs de service ou des solutions de confiance ;
- suivre la législation et répondre au renforcement de la réglementation.

Au niveau technologique

- 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 (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. Au final, 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. Et la sécurité de celle-ci ne peut se résumer à des parades logicielles et matérielles visant à repérer et à éradiquer des codes malveillants. Elle doit garantir aussi la fiabilité du transfert d'informations intégrées entre les différents équipements.

- 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.

- Sécuriser les produits et services connectés.
  Les objets connectés sont devenus omniprésents et deviennent de plus en plus exposés aux risques liés à la cybersécurité. Vendre des produits connectés ou des services associés nécessite donc la mise en place de mesures de sécurité permettant de protéger l'entreprise,

FICHE 17

CYBERSÉCURITÉ

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.

Au niveau numérique

- 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.

- Sécuriser la traçabilité de 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.

- 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.

- Bien utiliser services en ligne et le cloud.
  L'utilisation de services en ligne consistant 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…) 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 un chacun qui nécessitaient auparavant un investissement conséquent) et constituent un levier puissant de compétitivité en coûts 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 qui sont internalisés (sur des serveurs hébergés et exploitées par l'entreprise) ou non (sur des serveurs apprenants et exploités par une autre entreprise), dépend de ses contraintes et sa stratégie propre.

- Sécuriser les données numériques avec l'extérieur
  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 (AFNOR NF Z 42-013 ou ISO 14641-1).

Au niveau des compétences à mobiliser, des connaissances et de la formation

- Sensibiliser les 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

FICHE 17

CYBERSÉCURITÉ

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.

- Briser les frontières entre les différents services (notamment entre les systèmes informatiques et les systèmes industriels). 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 est nécessaire de construire un langage commun. Pour ce faire, les différents mondes du digital doivent se décloisonner.

- Utiliser des outils nomades pour l'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. Les risques importants d'intrusion et de malveillance reposent principalement sur deux vulnérabilités potentielles que sont la connexion et la perte ou le vol.

- 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.

Les questions à se poser

- Quels seront les impacts du règlement européen sur la protection des données (GDPR), qui devra être respecté dès 2018 par toutes les entreprises collectant et traitant des données personnelles ?

- Une politique de sécurité devrait être construite autour de trois grandes questions :

- Que dois-je protéger en priorité ? Quel est mon patrimoine informationnel ?

- Quels sont les risques encourus (externes, internes) ?

- Quels sont les facteurs aggravants de risque ?

- Une fois ces facteurs déterminés, la politique de sécurité doit permettre d'établir un niveau minimum de sureté permettant de protéger durablement l'entité.

▸ MATURITÉ DE L'OFFRE

Émergent	Laboratoire	Prouvé	Mature	Fréquent	Pervasif