GUIDE PRATIQUE DE LA CYBERSÉCURITÉ

pour les PME/ETI industrielles

Pourquoi sécuriser les installations industrielles, quelle démarche adopter ?

Un livre blanc Grand Est Transformation Numérique

Une initiative de La Région Grand Est

Édito

L'industrie est au cœur de l'économie du Grand Est. 3ème région industrielle française après l'Île-de-France et l'Auvergne-Rhône-Alpes, le Grand Est capitalise sur une culture industrielle historique, sur un leadership marqué sur plusieurs secteurs industriels et sur la diversité de ses territoires industriels pour relever les nouveaux défis posés à l'industrie en matière d'environnement, de concurrence mondiale et d'innovation.

Le numérique est une composante indispensable de cette innovation et plus largement du fonctionnement de nos entreprises industrielles. La connexion des outils industriels par les outils numériques, porteuse d'innovations, accroît néanmoins les opportunités de malversations dont se sont emparés depuis peu des acteurs criminels ou des concurrents malintentionnés. Ce risque cyberindustriel devient aujourd'hui un enjeu fort pour tout acteur industriel connecté, impliquant une mobilisation collective face à cette menace.

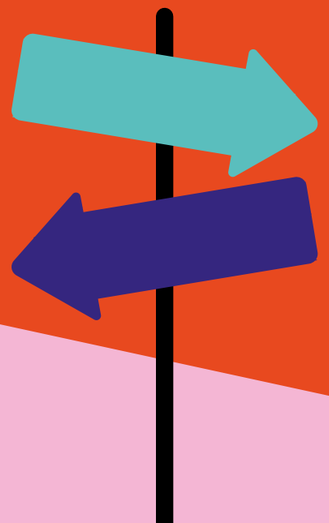
La Région Grand Est s'est donnée pour objectif de faire du Grand Est un territoire résilient face aux cybermenaces. Sans être une région « historique » de la cybersécurité, le Grand Est a enclenché depuis trois ans une dynamique remarquée, nous amenant à être parmi les premières régions à ouvrir un centre régional d'assistance aux victimes de cyberattaques (CSIRT).

À travers son plan régional de cybersécurité, la Région Grand Est vise à soutenir les acteurs régionaux, depuis leur sensibilisation jusqu'à la sécurisation de leurs systèmes d'informations, en passant par l'accompagnement des victimes de cyberattaques. Les acteurs industriels bénéficient alors de dispositifs tels que : le parcours régional d'accompagnement en cybersécurité, Grand Est Cybersécurité, ainsi que le CSIRT régional. Ils bénéficient également de l'EDIH Grand Est, un dispositif européen d'accélération de la transformation numérique des entreprises industrielles, dédié notamment à la cybersécurité.

Nos industries ont davantage besoin de comprendre les enjeux spécifiques de la cybersécurité industrielle et d'en voir les impacts opérationnels. En cela, ce guide pratique est un outil indispensable, dont la Région Grand Est accompagne la diffusion, dans le cadre du Business Act Grand Est.

Franck Leroy,
Président de la Région Grand Est

Ce guide a pour objectif d'accompagner les TPE, PME et ETI industrielles dans leur démarche de cybersécurité, tout en proposant de façon très concrète un processus à suivre pour protéger leurs installations.



AVANT-PROPOS

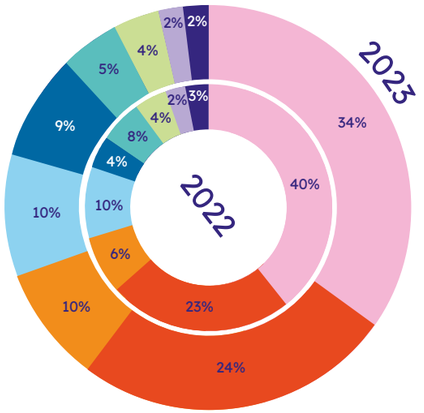
La numérisation croissante de l'activité professionnelle et l'évolution constante des techniques, tactiques et procédures des cyber-attaques augmentent le risque d'une attaque cyber. Ces attaques sont de plus en plus sophistiquées, innovantes et exécutées par des groupes de cybercriminels spécialisés.

Le dernier rapport de l'ANSSI / CERT-FR de 2023[1] confirme l'omniprésence de la menace cyber sur l'ensemble du territoire national, dont la région Grand Est. Il précise également que les TPE, PME et ETI sont les cibles privilégiées des cyberattaquants. L'actualité nous rappelle que les entreprises industrielles sont particulièrement exposées.

→ **En France, 34% des victimes de rançongiciel en 2023 étaient des PME/TPE/ETI.**

Chaque entreprise se doit d'intégrer la gestion du risque dans sa stratégie et ses procédés. Si les objectifs d'affaires restent primordiaux, il n'est plus possible d'élaborer une stratégie d'entreprise sans tenir compte du risque cyber.

Répartition des victimes d'attaque par rançongiciel en 2022 et 2023



- TPE/PME/ETI
- Collectivité territoriale/locale
- Entreprise stratégique
- Établissement de santé
- Association
- Établissement d'enseignement supérieur
- EPA/EPIC
- Ministère
- Autre

Source : ANSSI
Rapport CERTFR 2023

[1] Panorama de la cybermenace 2023 ANSSI.pdf (ssi.gouv.fr)

SOMMAIRE

Le contexte

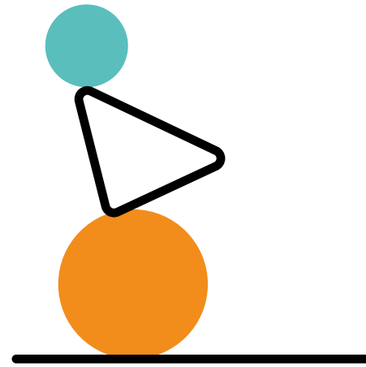
L'accélération de la transformation numérique des activités professionnelles stimule les opportunités d'innovation qui sont à la fois des leviers de croissance et de compétitivité. Pour prendre en compte ce changement de paradigme, les entreprises doivent adapter leurs processus métiers.

L'évolution technologique, l'arrivée de nouveaux capteurs et moyens de communication, le déploiement de nouvelles techniques d'exploitation des données, l'interconnexion des différents systèmes, la continuité numérique et l'apparition de services supplémentaires se traduisent par une forte augmentation des activités numériques.

Il s'agit d'un véritable défi à relever pour les entreprises industrielles dont les systèmes d'information supportent la gouvernance, les lignes de production, les utilités des bâtiments, les entrepôts, la performance énergétique... Un ensemble qui caractérise l'industrie du futur communément appelée « Industrie 4.0 ».

Les systèmes d'information industriels sont complexes, interactifs, et de plus en plus souvent connectés au réseau de l'entreprise. Le tout produit davantage de failles potentielles, des vulnérabilités qui sont exploitées par les cyberattaquants.

Les conséquences d'une cyberattaque peuvent être importantes : atteinte à la sécurité des personnes, dommages matériels, impacts environnementaux, mise hors service d'un service vital ou essentiel au bon fonctionnement de l'entreprise, perte ou atteinte à l'intégrité des actifs numériques (données), avec les conséquences financières induites...



CYBERSÉCURITÉ INDUSTRIELLE : DE QUOI PARLE-T-ON ?

La cybersécurité industrielle protège les systèmes industriels ou techniques d'une entreprise. Les systèmes industriels ou systèmes de contrôle industriels (ICS[2]) pilotent les processus physiques présents dans l'environnement de production ou la logistique, tels que des lignes d'assemblage automatisées, des îlots robotisés, des cabines de peinture, des fours, des postes opérateurs, partiellement ou totalement automatisés…

Les systèmes techniques, sont les systèmes d'informations n'ayant pas d'impact direct sur la production. Ces systèmes supportent la gestion des utilités et des infrastructures, le monitoring énergétique, les contrôles d'accès, la vidéo surveillance, la détection incendie, les logiciels de gestion des données métier…

L'ensemble de ces systèmes compose ce qu'on appelle communément le système d'exploitation opérationnelle de l'entreprise ou OT (Operational Technology), par comparaison avec le système d'information de gouvernance de l'entreprise que l'on nomme IT (Information Technology).

Sécuriser les systèmes industriels ou techniques revient à agir sur tous les composants du système :

- Le réseau
- Les postes utilisateurs
- Les données et leur stockage
- Les équipements industriels, automates, sous-systèmes, périphériques
- Les accès au système : utilisateurs, administrateurs
- Les serveurs, physiques ou virtuels.

Cela concerne également les utilisateurs : c'est donc aussi sensibiliser, former les salariés aux menaces et aux bonnes pratiques.

À l'instar de l'Information Technology (IT) ou système informatique de gouvernance d'une entreprise, les systèmes d'exploitation industriels ou Operational Technology (OT) sont polyvalents. On les trouve partout, dans les grands groupes industriels, comme dans les plus petites entreprises.

La pratique montre que les acteurs industriels ne disposent pas toujours du niveau d'expertise requis pour comprendre et répondre efficacement à un risque cyber omniprésent et en évolution constante.

Pour garantir le meilleur niveau de sécurité, il est primordial d'améliorer le niveau de maturité en cybersécurité de chacun des organismes et des parties prenantes, afin d'écarter au maximum le risque du maillon faible et de la faille qui seront exploités par un cyberattaquant.

Au-delà du défaut de compétence, les solutions déployées sont parfois inadaptées ou mal configurées. Soit elles ne correspondent pas au besoin de l'entreprise considérée, soit leur configuration ne respecte pas les bonnes pratiques de cybersécurité[3].

Le budget dédié à la cybersécurité doit être finement travaillé, en tenant compte de l'existant et des obsolescences programmées.

> **S'agissant de la cybersécurité, pour être efficace, il serait vertueux d'y consacrer un budget annuel à hauteur de 10% du montant du budget de la DSI.**
>
> **Guillaume Poupard, DG de l'ANSSI, 2022**

[2] Industrial Control System

[3] ISO 27002 code de bonne pratique pour le management de la sécurité de l'information

QUELLES SONT LES MENACES QUI PÈSENT SUR LES INDUSTRIELS ?

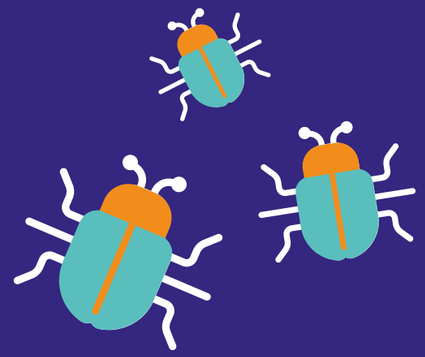
Il s'agit d'écarter au maximum le risque d'une atteinte à la disponibilité, l'intégrité ou à la confidentialité des actifs numériques. Une attaque sur un environnement industriel critique pourrait entraîner des conséquences dévastatrices allant d'une indisponibilité de la chaine de production jusqu'à la mise en danger du personnel.

Les attaques contre les systèmes de contrôle industriels (ICS[4]) ne concernent pas seulement le vol d'informations confidentielles ou le paiement d'une rançon. Un nombre croissant d'acteurs malveillants et d'attaques, potentiellement téléguidés par des États tiers, portent leur attention sur l'exploitation des actifs et des machines industrielles, à des fins d'espionnage ou encore pour nuire à l'image d'une industrie ou du pays considéré.

Le dysfonctionnement ou l'arrêt d'un site de production, d'un atelier ou d'un flux logistique peuvent entrainer des pertes financières significatives.

D'après le cabinet de conseil Asterès[5], qui se fonde sur l'analyse de 385 000 cyberattaques en France en 2022, le coût moyen grimpe à 59 000€ pour les entreprises et organisations.

La durée moyenne d'arrêt d'un système de production après une attaque par ransomware est de l'ordre de 21 jours. Cette durée de neutralisation peut varier selon la façon dont l'entreprise a anticipé et organisé sa stratégie de gestion de crise cyber. S'il n'existe pas de plan de reprise ou de continuité d'activité (PRA/PCA), la durée de neutralisation peut être encore plus importante.



En septembre 2023 une cristallerie dans le Grand Est a été victime d'une cyberattaque par ransomware « Les cybercriminels ont chiffré les dossiers de l'entreprise victime et demandé une rançon afin de débloquer les données ». Dans un communiqué envoyé à la presse, la prestigieuse cristallerie avait indiqué : « Baccarat est confrontée à l'indisponibilité d'une partie de ses données mais rien n'indique pour l'instant que des données personnelles ou confidentielles de ses clients, salariés ou partenaires aient été compromises. »

[4]Industrial Control System
[5]Les cyberattaques réussies en France : un coût de 2 Mds€ en 2022 - ASTERÈS (asteres.fr)

Pour réduire les risques de pertes de données ou limiter la durée d'indisponibilité d'un système d'information, il est indispensable de mettre en place une politique de sauvegarde des données (y compris des configurations industrielles) afin de pouvoir redémarrer au plus vite le système de production.

Le redémarrage d'un système de production est une opération particulièrement délicate. Dans le domaine industriel, il est fréquent que des outils modernes cohabitent avec des systèmes dont l'ancienneté se compte en décennies et dont la maitrise technique n'est plus garantie par les équipes techniques qui ont été renouvelées. Le coût lié à la reprise d'activité doit prendre en compte le potentiel remplacement des actifs spécifiques au monde industriel tels que les automates et autres équipements de type SCADA (système de contrôle et d'acquisition de données) dont les coûts peuvent être élevés.

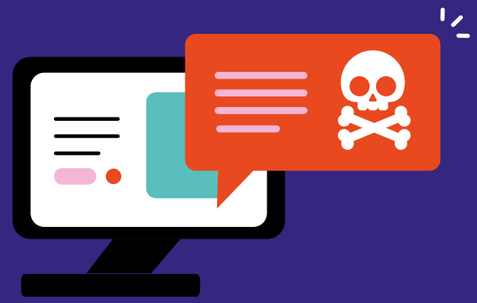
Une cyberattaque qui neutralise un système industriel peut rapidement entrainer des pertes de revenus ou des pénalités liées à l'arrêt de la production. À cela s'ajoutent des coûts supplémentaires de main-d'œuvre pour arrêter la cyberattaque, restaurer le système ou mettre en place de nouvelles protections.

Le domaine industriel, par nature plus complexe, exige un engagement fort de la direction[6] en appui de l'élaboration et de la mise en œuvre de la stratégie de cybersécurité.

Face aux nombreux risques et conséquences auxquelles elles sont exposées, les organisations industrielles peuvent se sentir démunies. Pour une grande majorité d'entre elles, elles ne savent pas par où commencer.

→ **Ce guide a pour ambition d'apporter aux organisations industrielles les notions clés et les bonnes pratiques qui leur permettront d'élaborer une politique de cybersécurité adaptée à leur stratégie d'affaires, à leur chaine de valeur et aux exigences réglementaires fixées par leur domaine d'activité.**

[6] ISO 27001 Système de management de la sécurité d'un système d'information - chapitre 5 - Leadership



DES MALWARES SPÉCIFIQUES QUI CIBLENT LES SYSTÈMES INDUSTRIELS

Stuxnet (2010), Industroyer (2015-16), ShadowPad (2023) sont de redoutables logiciels malveillants. Ces *malwares*, pour reprendre le terme anglais, développés sous licence « étatique » ont des finalités spécifiques (récupération de compte, destruction physique d'équipement, porte dérobée, …) qui, combinés, permettent de délivrer des effets dévastateurs sur les systèmes industriels.

Il existe de nombreux autres logiciels malveillants. Néanmoins au travers de ces 3 exemples il est possible de se rendre compte de la sophistication obtenue en un peu plus de 10 ans. Les organisations industrielles ont donc l'obligation de comprendre le fonctionnement de ces malwares et les procédés utilisés pour les mettre en œuvre afin d'y apporter la réponse la plus efficace.

LES DIFFÉRENTS TYPES D'ATTAQUES ET LEURS CONSÉQUENCES

Les cyberattaques peuvent être caractérisées par l'intention, le but recherché par les auteurs et par les moyens dont ils disposent. Il existe plusieurs types de malwares (logiciel malveillant) qui sont utilisés par les cyberattaquants :

LES VIRUS INFORMATIQUES

Des programmes malveillants qui s'attachent à des fichiers exécutables et se propagent lors de l'exécution de ces fichiers.

LES VERS INFORMATIQUES

Des programmes autonomes qui se propagent à travers les réseaux informatiques en exploitant les vulnérabilités des systèmes. Contrairement aux virus, ils n'ont pas besoin de fichiers hôtes pour se propager.

LES RANSOMWARES

Des logiciels malveillants qui chiffrent les fichiers d'un système informatique et demandent une rançon en échange de la clé de déchiffrement.

LES CHEVAUX DE TROIE

Des programmes malveillants qui se dissimulent dans des logiciels apparemment légitimes. Une fois installés sur un système, ils permettent aux cybercriminels d'accéder et de prendre le contrôle de l'ordinateur à distance.

LES LOGICIELS ESPIONS

Des programmes installés sur votre ordinateur, généralement à votre insu, qui capturent et transmettent des informations personnelles ou des habitudes et des détails de navigation Internet à son utilisateur.

LES ADWARES

Affichent des publicités non désirées sur un ordinateur, généralement sous forme de fenêtres pop-up intrusives.

LES CONSÉQUENCES PEUVENT ÊTRE MULTIPLES

- Pertes financières (coûts directs et indirects),
- Corruption, destruction ou exfiltration de données,
- Inaccessibilité des systèmes,
- Sabotage / blocage des installations,
- Risques de sécurité / salubrité / sureté
- Atteinte à l'image de l'organisation
- Risques juridiques

Pourquoi faut-il cybersécuriser IT et OT ?

Quelles que soient leur taille et secteur d'activité, les raisons qui amènent les entreprises industrielles à déployer une stratégie de cybersécurité sont les suivantes :

1. RÉPONDRE AUX OBLIGATIONS LÉGALES ET SE CONFORMER À LA RÉGLEMENTATION EN VIGUEUR

À l'instar des différentes organisations, les industries sont soumises à des exigences nationales et internationales. Il convient de respecter le Règlement Général sur la Protection des Données (RGPD) personnelles. La loi de programmation militaire (LPM) fixe des exigences particulières pour les opérateurs d'importance vitale (OIV). La directive NIS édicte une série de règles pour les systèmes d'informations des opérateurs de service essentiel (OSE). La directive NIS2 va renforcer (2e semestre 2024, décret d'application à venir) les exigences de la directive NIS et élargir le périmètre d'application à d'autres organisations (EE : Entités Essentielles et EI : Entités Importantes). À cela s'ajoutent les exigences réglementaires propres à chaque métier.

2. PRÉVENIR DES PERTURBATIONS DE LA PRODUCTION

Les attaques informatiques peuvent entraîner des perturbations dans les opérations de production (en s'attaquant aux équipements industriels, aux ERP, MES ...), ce qui peut entraîner des retards, des coûts supplémentaires et une perte de productivité. La cybersécurité permet de protéger les systèmes de contrôle industriel et les infrastructures critiques contre les attaques, elle garantit ainsi la continuité des opérations.

3. EXPLOITER EN TOUTE SÉCURITÉ

Il s'agit de protéger le personnel et l'environnement, les salariés et opérateurs de l'industrie, les consommateurs des biens produits, tout en écartant les potentiels risques environnementaux (ex : pollution).

4. PROTÉGER LES DONNÉES SENSIBLES

Éviter que des actifs industriels ne soient altérés et que des données confidentielles ne soient détruites, corrompues, volées, diffusées, soumises à rançon (atteinte à la Disponibilité, à l'Intégrité et à la Confidentialité) … Les entreprises industrielles stockent souvent des données sensibles telles que des plans de conception, des données de fabrication ou des informations sur les clients (personnel, données financières, stratégie d'entreprise, contrat…). La cybersécurité permet de protéger ces données contre les cyberattaques et les fuites potentielles, ce qui préserve la confidentialité, l'intégrité et la disponibilité des informations.

5. PROTÉGER LA PROPRIÉTÉ INTELLECTUELLE

L'industrie est souvent confrontée à des enjeux de propriété intellectuelle, avec des innovations, des brevets et des technologies développées en interne. La cybersécurité réduit le risque de vol ou de compromission de ces informations stratégiques, les investissements consacrés, dans un contexte où le sujet de la concurrence est omniprésent.

6. GARANTIR LA CONFIANCE DES CLIENTS ET DES PARTENAIRES

Le niveau de maturité en cybersécurité d'une industrie s'impose désormais comme un critère de choix d'une entreprise, d'un fournisseur ou d'un partenaire commercial.

[7] RGPD : Règlement Général sur la protection des données, applicable pour la protection des données personnelles
[8] CNIL : Commission Nationale Informatique et Liberté Le cadre national | CNIL
[9] LPM : Loi de Programmation Militaire fixe les exigences de sécurité qui s'imposent aux opérateurs régulés
[10] Directive NIS 2 : ce qui va changer pour les entreprises et l'administration françaises | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
[11] European Cyber Resilience Act (CRA) (european-cyber-resilience-act.com)
[12] Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

La mise en place d'une stratégie de cybersécurité repose sur un corpus réglementaire et normatif :

- L'ISO 27001 fixe les conditions pour mettre en place un système de management de la sécurité de l'information (SMSI).
- Le traitement des données personnelles et des bases de données doit être en conformité avec le RGPD[7] et les recommandations de la CNIL[8].
- Pour les opérateurs régulés (OIV, OSE) tenir compte des exigences fixées par la LPM[9].
- La Directive NIS 2 (Network and Information Security édition 2)[10] et le CRA (Cyber Resilience Act)[11] renforcent ce corpus en fixant de nouvelles obligations de cybersécurité et de souveraineté applicables au sein de l'union européenne.
- Selon le contexte et le domaine considéré, s'appuyer sur les différents guides et bonnes pratiques édités par l'ANSSI[12].

À RETENIR

L'investissement, c'est-à-dire la détermination et les ressources consacrées au service de la cybersécurité industrielle, est particulièrement vertueux. Il garantit la protection du patrimoine numérique d'une entreprise, préserve son fonctionnement, favorise son développement et sa croissance économique. En outre, il conditionne le niveau de maturité en cybersécurité d'une industrie qui est, désormais, à la fois un indicateur de confiance et un critère de choix.

Comment aborder votre projet de cybersécurité ?

➔ Beaucoup d'organisations, et notamment dans l'industrie, ne savent pas comment engager un processus de cybersécurité. Faut-il démarrer par une approche globale et une vision 360° ou faut-il cibler chaque action sur un périmètre défini ?

La norme internationale ISO 27001 spécifie les exigences relatives à l'établissement et à la mise en œuvre d'un système de management de la sécurité de l'information et recommande d'adopter une approche globale de la cybersécurité qui comprend :

1. La prise en compte du contexte de l'organisation.
2. L'engagement de la direction et des parties prenantes.
3. La conduite d'un diagnostic de cybermaturité avec analyse des risques.
4. L'application d'un plan d'action et de remédiation.
5. La mise en œuvre d'un processus de veille et d'amélioration continue.

LES ÉTAPES PRINCIPALES

	1. PRENDRE CONSCIENCE DE L'IMPORTANCE DE SE SÉCURISER	2. CONNAITRE LA SITUATION INITIALE	3. FAIRE LES PREMIÈRES ACTIONS DE SENSIBILISATION	4. MAINTENIR LA SÉCURITÉ DANS LE TEMPS
POURQUOI ?	• Suite contrainte légale • Attaque subie ou redoutée • Prise de conscience des enjeux techniques, financiers, humains, environnementaux	• Savoir d'où l'on part et quels sont les risques	• Première campagne de sécurisation qui fermera les plus importantes vulnérabilités et les plus faciles à mettre en oeuvre (quickwin)	• S'assurer que le système garde un niveau de sécurité minimal
QUOI ?	• Sensibiliser les parties prenantes • Définir un pilote	• Définir le périmètre • Réaliser un diagnostic • Cartographier le système • Faire l'inventaire matériel et logiciel • Faire une analyse de risque	• Sensibiliser les utilisateurs • Sécuriser les systèmes, les réseaux, les données, les postes utilisateurs, les équipements, les accès • Définir les procédures de continuité et de reprise d'activité	• Réaliser des veilles de vulnérabilité • Maintenir en conditions de sécurité • Maintenir les sensibilisations
QUI ?	• Direction générale • Service informatique	• Expert diagnostic cybersécurité • Service informatique	• Service informatique • Sous-traitant	• Service informatique • Sous-traitant

PRENDRE EN COMPTE LE CONTEXTE DE L'ORGANISATION

Afin d'identifier de façon aussi exhaustive que possible le périmètre d'application de la cybersécurité et les actifs numériques à protéger, il convient de prendre en compte le cadre particulier et les spécificités propres à l'industrie considérée.

Cela concerne toutes les données numériques qui ont de la valeur pour le système de production de l'entreprise et qui nécessitent d'être protégées :

- Les produits référencés ou façonnés par le système industriel ;
- Les configurations de chacun des composants du système industriel : sous-systèmes, machines, automates, capteurs, objets connectés ;
- Les interfaces qui permettent l'interconnexion à d'autres systèmes, qu'ils soient internes comme externes (clients, partenaires, sous-traitants, prestataires…).

Il s'agit de recueillir suffisamment de détails afin de pouvoir procéder à une bonne appréciation des risques cyber. Cela comprend notamment l'architecture du système industriel ainsi que la cartographie des différents composants et sous-systèmes : automates, postes de travail, stations opérateurs, équipements actifs du réseau, périphériques, sans oublier les liens qui modélisent toutes les connexions entre les sous-systèmes.

Pour chacun des composants, l'inventaire doit détailler la référence, la version, sa configuration, etc…

IMPLIQUER LA DIRECTION ET LES PARTIES PRENANTES

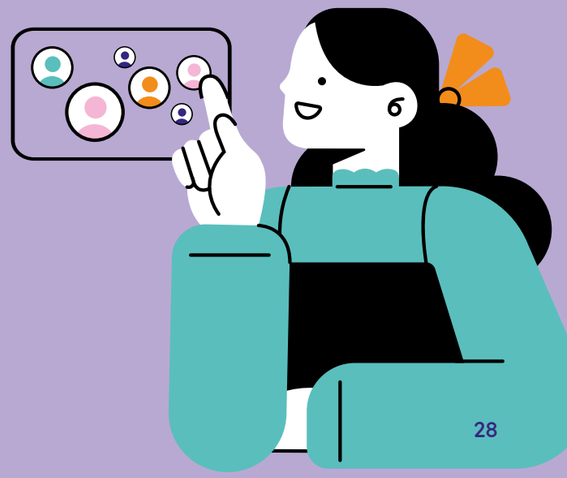
La mise en place d'un système de management de la sécurité d'un système d'information est conditionnée par l'implication et le leadership de la direction de l'organisation considérée.

Cela consiste, d'une part, en obtenant un engagement clair de la direction concernant les objectifs à atteindre et le périmètre d'application de la stratégie de cybersécurité et, d'autre part, en s'assurant que tous les moyens nécessaires, humains et financiers, seront mis en œuvre pour adopter et déployer cette stratégie.

L'efficacité de la démarche est également conditionnée par l'implication de toutes les parties prenantes : les experts métier et toutes les directions (DAF, RH, COM, juridique) qu'il est nécessaire de mettre à contribution pour apprécier de la façon la plus précise les risques, les conséquences potentielles et les mesures de sécurisation à adopter.

Le propriétaire de chaque actif doit contribuer à la démarche d'analyse des risques et à l'élaboration du plan de traitement. Il est celui qui peut le mieux déterminer la valeur que chaque actif représente pour l'entreprise.

C'est également lors de cette première étape qu'il faut sensibiliser tous les acteurs de l'entreprise sur les enjeux de cybersécurité, sur le processus qui sera mis en œuvre et sur le rôle que chaque membre de la société joue, de façon directe et indirecte.



CONDUIRE UN DIAGNOSTIC DE CYBERSÉCURITÉ

L'ANALYSE DES RISQUES

Cette démarche s'appuie sur une analyse des risques cyber (référence ISO 27005[13]). Elle se compose, en impliquant les experts métier de l'entreprise, d'une identification de façon aussi exhaustive que possible des menaces potentielles qui pèsent sur les actifs numériques de l'entreprise et sur le fonctionnement de son système de production. Cela afin d'évaluer l'impact et d'adopter des mesures de sécurité nécessaires pour les réduire ou les interdire. Cette démarche comprend notamment :

L'identification des vulnérabilités
L'analyse des risques permet d'identifier les points faibles dans les systèmes informatiques, les réseaux et les applications utilisés par l'entreprise. Cela inclut les failles de sécurité potentielles qui pourraient être exploitées par des attaquants.

L'évaluation des menaces
L'analyse des risques permet de déterminer les types de menaces et d'attaques auxquelles l'entreprise est susceptible d'être exposée. Cela peut inclure des attaques par hameçonnage, des logiciels malveillants, des attaques par déni de service (DDoS), etc.

L'évaluation de l'impact potentiel
En identifiant les menaces possibles, l'analyse des risques permet d'évaluer l'impact potentiel que ces attaques pourraient avoir sur les opérations et les activités de l'entreprise en termes de conséquences, de vraisemblance et de gravité.

La priorisation des mesures de sécurité à adopter
L'analyse des risques aide à hiérarchiser les mesures de sécurité à mettre en place en fonction de la probabilité et de l'impact des menaces identifiées. Cela permet de cibler les ressources à consacrer en faisant les efforts sur les domaines les plus critiques.

Une prise de décision éclairée
En comprenant les risques auxquels l'entreprise est exposée, les dirigeants peuvent prendre des décisions argumentées concernant les investissements à engager (financiers et humains) en matière de sécurité informatique ainsi que les stratégies de protection à adopter, sous la forme d'un plan de traitement des risques.

Conformité réglementaire
Dans chaque secteur, les entreprises sont soumises à des exigences particulières en matière de cybersécurité. L'analyse et le plan de traitement des risques induits, documentés, permettent de démontrer que les mesures appropriées ont été prises pour se conformer à ces réglementations.

La sensibilisation à la sécurité
L'analyse des risques permet de sensibiliser les collaborateurs et les membres de l'entreprise aux risques informatiques et à l'importance de la sécurité des données et des systèmes.

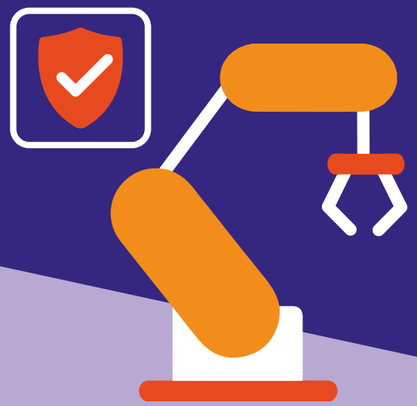
L'analyse des risques est une démarche indispensable pour protéger efficacement les actifs informatiques d'une entreprise, minimiser les risques d'attaques et assurer la continuité des activités dans un environnement de plus en plus connecté et vulnérable aux cybermenaces.

[13] ISO 27005 techniques de sécurité, gestion des risques liés à la sécurité de l'information

RETOUR D'EXPÉRIENCE : DIAGNOSTIC DE CYBERSÉCURITÉ EN ENVIRONNEMENT INDUSTRIEL

Charbonneaux Brabant, une entreprise familiale fondée en 1797 à Reims, spécialisée dans la fabrication de condiments et de produits d'entretien, a récemment réalisé un diagnostic de cybersécurité en partenariat avec un prestataire référencé par la Région Grand Est. Voici un résumé des principaux points de leur expérience :

Raison du diagnostic :
Charbonneaux Brabant a décidé de réaliser ce diagnostic pour évaluer précisément sa vulnérabilité face aux menaces cybernétiques, compte tenu de l'absence d'expertise interne dédiée à cette problématique et de l'opportunité financière offerte par la Région Grand Est.



Focus du diagnostic
L'entreprise a mis l'accent sur deux aspects majeurs : l'audit technique visant à évaluer les risques potentiels pour leurs systèmes de production en cas d'attaque, et la gouvernance afin d'établir un plan d'action à long terme en concertation avec la direction.

Implication des métiers
Le diagnostic a permis un échange avec les métiers, notamment en sensibilisant l'ensemble du personnel et en renforçant la sécurisation des transferts de données entre les différentes activités de l'entreprise.

Atteinte des objectifs
Le diagnostic a pleinement atteint ses objectifs en fournissant un rapport d'audit technique détaillé, une restitution transparente avec la direction, et un plan d'actions sur plusieurs années adapté au contexte spécifique de l'entreprise.

Mise en œuvre du plan d'actions
Malgré les progrès réalisés, la mise en œuvre du plan d'actions reste un défi en raison de contraintes de ressources, nécessitant une gestion rigoureuse et des arbitrages réguliers.

Sentiment de sécurité accru
Bien que le diagnostic ait renforcé la maturité cyber de l'entreprise, celle-ci reste consciente de la nécessité de maintenir une vigilance constante et d'adapter son plan d'actions en fonction de l'évolution des menaces.

Les prestataires référencés par la Région Grand Est soulignent l'importance de prendre en compte les spécificités industrielles lors de ces diagnostics et mettent en avant la nécessité d'une collaboration étroite entre les équipes métiers et informatiques pour garantir une sécurité optimale.

LE DIAGNOSTIC DE CYBERSÉCURITÉ

Un diagnostic Cybersécurité permet d'améliorer la prise en compte du risque cyber en évaluant le niveau de sécurité du système d'information d'une entreprise sur les aspects organisationnels et techniques. Cela revient à évaluer la sécurité des interconnexions, identifier les actifs critiques, les vulnérabilités potentielles ...

Les non-conformités relevées par rapport à la réglementation et aux normes métier ainsi que les failles techniques de sécurité détectées servent à lister et à qualifier, par ordre de criticité et de priorité de traitement, toutes les vulnérabilités d'un système d'information.

L'offreur de service en cybersécurité, choisi pour conduire le diagnostic, peut ainsi établir, en relation étroite avec la direction et les experts métier de l'entreprise, un plan d'action et de remédiation adapté au contexte, à la stratégie et aux objectifs de l'entreprise.

La Région Grand Est a mis en place un diagnostic de cybersécurité qui permet d'évaluer le niveau de maturité en cybersécurité d'une entreprise, d'identifier les failles (organiques, techniques) et de proposer un plan d'action et de remédiation. Ce diagnostic est subventionné à hauteur de 50% du cout total plafonné à 10 000€.
(cf annexe)

APPLIQUER LES MESURES CORRECTIVES NÉCESSAIRES

Il s'agit de mettre en œuvre, de façon autonome ou accompagné d'un offreur de cybersécurité, le plan d'action et de remédiation issu du diagnostic de cybersécurité. Les bonnes pratiques de sécurité s'appliquent aux systèmes IT et OT, ce qui les différencie ce sont les solutions de sécurité mises en place qui doivent être compatibles avec l'environnement industriel considéré.

Tout commence par respecter les bonnes pratiques suivantes :

Segmenter les réseaux IT et OT en utilisant des équipements et/ou techniques adaptés (pare-feu, réseaux virtuels, air-gap ou réseaux physiques distincts). Cette ségrégation réduit les risques de propagation d'une cyberattaque, d'un domaine à l'autre, et limite les mouvements latéraux des personnes malveillantes ;

Mettre en place une surveillance continue en déployant des outils de détection d'intrusion (IDS/IPS), des systèmes d'analyse des journaux d'événements (SIEM) et d'autres solutions de surveillance (XDR) pour détecter rapidement les activités suspectes ou malveillantes dans les environnements IT et OT ;

Renforcer l'authentification en déployant des mécanismes d'authentification robustes tels que l'authentification à deux facteurs ;

Mettre à jour et patcher régulièrement tous les systèmes, logiciels et équipements dans les environnements IT et OT avec les derniers correctifs de sécurité. Cela permet de combler les vulnérabilités connues et de réduire les risques d'exploitation ;

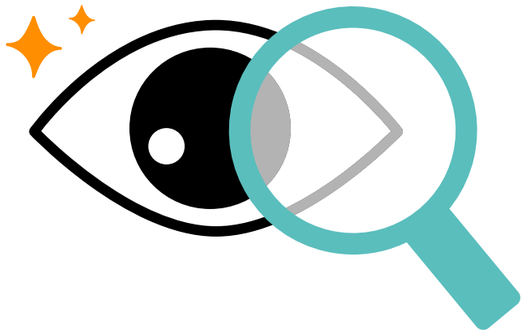
Appliquer des contrôles d'accès stricts en limitant l'accès physique et logique aux systèmes IT/OT par la mise en place de contrôle d'accès approprié ;

Sensibiliser et former régulièrement le personnel concerné aux risques de sécurité liés aux interactions entre OT/IT. L'organisation doit faire en sorte que tous les collaborateurs comprennent les bonnes pratiques en matière de sécurité, comme l'identification des tentatives de phishing, la gestion des mots de passe forts, l'utilisation de périphériques non validés (clé USB fournisseur par exemple) et la protection des informations sensibles ;

Collaborer avec les fournisseurs et les partenaires, et établir des relations de confiance avec les fournisseurs et les partenaires impliqués dans les interconnexions IT/OT. S'assurer que les contrats et les accords de niveau de service (Service Level Agreement) incluent des exigences de sécurité claires et veiller à ce que les fournisseurs respectent ces exigences ;

Adopter une approche de défense en profondeur, en mettant en place des couches de sécurité multiples pour renforcer la protection de vos interconnexions IT/OT. Cela peut inclure des pare-feux, des systèmes de détection d'intrusion, des solutions de sécurité des points finaux (postes informatiques, smartphones et périphériques), des contrôles d'accès physiques, des sauvegardes régulières des données, etc. ;

Mettre en place un processus de gestion des vulnérabilités pour identifier, évaluer et atténuer les vulnérabilités des systèmes IT/OT. Une approche de la priorisation des correctifs en fonction du niveau de risques est à effectuer.



CONSOLIDER LA STRATÉGIE DE CYBERSÉCURITÉ ET LA MAINTENIR AU MEILLEUR NIVEAU DE L'ÉTAT DE L'ART

Afin de maintenir la cybersécurité au meilleur niveau de l'état de l'art, il est nécessaire de surveiller et de mesurer l'efficacité de la stratégie de cybersécurité de l'entreprise.

Cela passe par la mise en place d'un processus de surveillance de mesurage et d'analyse des informations de sécurité délivrées au fil de l'eau par les différents capteurs et outils de gestion de la cybersécurité :

Mettre en place une gestion des incidents en développant et en testant le plan de réponse aux incidents pour les interconnexions IT/OT. Ce plan devrait inclure des procédures de détection, d'isolement et de résolution des incidents, ainsi que des mécanismes de communication et de notification appropriés.

Il s'agit également de planifier des audits internes afin de recueillir les informations complémentaires qui permettent de vérifier que la stratégie de cybersécurité est toujours efficace et bien mise en œuvre, en prenant notamment en compte l'évolution de la menace et des outils de sécurité :

Effectuer des tests d'intrusion et des audits de sécurité. Mener régulièrement des tests d'intrusion pour évaluer la résistance de vos systèmes IT/OT aux attaques. Effectuer également des audits de sécurité pour identifier les lacunes potentielles dans vos mesures de sécurité - et prendre des mesures correctives.

Une nouvelle analyse des risques doit être conduite dès lors qu'une évolution significative de la menace est observée ou que l'obsolescence d'un outil de cybersécurité est identifiée, ceci afin d'adopter les mesures correctives nécessaires pour maintenir la cybersécurité au meilleur état de l'art.

Présentation de cas d'usages concrets

CAS D'USAGE 1 : TRAÇABILITÉ DES ACCÈS AUX APPLICATIONS DE PILOTAGE DES AUTOMATES INDUSTRIELS

Sur un site industriel, on retrouve en général quatre types d'équipes et d'applications, qui peuvent être portées par des réseaux distincts :

- **La supervision :** le monitoring, les tableaux de bord, les alarmes ;
- **L'acquisition :** la remontée des données ;
- **La conduite :** les postes utilisateurs, « engineering Workstation », avec les applications de pilotage, les automates ;
- **La maintenance :** les interventions de maintenance sur les applications et les équipements.

Les actions de conduite et de maintenance des automates exigent un haut niveau de sécurité et de traçabilité. C'est pourquoi, il est indispensable de pouvoir identifier « qui a fait quoi et quand » sur quel équipement, sur quel système ou sur quelle application.

Il est ici question d' « imputabilité » : c'est-à-dire être capable d'identifier, voire de prouver « qui a fait quoi et quand » sur une installation industrielle.

Sous l'effet de la numérisation croissante des systèmes de production, combinée avec des exigences contractuelles ou réglementaires de cybersécurité de plus en plus forte, la gestion des accès logiques est devenue un sujet central. Avec pour corollaire, le suivi détaillé des actions réalisées sur le système de production, des systèmes dont on peut aujourd'hui prendre le contrôle à distance.

Les postes ou les comptes génériques partagés sont amenés à disparaitre car ils ne sont plus en conformité avec les exigences de cybersécurité. Il est indispensable désormais d'adopter une politique rigoureuse de gestion des identités et des accès, qu'ils soient physiques ou logiques, du personnel qui intervient dans la conduite et la maintenance de l'infrastructure industrielle.

Les solutions de gestion des identités et des accès (IAM[14]), ainsi que les solutions de gestion des accès à privilèges (PAM[15]) mis en place sur les systèmes d'information de gouvernance de l'entreprise (IT), sont également déployés au profit des systèmes d'exploitation (OT).

[14] Identity Access Management
[15] Privileged Access Management

Ces solutions présentent plusieurs avantages :

L'adoption d'une solution unique de gestion des accès, quels que soient les cas d'usage, afin de s'affranchir des particularités propres à chaque fabricant de machines et favoriser une expertise utilisateur partagée.

Un outil d'authentification centralisé : la sécurisation via un accès unique qui peut être renforcé par l'adoption d'une solution d'authentification multi facteurs (Multi-Factor Authentification ou MFA), avec un même MFA déployé sur l'ensemble des systèmes, au lieu d'autant de solution d'authentification que de systèmes déployés, chaque fabricant de machine proposant une solution différente.

Une solution unique de traçabilité détaillée des flux et des échanges numériques, utilisable quels que soient les fabricants de machines. Il s'agit de pouvoir disposer de bilans et d'audits d'activité, ou d'enregistrements vidéos qui permettent, sur la base d'un référentiel de comptes utilisateurs individuels bien identifiés et tenus à jour, de savoir qui a fait quoi et quand sur tel équipement, système ou application.

Un outil de génération et de gestion sécurisée des mots de passe qui permet de limiter la multiplication des mots de passe (avec le risque qu'un utilisateur finisse par les noter sur des post-it) ou encore d'écarter le risque du partage d'un même identifiant et d'un même mot passe par plusieurs utilisateurs.

L'adoption d'une politique de mots de passe qui impose le changement régulier des mots de passe, sans avoir recours à une intervention humaine, avec le déploiement d'une solution de contrôle automatique des renouvellements et de la robustesse des mots de passe.

Les applications de conduite de systèmes industriels sont souvent des applications assez lourdes, hébergées sur un poste dédié qui peut être propre à un fabricant de machine. Les solutions PAM ne gèrent pas nativement les sessions des protocoles industriels. Ces protocoles, entre les applications et les équipements, sont des protocoles standards industriels qui se démarquent des protocoles informatiques.

L'utilisation d'une solution de PAM dans l'industrie permet en revanche de tracer l'utilisation des différentes applications de conduite des systèmes d'exploitation.

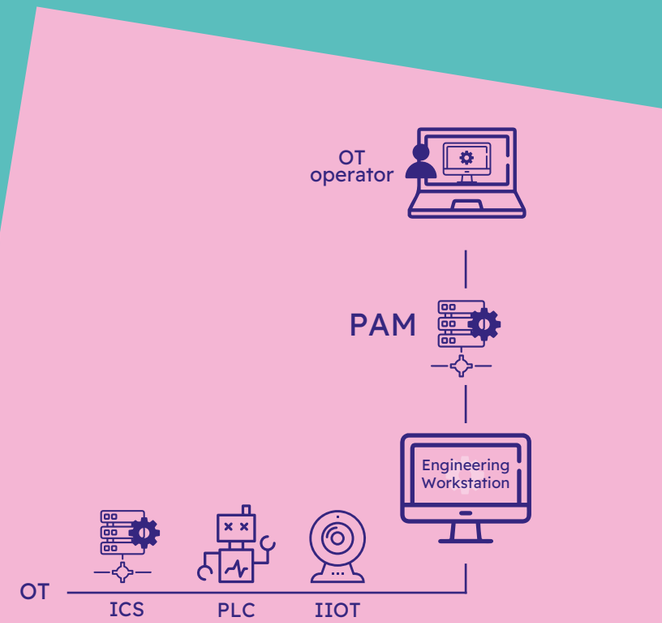
On distingue à cet effet deux architectures.

ARCHITECTURE 1 : ENGINEERING WORKSTATION DÉPLOYÉE "ON PREMISE" SUR LE SYSTÈME D'EXPLOITATION

A1 : Engineering Workstation déployée « on premise » sur le système d'exploitation, consiste à donner aux opérateurs qui interviennent sur les équipements d'un fabricant de machine déterminé, un accès aux postes « engineering Workstation » qui hébergent les applications propriétaires dudit fabricant. Le déploiement en amont d'une solution PAM permet de tracer et d'enregistrer toute l'activité effectuée par l'opérateur.

Dans cette configuration, l'application de pilotage est déployée sur un poste dans le réseau industriel, avec d'un côté le réseau d'accès à l'application, et de l'autre le réseau d'accès aux équipements et aux automates.

Tout le système (pilotage et équipements) est hébergé dans le datacenter de l'usine de l'entreprise, qui dispose alors de toutes les licences d'utilisation des applications de conduite des systèmes.



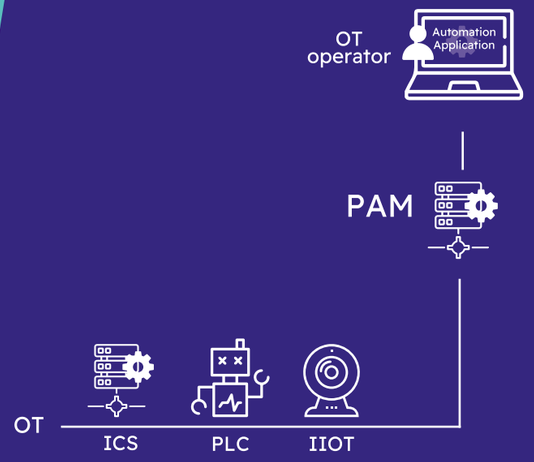
ARCHITECTURE 2 : INTERVENTION À DISTANCE

A2 : intervention à distance, correspond au cas d'une entreprise ayant déployé des équipements et des systèmes d'un fabricant de machine et qui souhaite lui (à lui ou à un prestataire) permettre le calibrage et la maintenance à distance. Il s'agit dans ce cas de permettre un accès distant sécurisé.

Dans le cas de la première architecture (A1) – sous réserve de disposer des licences d'utilisation des applications pour des tiers - l'entreprise peut donner au fabricant un accès à privilèges, distant, au travers de la solution de PAM au poste de travail local qui héberge les applications considérées. Toutes les actions du fabricant ou du prestataire seront alors tracées et enregistrées.

Si l'entreprise ne dispose pas de licence d'utilisation pour des tiers, elle pourra permettre au fabricant, ou au prestataire mandaté, d'utiliser ses propres applications avec ses propres licences. Celles-ci interagiront à distance avec les automates de l'entreprise, tous les détails de cette activité devront également être tracés et enregistrés.

L'architecture du système d'exploitation sera alors sensiblement différente selon les fabricants. Le choix de l'architecture de la solution de PAM est déterminant : dans tous les cas, elle doit permettre de s'intégrer dans une architecture de réseau industriel, tout en sécurisant l'accès aux applications et aux équipements.



D'une manière générale, les réseaux locaux d'automates sont isolés par des diodes réseaux sortantes. La solution doit fonctionner dans des environnements réseaux hautement sécurisés, en partant du principe que l'accès doit toujours se faire depuis la zone la plus sécurisée vers la zone la moins sécurisée.

Dans le cas de l'accès distant sécurisé, on distingue deux types d'architecture :

1

La première - à privilégier car plus sécurisée - s'appuie sur la mise en place d'un « tunnel sécurisé » de bout en bout, depuis la « sortie » de l'application de pilotage jusqu'à la passerelle d' « entrée » dans le réseau industriel. Réseau industriel sur lequel se trouvent les automates, dans lequel passent les protocoles industriels de connexion aux automates et aux équipements.

2

La seconde basée sur le déploiement d'un « VPN » (idéalement un VPN qui filtre les flux au niveau des adresses réseaux et des ports d'entrée sur les serveurs), qui permet à l'application de pilotage d'être sur « le même réseau » que le réseau des automates et des équipements.

CAS D'USAGE 2 : OBSOLESCENCE DU SYSTÈME DE SÉCURITÉ, ÉVOLUTION DE LA MENACE ET DU RISQUE INDUIT : DE LA NÉCESSITÉ DE CONDUIRE UNE NOUVELLE ANALYSE DES RISQUES.

Un système de contrôle commande d'installation industrielle a été déployé en 2010 chez un industriel français de taille moyenne. En 2020, au vu de l'augmentation du nombre des attaques et des conséquences potentielles de neutralisation ou d'altération du système d'exploitation, l'industriel a souhaité réévaluer le niveau de cybersécurité de son dispositif.

Une analyse de risque a ainsi été mandatée et réalisée selon la méthode EBIOS[16] de l'ANSSI.

Le niveau de protection recherché par l'industriel correspondait à la classe 2[17] des systèmes industriels de l'ANSSI[18].

Pour les systèmes industriels de classe 2, pour lesquels le risque ou l'impact d'une attaque est significatif, il n'y a pas de contrôle réalisé par l'Etat, mais l'entité responsable doit pouvoir apporter la preuve de la mise en place des mesures adéquates en cas de contrôle ou d'incident.

Les prestations qui ont été réalisées pour conduire cette démarche vertueuse comprennent :

- Analyse de risque Cybersécurité (EBIOS ou autre méthode).
- Analyse détaillée du système existant.
- Mise en place d'une infrastructure d'administration centralisée (Active Directory Windows redondé primaire & secondaire).
- Sécurisation des serveurs et des postes opérateur.
- Sécurisation des accès de la télémaintenance.
- Mise en place d'une gestion centralisée des logs (Syslog).
- Simulation d'attaque Cybersécurité avec scénarios de mise en oeuvre virtuelle, Rédaction de fiches réflexes.
- Sensibilisation des opérateurs à la Cybersécurité (formation issue du référentiel SecNumEdu[19] de l'ANSSI).
- Élaboration du socle documentaire (Plan d'Assurance Cybersécurité ; Plan de Développement Sécurité ; Plan d'Exécution Sécurité).
- Élaboration des Fiches des risques résiduels.

→ **Le niveau de sécurité de l'installation a été fortement augmenté et les actions de maintien en conditions de sécurité à venir vont maintenir dans le temps un certain niveau de sécurité.**

[16] anssi-guide-ebios_risk_manager-en-v1.0.pdf
[17] securite_industrielle_GT_methode_classification-principales_mesures.pdf
[18] La cybersécurité des systèmes industriels | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
[19] SecNumEdu | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

Conclusion

Le risque cyber appliqué aux systèmes industriels est encore mal compris ou sous-estimé. Les entreprises industrielles ne prennent pas suffisamment en compte les risques qui pèsent sur leur activité et ne mesurent pas assez finement l'impact potentiel des cybermenaces sur leur système de production et sur leur supply chain.

Faire un état des lieux. Le déploiement par la région Grand Est d'un diagnostic de cybersécurité co-financé doit servir de catalyseur pour apprécier le niveau de cybermaturité de l'entreprise industrielle et opérer les actions de remédiation nécessaires pour renforcer sa cybersécurité.

Rapprocher les Industriels et les experts de la cybersécurité. Il convient d'apprécier, au plus près du terrain, les risques et les spécificités propres à chaque activité industrielle, de façon à adopter les mesures de sécurité et de remédiation les plus efficaces.

Définir un socle robuste de cybersécurité. Il est indispensable de respecter les exigences de cybersécurité (réglementation et normes métiers) appliquées à l'IT et à l'OT. Il convient à cet effet d'adopter les outils et les processus qui correspondent au mieux, en termes d'objectifs, de performances et de coût au contexte spécifique du système industriel considéré.

Favoriser une gestion dynamique de la cybersécurité. Le socle de cybersécurité doit être renforcé en mettant en place une gestion proactive de la cybersécurité afin de détecter au plus tôt les comportements anormaux, l'obsolescence des outils de sécurité, planifier les opérations de mise à jour et de maintenance. Il s'agit de réagir au plus vite pour limiter au maximum le risque d'un arrêt ou d'une altération du système d'information.

Anticiper les cybermenaces. En adoptant des outils et une stratégie de Cyber Threat Intelligence (collecte d'information sur les menaces ou les acteurs de la menace) adaptée au contexte de l'entreprise. Mettre en œuvre un processus de veille sur les cybermenaces et sur les technologies de cybersécurité adapté aux systèmes et environnements industriels.

→ **Le plan régional de cybersécurité adopté par la Région Grand Est vient en appui de cette dynamique vertueuse pour réussir la transformation numérique des entreprises, en bénéficiant de l'expertise des offreurs de service et de solution de territoire maintenus au meilleur niveau de l'état de l'art.**

La Région Grand Est à vos côtés

LES DISPOSITIFS MIS EN PLACE PAR LA RÉGION POUR VOS PROJETS DE CYBERSÉCURITÉ INDUSTRIELLE

LE DIAGNOSTIC RÉGIONAL DE CYBERSÉCURITÉ

Pour renforcer la prévention des risques cyber, un diagnostic de cybersécurité a été élaboré par la Région Grand Est en 2022.

La Région a procédé à un référencement de prestataires spécialisés en cybersécurité pour mettre en œuvre le diagnostic à l'été 2022 et 25 prestataires ont été retenus : https://www.grandest.fr/wp-content/uploads/2022/10/liste-prestataires-references-diagnostic-cybersecurite-grand-est-26-10-2022-2.pdf

Le diagnostic permet d'évaluer le niveau de maturité en cybersécurité de son entreprise et définir un plan d'actions, à travers un audit organisationnel et un audit technique, d'une durée d'environ 10 jours/homme. Toute entreprise immatriculée dans le Grand Est est éligible.

La Région peut rembourser jusqu'à 50% d'une prestation plafonnée à 10 000€, soit un montant d'aide de 5000€ maximum.

Plus d'informations sur la page de présentation du dispositif : https://www.grandest.fr/vos-aides-regionales/diagnostic-cybersecurite/

C'est également sur cette page qu'on accède au téléservice de demande d'aide.

GRAND EST COMPÉTITIVITÉ

C'est un dispositif d'accompagnement des entreprises industrielles ou de services à l'industrie qui comprend une aide à l'investissement productif.

Les projets de cybersécurité industrielle sont éligibles à la condition d'avoir effectué un diagnostic régional de cybersécurité.

L'aide régionale peut atteindre 400 000€ en fonction du projet, de la taille d'entreprise et de la réglementation en vigueur

Plus d'informations sur le dispositif et la procédure sur la page de présentation du dispositif : https://www.grandest.fr/vos-aides-regionales/grand-est-competitivite/

L'EDIH GRAND EST

Les pôles européens d'innovation numérique (EDIH) sont des guichets de l'écosystème manufacturier pour l'adoption de nouvelles technologies – IA, cybersécurité puis HPC (High Performance Computing et IoT) pour obtenir des processus industriels et de chaîne d'approvisionnement compétitifs et durables.

L'EDIH Grand Est est un point d'entrée unique solide pour aider les entreprises manufacturières Grand Est à trouver des investissements, accéder à des connaissances, à la recherche, aux réseaux clés grâce à ses partenariats et à sa présence dans plusieurs initiatives et programmes européens.

Avec le réseau EDIH, la Commission européenne souhaite ainsi créer une communauté dynamique de pôles et d'autres parties prenantes favorisant la mise en réseau, la coopération et les activités de transfert de connaissances entre l'EDIH, les PME et les entreprises de taille intermédiaire et les autres parties prenantes et initiatives concernées. Le Digital Transformation Accelerator (DTA) soutient la réalisation de cet objectif, en gérant la présence web du réseau et en hébergeant la plateforme logicielle et les outils appropriés, y compris le catalogue en ligne des EDIH.

GRAND EST CYBERSÉCURITÉ

Le centre régional d'assistance aux victimes de cyberattaques (CSIRT) a été mis en place par la Région Grand Est avec l'appui de l'ANSSI.

Depuis février 2023, il permet à toute entreprise industrielle victime de cyberincident sur son système d'information (IT) ou son système industriel (OT) d'appeler gratuitement l'équipe d'analystes de Grand Est Cybersécurité pour :

- qualifier l'incident,
- connaître et appliquer les premières recommandations de cybersécurité (fiches de bonnes pratiques),
- être mis en relation, si l'incident est grave, avec des prestataires en cybersécurité, spécialisés dans la remédiation et référencés par Grand est cybersécurité,
- être accompagné dans les démarches de déclaration à la CNIL et le dépôt de plainte auprès de la Gendarmerie et la Police Nationales.

L'équipe est joignable au 0 970 512 525 (appel non surtaxé).

Toutes les informations sur l'offre de service de Grand Est cybersécurité sont disponibles via le lien suivant : https://www.cybersecurite.grandest.fr

Glossaire

Sources documentaires : Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr) ; ENISA (europa.eu) ; ISO 27000.

A

Actifs : dans le processus d'analyse des risques, les différents éléments des systèmes étudiés sont appelés « biens » ou « actifs », traduction de l'anglais « assets ». Un bien est un élément ou une ressource du système étudié. Un bien est géré par un propriétaire ou dépositaire (owner).
On rencontre différentes catégories de biens :

- matériel : cela comprend les systèmes d'ordinateurs et autres dispositifs de traitement de données, de stockage de données et de communication de données ;
- logiciel : dans cette catégorie, on trouve les systèmes d'exploitation, les utilitaires système et les applications ;
- données : cela comprend les fichiers et bases de données, ainsi que les données relatives à la sécurité, telles que fichiers de mots de passe ;
- installations et réseaux de communication : ce sont les équipements permettant la communication par le réseau local et étendu comme les routeurs, switch, etc.

Air-Gap : En sécurité informatique, un air gap, aussi appelé air wall, est une mesure de sécurité consistant à isoler physiquement un système à sécuriser. Cette implémentation rend toute tentative de piratage à distance impossible, quelle que soit sa sophistication. Cette mesure permet un niveau de sûreté très élevé mais présente des contraintes d'exploitations importantes. Elle est en général limitée aux systèmes critiques.

Analyse du risque : processus mis en œuvre pour comprendre la nature d'un risque et pour déterminer le niveau de risque. L'analyse du risque fournit la base de l'évaluation du risque et des décisions relatives au traitement du risque. L'analyse du risque inclut l'estimation du risque.

Appréciation du risque : ensemble du processus d'identification du risque, d'analyse du risque et d'évaluation du risque.

Authentification : méthode permettant de garantir qu'une caractéristique revendiquée pour une entité est correct.

C

Contrôle d'accès : moyens mis en œuvre pour assurer que l'accès aux actifs est autorisé et limité selon les exigences propres à la sécurité et à l'activité métier.

Confidentialité : propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus (3.54) non autorisés.

Cybercriminalité : infractions commises dans le cyberespace ou avec des cybers moyens dans un but d'enrichissement.

Cyber extorsion : chantage exercé à l'aide de rançongiciels.

Cybersabotage et cyberterrorisme : dommages infligés aux infrastructures informatiques et à des biens physiques, parfois dans un but de démonstration de force et d'intimidation.

Cyber espionnage : accès non autorisé à des informations économiques, politiques ou militaires (confidentielles).

Cyberattaques lors de conflits : attaques hybrides et asymétriques pouvant aller jusqu'à une véritable cyberguerre.

D

Disponibilité : propriété d'être accessible et utilisable à la demande par une entité autorisée.

Désinformation et propagande : désorientation du public par la diffusion ciblée de fausses informations.

E

Edge Computing : pour informatique en périphérie ou informatique en périphérie de réseau, est une méthode d'optimisation employée dans le cloud computing qui consiste à traiter les données à la périphérie du réseau, près de la source des données.

I

IAM : (Identity Access Management), en français gestion des identités et des accès est une partie essentielle de la sécurité informatique globale qui gère les identités numériques et l'accès des utilisateurs aux données, aux systèmes et aux ressources au sein d'une organisation. La sécurité IAM comprend les politiques, les programmes et les technologies qui réduisent les risques d'accès liés à l'identité numérique au sein d'une entreprise. Les programmes IAM permettent aux organisations d'atténuer les risques, d'améliorer la conformité et d'accroître l'efficacité au sein de l'entreprise.

ICS : Industrial Control System, en français « le système de contrôle industriel », est un terme collectif utilisé pour décrire différents types de systèmes de contrôle et d'instruments associés, qui comprennent les dispositifs, les systèmes, les réseaux et les contrôles utilisés pour faire fonctionner et/ou automatiser les processus industriels.

Identification des risques : processus de recherche, de reconnaissance et de description des risques. L'identification du risque comprend l'identification des sources de risque, des événements, de leurs causes et de leurs conséquences potentielles. L'identification du risque peut faire appel à des données historiques, des analyses théoriques et des avis d'experts et autres personnes compétentes, et tenir compte des besoins des parties prenantes.

IIOT : Industrial Internet Of Things, en français « l'internet industriel des objets », correspond à l'application des technologies de l'internet et de l'internet des objets au domaine industriel qui permet d'interconnecter les systèmes informatiques, les capteurs et les équipements industriels intelligents.

Industrie du futur ou industrie 4.0[20]: s'appuie sur une combinaison de technologies de production de pointe également dites « avancées ». On peut notamment citer les robots collaboratifs, les robots mobiles, les drones, les exosquelettes, l'impression 3D (ou fabrication additive) ainsi que la réalité virtuelle. Ces technologies se caractérisent également par une plus grande intégration du numérique ce qui ouvre la voie à la création d'îlots de production interconnectés et pilotés en temps réel à distance. Si certaines de ces innovations sont déjà opérationnelles, d'autres sont encore en phase de test voire en cours de développement en laboratoire.

IT : (Information Technology), en français, les technologies de l'information (désignées par le sigle IT) sont le pendant des technologies d'exploitation (OT). Les systèmes OT sont essentiellement utilisés pour les interactions physiques, tandis que les systèmes IT s'utilisent dans le cadre de la résolution des problèmes métier. L'OT et l'IT se recoupent par bien des aspects, car les systèmes de technologies d'exploitation sont souvent connectés à des réseaux et ils gèrent et utilisent toujours plus de données.

Intégrité : propriété d'exactitude et de complétude d'une donnée.

M

Mesure de sécurité : mesure qui modifie un risque. Les mesures de sécurité comprennent tous les processus, politiques, dispositifs, pratiques ou autres actions qui modifient un risque. Il est possible que les mesures de sécurité ne puissent pas toujours aboutir à la modification voulue ou supposée.

O

OT : (pour Operational Technology), en français les technologies d'exploitation font référence à l'utilisation de matériel et de logiciels pour contrôler des équipements industriels. Souvent désignées par le sigle OT, elles concernent les systèmes spécialisés utilisés pour la fabrication, la distribution d'énergie, les services médicaux, la gestion des bâtiments et d'autres secteurs. Les systèmes OT sont essentiellement utilisés pour les interactions physiques. L'OT et l'IT se recoupent par bien des aspects, car les systèmes de technologies d'exploitation sont souvent connectés à des réseaux et ils gèrent et utilisent toujours plus de données. Les technologies d'exploitation sont le pendant des technologies de l'information (désignées par le sigle IT, pour Information Technology). Qui concernent les systèmes de données. Les systèmes OT sont essentiellement utilisés pour les interactions physiques, tandis que les systèmes IT s'utilisent dans le cadre de la résolution des problèmes métier. L'OT et l'IT se recoupent par bien des aspects, car les systèmes de technologies d'exploitation sont souvent connectés à des réseaux et ils gèrent et utilisent toujours plus de données.

P

PAM : (pour Privileged Access Management) en français, gestion des accès à privilèges, est l'un des processus et systèmes préventifs les plus efficaces dont disposent les organisations qui souhaitent réduire le risque que représentent pour elles leurs employés, partenaires, fournisseurs, systèmes et tiers.

Partie intéressée (terme préféré) ou partie prenante (terme admis) : personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité.

PCA : pour Plan de Continuité d'Activité, vise à garantir la haute disponibilité du système informatique de l'entreprise en cas de crise. Il s'agit de s'assurer que toutes les applications critiques nécessaires à l'activité de l'entreprise restent disponibles. La conception de l'architecture du système informatique de l'entreprise est au centre du PCA avec, notamment, la mise en place des équipements redondants (réseau, système de stockage de données, serveurs, datacenters), capables de prendre automatiquement le relai si l'un des éléments principaux venait à tomber en panne ou à être mis hors service.

PLC : Programmable Logic Controller, en français « automate programmable industriel » ou API est un dispositif qui sert à commander les processus industriels en s'appuyant sur des données d'entrées (des capteurs), des consignes et un programme informatique.

[20] Livre Industrie 4.0 Georg Edition Genève

PRA : pour Plan de Reprise d'Activité est un ensemble de procédures (techniques, organisationnelles, sécurité) qui permettent à une entreprise de prévoir par anticipation, les mécanismes pour reconstruire et remettre en route un système d'information en cas de sinistre important ou d'incident critique.

Propriétaire du risque : personne ou entité ayant la responsabilité du risque et ayant autorité pour le gérer.

R

Risque : effet de l'incertitude sur les objectifs. Un risque est souvent caractérisé en référence à des événements potentiels et des conséquences potentielles ou à une combinaison des deux. Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement et de sa vraisemblance. Les risques liés à la sécurité de l'information peuvent être exprimés comme l'effet de l'incertitude sur les objectifs de sécurité de l'information.

S

Sécurité de l'information : protection de la confidentialité, de l'intégrité et de la disponibilité de l'information. D'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité peuvent également être concernées.

Système d'information : ensemble d'applications, services, actifs informationnels ou autres composants permettant de gérer l'information intégrité propriété d'exactitude et de complétude partie intéressée (terme préféré) partie prenante (terme admis) personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité.

Système de management : ensemble d'éléments corrélés ou interactifs d'un organisme visant à établir des politiques, des objectifs et des processus permettant d'atteindre ces objectifs. Un système de management peut recouvrir une ou plusieurs disciplines. Les éléments du système comprennent la structure de l'organisme, les rôles et responsabilités, la planification et les opérations. Le domaine d'un système de management peut comprendre l'organisme dans son ensemble, certaines de ses fonctions spécifiques et identifiées, certaines de ses sections spécifiques et identifiées, ou une ou plusieurs fonctions au sein d'un groupe d'organismes.

Système d'information industriel ou ICS (Industrial Control System) : Un système d'information industriel ou un système de commande industriel (ICS) est un système composé d'un système d'information classique auquel s'ajoute des équipements spécifiques pour le contrôle et la mesure qui permettent d'interagir avec le monde physique. Cette définition inclut les SCADA (Supervisory control and data acquisition), les SIS (Safety Instrumented Systems) et les DCS (Distributed Control Systems).

T

Traitement du risque : processus destiné à modifier un risque. Le traitement du risque peut inclure :

- un refus du risque en décidant de ne pas démarrer ni poursuivre l'activité porteuse du risque
- la prise ou l'augmentation d'un risque afin de saisir une opportunité
- l'élimination de la source du risque
- une modification de la vraisemblance
- une modification des conséquences
- un partage du risque avec une ou plusieurs autres parties (incluant un contrat et un financement du risque)
- un maintien du risque fondé sur un chois argumenté

V

Vulnérabilité : faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces.

Guide sur la cybersécurité industrielle

Ce document a été réalisé à l'initiative de la communauté
cybersécurité du GET Numérique

Membres du groupe de travail
Jocelyn ZINDY (Eiffage Énergie Systèmes), pilote du projet
Christophe CORNE (Systancia)
David DUBUS (UnumKey)

Contributeurs aux travaux
Bernard DEBAUCHE (Systancia)
Hervé LINH (Eiffage Énergie Systèmes)

GRAND EST
TRANSFORMATION
ANTICIPER, ACCOMPAGNER, ACCÉLÉRER
NUMÉRIQUE

Communauté
Cybersécurité

www.grandest-transformation.fr

Une initiative de

La Région Grand Est

Coordonnée par

GRAND E·NOV+
L'AGENCE RÉGIONALE DES TRANSFORMATIONS

Financée par

Financé par l'Union européenne

Octobre 2024