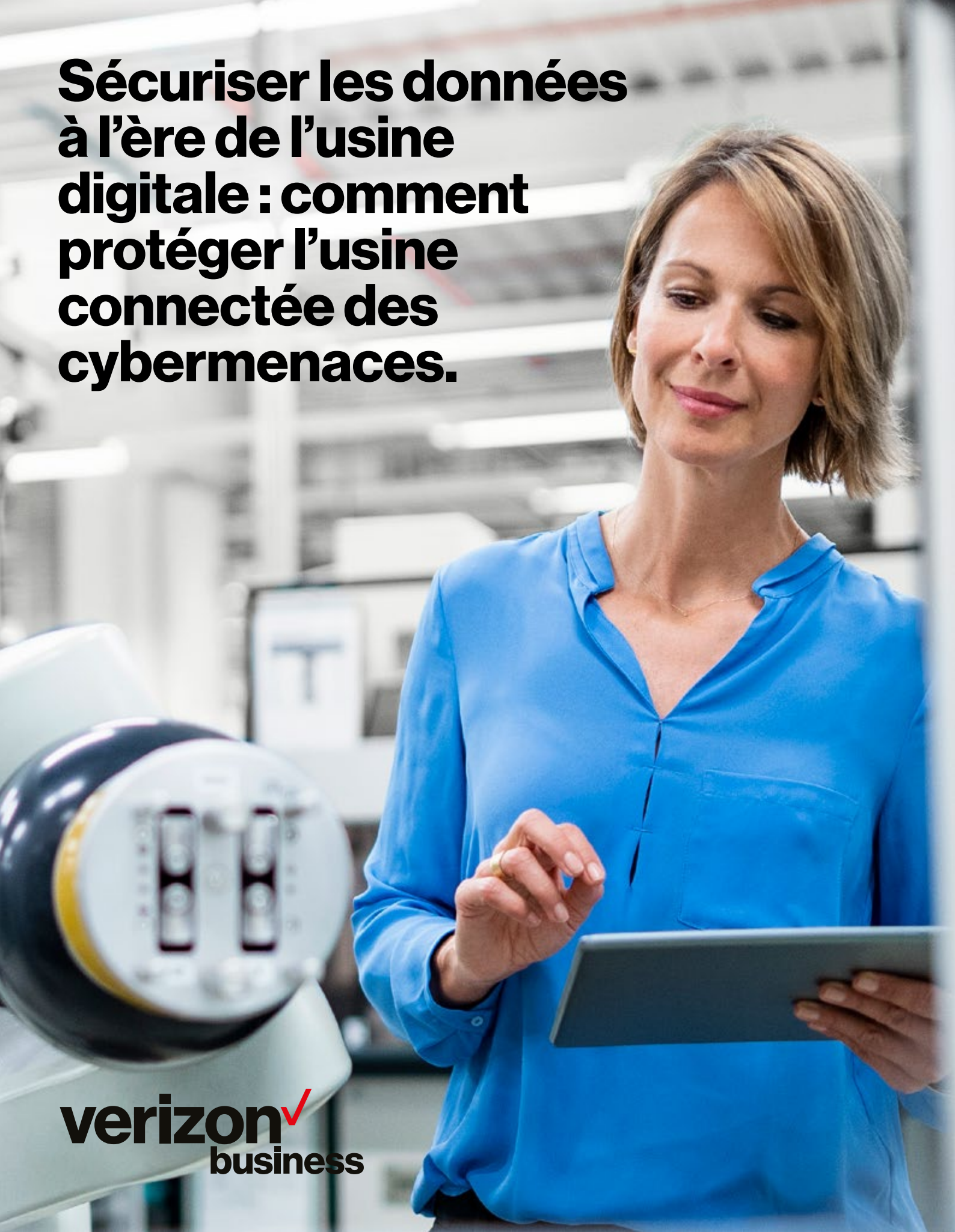
Sécuriser les données à l'ère de l'usine digitale : comment protéger l'usine connectée des cybermenaces.



verizon business

Avec la transition vers l'Industrie 4.0, les entreprises industrielles sont confrontées à de nouvelles cybermenaces pouvant compromettre leurs données sensibles et perturber leurs opérations. Face à ce risque, les usines connectées doivent se protéger pour préserver l'intégrité, la confidentialité et la disponibilité de leurs informations stratégiques.

Dans ce document, nous passerons en revue les stratégies et bonnes pratiques qui permettent d'assurer la sécurité des données dans les usines digitales.

Principales menaces impactant l'industrie :

Face à des attaques de plus en plus fréquentes et sophistiquées, les entreprises industrielles voient leurs données sensibles particulièrement exposées à des risques de compromission.

tels que :

- Attaques par ransomware : les cybergangs prennent vos données en otage jusqu'au paiement d'une rançon
- Phishing : les cybercriminels conçoivent des pages web ou e-mails frauduleux pour inciter leurs victimes à divulguer des données sensibles ou télécharger un malware
- Attaques par interception (« Man-in-the-middle ») : Les cybercriminels interceptent des conversations pour obtenir des informations confidentielles transmises à d'autres destinataires

Ces types d'attaques permettent à leurs auteurs de faire main basse sur de nombreuses informations confidentielles (données R&D, propriété intellectuelle, études de marché, données client sensibles, informations financières, etc.).

L'industrie, cœur de cible des cyberattaquants

C'est aujourd'hui le secteur le plus visé par les groupes cyber, devant les services financiers et les assurances.

La pandémie de Covid-19 a mis en lumière les risques que représentent à la fois les supply chains et le télétravail. Entre la pénurie de composants, la perturbation des systèmes just-in-time et l'utilisation d'appareils personnels à des fins professionnelles sur des réseaux non sécurisés, les risques se sont multipliés et ont contribué à complexifier la gestion des accès aux données de l'entreprise.

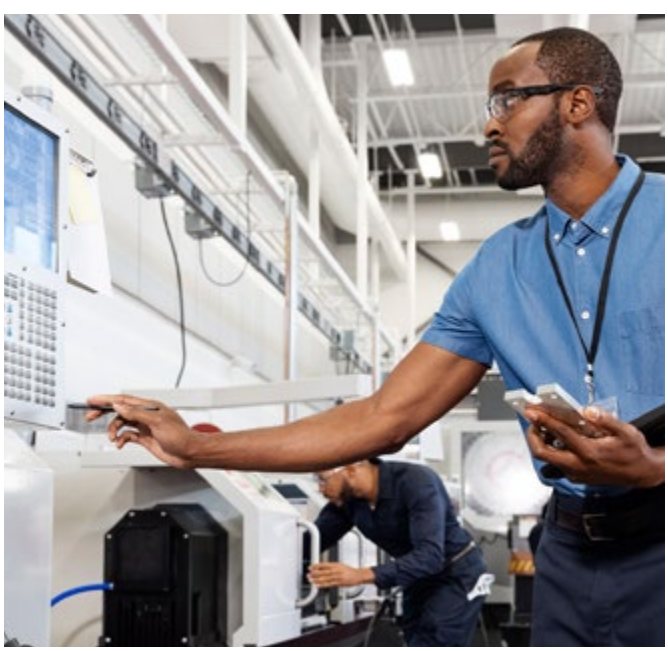
Dans un autre registre, des hackers ont pu accéder aux images vidéo des usines et entrepôts d'un grand constructeur automobile américain en ciblant un fournisseur de caméras de sécurité connectées au cloud.

Cybersécurité et Industrie 4.0 : pourquoi les usines intelligentes doivent renforcer leur protection.

La transition vers l'Industrie 4.0 et la mise en réseau des machines, produits, utilisateurs et entreprises partenaires apportent leur lot de nouveaux défis dans les usines.

Avec la sophistication croissante des technologies de production, on assiste à une intégration des capteurs d'équipements, systèmes CVC et autres technologies opérationnelles (OT) aux infrastructures IT internes et même à celles des fournisseurs. C'est ainsi que s'opère la fusion de mondes IT et OT autrefois séparés.

Généralement moins sécurisées que les ordinateurs portables, téléphones et tablettes, les OT restent pourtant les grandes oubliées des systèmes de monitoring de la sécurité. Et ce, bien qu'elles intègrent parfois des systèmes anciens, dépourvus de dispositifs modernes de détection et de réponse aux cybermenaces. Cette situation ne facilite pas les audits de sécurité de l'écosystème technologique global et des risques auxquels les entreprises sont confrontées.



Sans compter que les OT ne sont pas toujours soumises aux mêmes exigences de gouvernance des données que les technologies IT. Les décisions les concernant sont généralement prises dans l'environnement de production, sans concertation avec les équipes IT et de sécurité de l'entreprise.

Pour toutes ces raisons, et du fait de leur rôle clé dans la production, les OT représentent une cible de choix pour les groupes de hackers. Un chiffre en témoigne : les compromissions de technologies opérationnelles ont bondi de 50 % l'an passé.

Dans cet environnement en perpétuelle mutation, les opportunités ne manquent pas pour les attaquants. Les entreprises industrielles dotées d'infrastructures technologiques de pointe ont donc tout intérêt à mettre en place des standards de sécurité et des mesures de protection renforcées.

Usines intelligentes, protection rudimentaire

En 2021, le cabinet McKinsey a évalué le niveau de sécurité de plus de 100 entreprises et organismes opérant dans différents secteurs. Ses conclusions : en dépit de progrès significatifs réalisés dans les secteurs de la banque et de la santé, la majorité des entreprises, tous secteurs confondus, ont encore beaucoup de chemin à parcourir pour mettre leur capital informationnel à l'abri de menaces en perpétuelle mutation. Dans bien des cas, ce manque de protection semble résulter d'une incompréhension des risques associés aux systèmes en place, mais aussi d'un déficit d'investissement dans la sécurité IT/OT.

Les conséquences d'une protection insuffisante sont multiples :

- Impact financier
- Perte de propriété intellectuelle ou de données sensibles
- Baisse de la productivité
- Problèmes de supply chain
- Perte de confiance des clients et partenaires

Cybersécurité : mode d'emploi

La première mesure de protection consiste à former et à familiariser les collaborateurs à l'usage des logiciels de sécurité, à leur mise à jour régulière et à l'installation de tous les correctifs nécessaires.

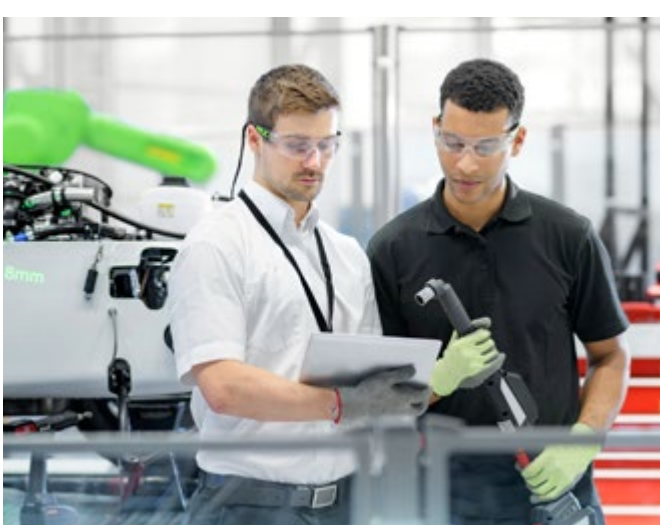
Sachant que les appareils IoT d'anciennes générations sont une cible privilégiée des attaquants, les entreprises industrielles doivent tenir compte des limites de ces appareils dans la mise à jour proactive de leurs firmwares. Comme ces équipements opèrent souvent à faible débit, elles veilleront donc à bien équilibrer leurs mises à jour pour éviter toute surcharge du système pouvant conduire à des perturbations des fonctions critiques. Ce qui compte ici, c'est de parvenir au meilleur compromis possible entre sécurité et performance.

Alors que 80 % des compromissions de données résultent de vols d'identifiants, les industriels devront limiter l'accès réseau aux seuls appareils IoT dotés d'identifiants.

De même, ils s'assureront de la bonne configuration de leurs datastores, sur site comme dans le cloud, en veillant à ne pas stocker toutes leurs données dans un seul lieu. L'utilisation de services cloud, d'une sécurité managée ainsi que d'autres ressources leur permettra de rester proactifs et vigilants face aux menaces émergentes.

Avant d'implémenter toute nouvelle technologie, les entreprises doivent évaluer son niveau de sécurité, son profil de risque et sa capacité de résistance à une cyberattaque. En ce sens, les tests d'intrusion reproduisant les modes opératoires de cyberattaques réelles pourront les aider à détecter les éventuelles failles dans leur réseau IoT.

Selon une étude récente du Manufacturing Leadership Council, 83 % des industriels placent la cybersécurité au cœur de leurs préoccupations. Et 79 % d'entre eux s'attendent à une hausse des attaques dans l'année à venir. Mais dans le même temps, seuls 40 % des sondés sont confiants dans leur niveau d'expertise interne en matière de cybersécurité.

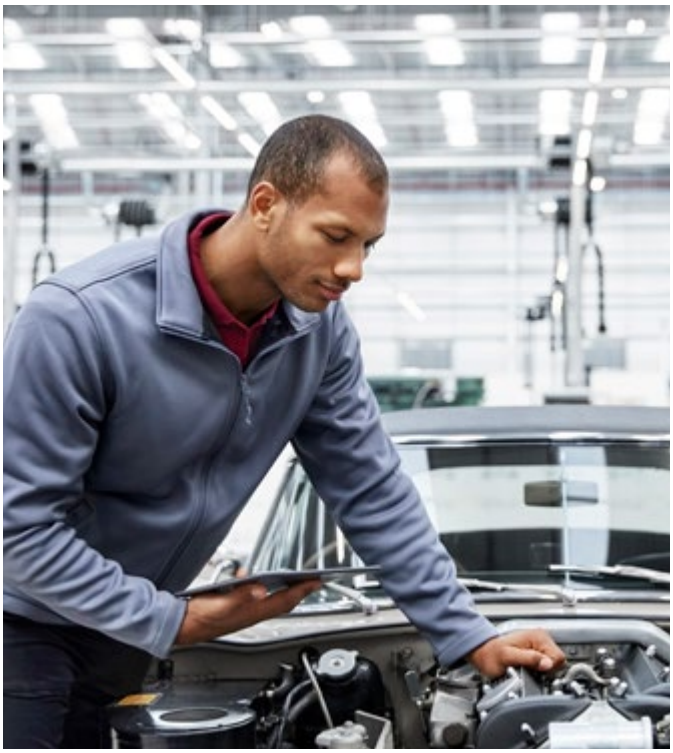


Un framework de cybersécurité au service d'une protection renforcée.

Elément essentiel mais souvent négligé, la mise en place d'un programme de gouvernance de la sécurité devrait inclure :

- Une cartographie des risques représentant le profil de risque de l'entreprise
- Un protocole d'escalade des risques comprenant des seuils de reporting
- Un plan de réponse et de confinement rapide, avec priorisation des actions en fonction des profils de risque
- Un inventaire actualisé de l'ensemble des ressources IT et OT, des données collectées et des points d'interconnexion IT/OT
- Une formation cyber de tous les collaborateurs, en mettant notamment l'accent sur les télétravailleurs et les employés ayant accès à des informations et assets stratégiques (données sensibles, systèmes de contrôle industriel et produits connectés)
- Une sauvegarde sécurisée des systèmes critiques, pour une restauration facile en cas de nécessité
- Une installation des correctifs et mises à jour de sécurité pour les systèmes de contrôle industriel (ICS) et fonctionnalités de sécurité
- Un chiffrement des données avec des clés cryptographiques stockées et sauvegardées de manière sécurisée

Les industriels doivent désigner des responsables capables à la fois de gérer efficacement les risques, de prendre les bonnes décisions d'investissement et de maîtriser les complexités des systèmes de contrôle industriel et produits connectés. Les RSSI ont un rôle crucial à jouer pour les accompagner dans cette démarche, notamment dans la recherche de partenaires externes disposant de toute l'expertise nécessaire pour les accompagner dans leur parcours et les aider à sécuriser leurs processus et données. Dans le même temps, les industriels doivent se montrer prêts à investir dans leur sécurité et à mesurer les résultats obtenus grâce à ces solutions.



Avec l'intégration croissante des systèmes OT et IT dans les environnements industriels, les entreprises de ce secteur doivent bénéficier d'une visibilité complète sur les menaces qui pèsent sur elles.

Avec Verizon, elles bénéficient de toutes les garanties pour mettre en place une stratégie forte de prévention, de détection et de réponse forte. 5G privée, Mobile Edge Computing (MEC), services cloud... Verizon propose également toute une gamme de technologies garantes d'une connectivité à faible latence et à très haut débit.

Dès lors qu'ils disposent d'un plan d'action adapté, de solutions de pointe et d'un partenaire comme Verizon, les acteurs industriels ont toutes les cartes en main pour négocier le virage de l'Enterprise Intelligence tout en protégeant leur capital le plus précieux : leurs données.

Découvrez comment Verizon peut vous aider à optimiser vos opérations de cybersécurité pour permettre à votre équipe de se concentrer sur son cœur de mission : impulser la croissance de votre entreprise.

verizon business