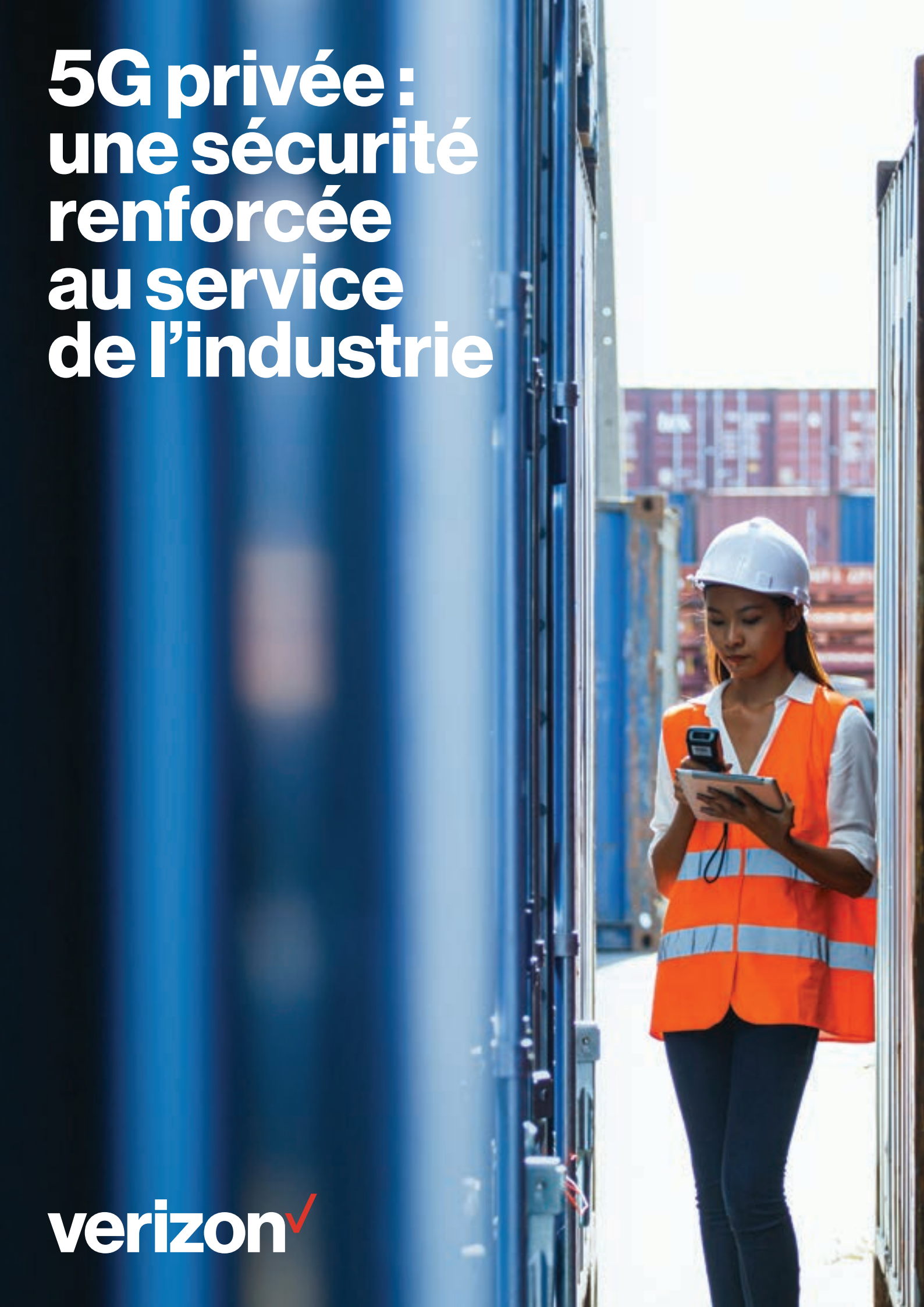
5G privée : une sécurité renforcée au service de l'industrie



verizon

Sommaire

Quel est l'objet de ce livre blanc ?

Aujourd'hui, la technologie 5G n'est plus une vision, mais bien une réalité pour des entreprises déjà nombreuses à exploiter les bénéfices de réseaux 5G privés. Ces dernières années, les champions de l'innovation, en particulier dans le secteur industriel, ont imaginé de nouveaux cas d'usage 5G dans une optique de transformation de leur modèle opérationnel. C'est ainsi que des applications dérivées de la 5G sont désormais à l'œuvre dans les usines, les laboratoires et sur le terrain : la « quatrième révolution industrielle » est en marche

Mais n'oublions pas que la sécurité reste un enjeu majeur pour toutes les entreprises.

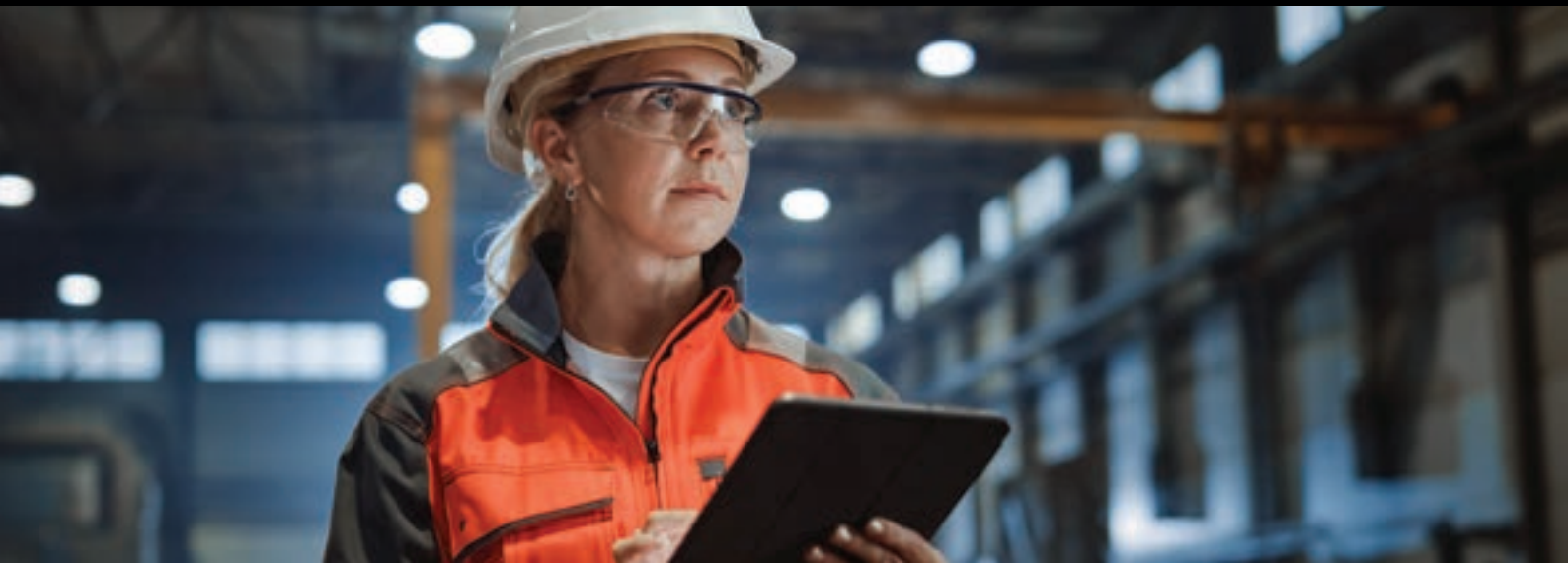
C'est pourquoi la 5G intègre en natif des contrôles de sécurité renforcés visant à mieux protéger les données et systèmes sensibles. Toutefois, la 5G n'est pas non plus la solution miracle aux carences ancrées au plus profond de votre programme de sécurité. En effet, les équipes qui, historiquement, ont eu du mal à suivre la cadence d'adoption de technologies disruptives – cloud, mobile et Internet industriel des objets (IIoT) – éprouveront à coup sûr des difficultés avec la 5G.

Cela étant dit, il existe une voie à suivre pour qui souhaite renforcer la sécurité de l'entreprise via la 5G.

Le NIST (National Institute of Standards and Technology du département du Commerce des États-Unis) offre en ce sens un cadre de cybersécurité (CSF) permettant d'améliorer les défenses de l'environnement IT tout en réduisant les risques inhérents à certains cas d'usage 5G. Ce programme fait office de référence internationale sur laquelle s'alignent d'autres standards tels que la norme ISO 27110.

Le présent document couvre trois grands axes :
- Les différences entre réseaux 5G publics et privés
- L'usage de la 5G privée dans un environnement industriel et les enjeux de cybersécurité connexes
- Les leviers proposés par le CSF du NIST afin de renforcer la sécurité des entreprises à l'heure de la 5G et de l'Industrie 4.0

Une étroite collaboration transfonctionnelle (sécurité, IT, réseau et pôles métiers) est essentielle pour parvenir à récolter les fruits de la technologie 5G, efficacement et en toute sécurité. Ce livre blanc propose donc un cadre de référence commun en vue d'atteindre cet objectif.



Solutions de connectivité avancée : l'embarras du choix.

Les cas d'usage fondés sur des fonctionnalités réseau avancées révolutionnent en profondeur l'activité des entreprises dans bon nombre de secteurs, à commencer par l'industrie, la distribution, l'exploitation minière et la production d'énergie.

La communication M2M (machine to machine) transforme peu à peu les procédures opérationnelles traditionnelles, tandis que l'IIoT génère des données en masse qui, lorsqu'elles sont analysées en quasi-temps réel, constituent un levier de compétitivité. Du TSN (Time-Sensitive Networking) sans fil aux véhicules à guidage automatique (VGA), en passant par les caméras connectées et les dispositifs de réalité virtuelle/augmentée, tous les cas d'usage émergents gourmands en bande passante s'appuient nécessairement sur un socle réseau solide.

Mais entre la 5G privée, la 5G publique, le Wi-Fi 5 ou encore le Wi-Fi 6, quelle est la technologie réseau la mieux adaptée à vos besoins métiers spécifiques ?

Et quels sont les différents enjeux de sécurité à prendre en compte selon le type de connectivité choisi ?

Quels sont les atouts de la 5G par rapport au Wi-Fi ?

Le choix de la 5G mobile pour les réseaux critiques offre un certain nombre d'avantages par rapport aux solutions de connectivité sans fil comme le Wi-Fi 6, notamment pour les grandes entreprises du secteur industriel. Ces deux technologies font actuellement l'objet d'avancées majeures afin de soutenir les nouveaux cas d'usage émergents et les tendances de l'Industrie 4.0.

Augmentation des débits, déploiement de services, réduction de la latence, traitement de volumes de données accrus, fiabilité… la 5G offre des performances spectaculaires. En digne successeur de la 4G, cette technologie mobile s'appuie sur les bonnes pratiques de sécurité développées pour les opérateurs par l'organisme de normalisation 3GPP (3rd Generation Partnership Project). Autrement dit, les réseaux 5G sont sécurisés dès la conception et intègrent entre autres certaines fonctionnalités telles que l'authentification et l'autorisation des équipements utilisateurs, le chiffrement de données de bout en bout, l'amélioration de la confidentialité ainsi qu'une architecture Zero Trust. Tous ces éléments contribuent à renforcer la sécurité et permettent à la 5G de protéger nativement les communications réseau.

Par ailleurs, il faut savoir que la 5G utilise des bandes de fréquences sous licence – ce qui permet de réduire les interférences issues d'autres appareils sans fil – et offre des capacités de découpage réseau pour améliorer la qualité de service (QoS). Grâce aux solutions cloud telles que la virtualisation, cette nouvelle technologie mobile offre en outre davantage de flexibilité pour le déploiement de services. La 5G est donc parfaitement adaptée à l'Edge Computing (informatique en périphérie), car elle apporte une solution rentable aux problèmes de latence. Ce type de connectivité assure enfin un accès ubiquitaire et une feuille de route flexible, sans oublier la compatibilité avec les technologies WAN et LAN.

Par contraste, l'infrastructure Wi-Fi 6 utilise exclusivement des bandes de fréquence sans licence, ce qui l'expose au risque d'interférences gênantes dans les environnements encombrés. Le Wi-Fi étant surtout utilisé à domicile ainsi que dans les réseaux LAN professionnels, son écosystème d'équipements privilégie avant tout ce type d'infrastructure. En tant que technologie mobile, la 5G convient quant à elle aussi bien à une utilisation fixe, itinérante, intérieure et extérieure.

Malgré tout, le Wi-Fi devrait continuer de jouer un rôle important au sein des environnements LAN publics et privés, notamment grâce aux améliorations du Wi-Fi 6 par rapport à la norme précédente. Les nouveaux réseaux sans fil proposent en effet de meilleurs débits, une plus faible latence ainsi que des améliorations en matière de densité et d'efficacité énergétique.

L'authentification et l'autorisation des équipements utilisateurs, le chiffrement des données de bout en bout, la confidentialité et l'architecture Zero Trust, entre autres, renforcent la sécurité et permettent à la 5G de protéger nativement les communications réseau.

Réseaux 5G : infrastructure publique ou privée ?

Les technologies réseaux mobiles se divisent en deux catégories : publique et privée. Les infrastructures privées répondent à des cas d'usage très spécifiques articulés autour d'une couverture locale, dont les exigences diffèrent de celles des services mobiles grand public. C'est notamment le cas de la gestion des chaînes de production ou des VGA.

Bien que ces deux options emploient les mêmes technologies, la 5G privée a la particularité de proposer un réseau qui vous est propre, ce qui vous permet de bénéficier d'une bande passante entièrement consacrée aux besoins de votre entreprise. Cette alternative offre donc un meilleur contrôle sur les données et le réseau, puisqu'elle exclut tout partage avec l'extérieur. Elle s'accorde parfaitement avec les déploiements d'appareils IoT, par exemple des capteurs ou des caméras, qui restent dans l'enceinte de l'entreprise et ne requièrent donc aucune fonction d'itinérance.

La 5G privée est aussi très avantageuse sur le plan de la sécurité. Même si les menaces restent identiques, le fait que le réseau soit utilisé exclusivement sur un site directement contrôlé et sécurisé par l'entreprise contribue à renforcer vos défenses. Par exemple, un individu souhaitant brouiller les signaux devrait se rendre sur site et passer outre les contrôles de sécurité sans jamais être détecté. Pour rappel, une protection multicouche combine à la fois des contrôles de sécurité physiques et logiques.

Principaux attributs des réseaux 5G

Public

- Expertise, solutions et largeur de fréquence propres aux opérateurs de réseau mobile
- Interopérabilité et provisionnement complets à partir d'un réseau public
- Qualité de service (QoS) accrue, avec accès prioritaire aux équipements et applications critiques
- Edge Computing au sein du réseau public, avec passerelles sur site en option pour une latence inférieure ainsi que le stockage et le traitement localisés des données

Privé

- Réseau dédié offrant une sécurité et une confidentialité renforcées
- Infrastructure isolée, sans contact avec les réseaux mobiles publics
- Maîtrise complète de la conception, du déploiement et de l'exploitation
- Contrôle total sur les accords de niveau de service (SLA)
- Edge Computing : latence inférieure, stockage et traitement localisés des données
- Externalisation partielle ou complète de la conception ou de la gestion du réseau
- Responsabilité directe de l'accès et de l'utilisation du spectre 5G

Informations tirées et adaptées de : https://www.gsma.com/iot/wp-content/uploads/2020/10/2020-10-GSMA-5G-IoT-Private-and-Dedicated-Networks-for-Industry-4.0.pdf

Sécurité industrielle : les avantages de la 5G privée.

Les environnements complexes et critiques, reposant sur les systèmes de contrôle industriels (ICS) et les technologies opérationnelles (OT), se prêtent davantage aux réseaux 5G privés. Des ateliers de production aux grands ports maritimes, certains types de connectivité sont très sensibles au risque d'interférences issues de structures physiques ou d'autres signaux sans fil. Grâce à ses débits constants et à sa faible latence, la 5G privée est particulièrement adaptée à ce type d'infrastructure où tout doit être fait pour éviter une interruption de service.

Tous les experts vous le diront : la disponibilité est l'une des pierres angulaires de la cybersécurité, à laquelle s'ajoutent l'intégrité des systèmes/données et la protection des informations confidentielles.

La 5G permet le déploiement massif d'appareils connectés (IoT), à condition de pouvoir s'appuyer sur un programme de sécurité évolutif, capable de protéger les équipements, gérer les vulnérabilités et garantir le transfert sécurisé des données vers les plateformes analytiques. Ces appareils doivent faire l'objet d'une surveillance continue et exigent des fonctions de sécurité capables de détecter et répondre immédiatement aux cyberattaques. Récemment, les médias se sont fait l'écho d'attaques DDoS de grande ampleur à partir d'équipements IoT détournés. Or, les attaques ciblant les applications 5G – y compris celles basées sur des malwares et des ransomwares – peuvent perturber les processus de production, nuire à la qualité du service client et freiner la création de valeur. Ces incidents peuvent également entraîner le non-respect de clauses contractuelles ou la non-conformité réglementaire, tout en écornant la réputation de l'entreprise. Une mauvaise sécurité des données en transit peut aussi aboutir au vol d'informations propriétaires ou de données personnelles de vos clients.

Enfin, n'oublions pas qu'une sécurité défaillante, tant au niveau de la conception que de l'exécution, peut mettre des vies en danger. Par exemple, voyageriez-vous à bord d'une voiture autonome susceptible d'être piratée à tout moment ?

Des centrales électriques aux usines de traitement de l'eau, le risque d'attaque contre les opérateurs d'importance vitale (OIV) est bien réel et peut avoir de lourdes répercussions. En 2014, une cyberattaque visant le réseau d'une aciérie allemande a provoqué un lourd préjudice[1]. Début 2021, des hackers ont même tenté d'empoisonner un réseau d'eau potable de Floride en infiltrant les systèmes de contrôle industriels d'une usine d'approvisionnement en eau[2].

Comment le CSF du NIST aide à sécuriser votre réseau 5G privé

Le CSF du NIST propose une approche éprouvée de la conception des programmes de cybersécurité qui, appliquée aux réseaux 5G privés et à leurs cas d'usage, permet de réduire significativement le risque. Ce framework souligne cinq fonctions essentielles pour les entreprises :

Identification
Familiarisez-vous avec les menaces internes et externes pesant sur vos ressources et sur votre entreprise.

Protection
Sécurisez l'infrastructure, les ressources et les données critiques, quel que soit leur emplacement (du cloud au mobile en passant l'IoT).

Détection
Améliorez et accélérez votre capacité à détecter la compromission des systèmes et des données.

Réponse
Élaborez et maintenez un plan de gestion des incidents de sécurité à la fois rapide et efficace.

Restauration
Planifiez votre résilience afin d'optimiser la disponibilité des systèmes et de réduire les coûts liés aux interruptions de service.

verizon

[1] https://www.bbc.com/news/technology-30575104 [2] https://www.bbc.com/news/world-us-canada-55989843

Le cadre de sécurité industriel comprend trois grandes composantes :

- Framework central
- Niveaux d'implémentation
- Profils

Le framework central se décline en trois parties :

- Fonctions
- Catégories
- Sous-catégories

Et comprend cinq fonctions générales :

- Identification
- Protection
- Détection
- Réponse
- Restauration

Ces dernières se divisent en 23 catégories réparties à travers les cinq fonctions :

Fonction	Catégorie
Identification	Gestion des ressources Environnement de l'entreprise Gouvernance Évaluation des risques Stratégie de gestion des risques Gestion de la supply chain
Protection	Gestion des identités et contrôle des accès Sensibilisation et formation Sécurité des données Protection de l'information, des processus et procédures Maintenance Technologies de protection
Détection	Anomalies et événements Surveillance continue de la sécurité Processus de détection
Réponse	Planification de la réponse à incident Communication Neutralisation Amélioration
Restauration	Planification de la restauration Amélioration Communication

Gros plan sur le CSF du NIST.

Identification

La conception d'un programme de sécurité passe nécessairement par l'identification des équipements connectés à votre réseau d'entreprise, ainsi que des données qu'ils contiennent. Autrement dit, vous ne pouvez pas protéger ce dont vous n'avez pas connaissance. Dans cette perspective, les entreprises doivent donc identifier quelles sont leurs ressources essentielles, c'est-à-dire celles dont la compromission ou l'indisponibilité aurait un impact opérationnel majeur.

En définitive, une entreprise doit toujours veiller à disposer d'une visibilité complète sur son environnement d'exploitation. Avant d'adopter une infrastructure 5G privée, vous devez parfaitement comprendre tout ce qu'implique une telle implémentation : outre le réseau, les équipements et les logiciels à installer, il faut aussi tenir compte des divers composants qui sous-tendent les différents cas d'usage et exploitent cette technologie.

Par ailleurs, il est essentiel de savoir où sont traitées puis stockées les données collectées pour un accès ultérieur. Vous devez également établir une hiérarchie entre les différents cas d'usage selon leur rôle dans la bonne marche de votre entreprise, tout en accordant la priorité aux technologies et aux données requises pour y parvenir.

Cette étape implique aussi l'identification et la maîtrise du profil de risque. En effet, les entreprises se composent aujourd'hui de multiples départements dont le mode d'opération diffère, tandis que certaines possèdent des filiales évoluant dans divers segments industriels. Or, tout ceci ajoute à la complexité de votre programme de sécurité : vous devrez donc collecter et contextualiser les données afin de déterminer les profils de risque de vos différents réseaux.

En ce qui concerne la 5G privée, nous avons déjà évoqué divers enjeux de sécurité essentiels dans le secteur industriel. Votre profil de risque doit également tenir compte des technologies propriétaires ainsi que des solutions IT et OT spécialisées sur lesquelles reposent vos opérations, sans oublier leur impact sur les capacités de restauration.

Jusqu'à présent, les industriels ont eu recours à des technologies propriétaires, mises en œuvre au sein d'un réseau privé et isolé pour ajouter une couche de sécurité. Mais aujourd'hui, les cas d'usage rendus possibles par la 5G privée requièrent souvent l'accès au cloud public.

Ces changements d'architecture réseau ont un impact sur votre profil de risque et doivent être pris en compte. Vous devrez d'autre part identifier et évaluer régulièrement les technologies, collaborateurs et processus de sécurité en place afin de détecter de potentielles lacunes. Ce travail est généralement réalisé par l'intermédiaire d'une évaluation réalisée chaque année par un prestataire externe. Tous ces différents enjeux sont sous-tendus par les objectifs de sécurité de votre entreprise, y compris le niveau d'atténuation des risques, de conformité et de confidentialité.

Protection

Les technologies de protection sont le socle de votre programme de sécurité. Or, celles-ci ont nettement évolué depuis que les entreprises ont abandonné l'approche périmétrique traditionnelle – à l'image d'un château entouré de ses douves – au profit d'infrastructures hybrides caractérisées par des composants virtuels, des fonctions réseau sur site et dans le cloud, des services SaaS et la généralisation du télétravail.

Vos stratégies de défense doivent donc refléter ce changement de paradigme. Or, puisque la sécurité intégrée des réseaux 5G privés offre déjà une protection intrinsèquement renforcée, notamment grâce au chiffrement et à l'application des principes Zero Trust, vous devez mettre l'accent sur la protection des différents composants de vos nouveaux cas d'usage.

Dans cette perspective, plusieurs solutions s'offrent à vous. Le découpage réseau, par exemple, ajoute une couche de protection en séparant les capacités selon les cas d'usage et les données associées, qui sont alors isolées du reste du réseau.

La protection des terminaux représente également un enjeu incontournable. Si certains équipements tels que les ordinateurs portables et les appareils mobiles sont compatibles avec les capteurs de sécurité, les appareils IoT requièrent quant à eux une technologie spécialisée, reflétant à la fois leur taille et leurs capacités.

Outre les terminaux, les cas d'usage 5G nécessitent une protection des applications et du traitement de données. Votre stratégie dépendra toutefois du type de technologie utilisé, du degré de protection intégré, de l'utilisation ou non du cloud public et des risques associés. Face à la sophistication et la diversification des menaces d'une part, et à la nécessité de protéger les ressources essentielles de l'entreprise d'autre part, le Zero Trust reste le socle idéal du pilier « Protection » décrit par le CSF du NIST.

Enfin, puisque les salariés sont en première ligne de votre programme de sécurité, n'oubliez pas que tout changement aux niveaux des cybermenaces, des technologies et des processus doit être pris en compte dans la formation et la sensibilisation de vos collaborateurs.

Détection

Pour les experts en cybersécurité, la question n'est pas de savoir si mais plutôt quand votre entreprise sera victime d'une attaque : d'où la nécessité de pouvoir compter sur une détection rapide. Comme le montre le rapport DBIR (Data Breach Investigations Report) de Verizon, près de 20 % des compromissions passent inaperçues pendant des mois, voire des années.

Étant donné l'ampleur des risques déjà évoqués, qui peuvent aller jusqu'à mettre des vies humaines en péril, la vitesse de détection est un facteur absolument crucial. Il s'agit donc d'un volet essentiel de votre programme de sécurité. Par conséquent, l'introduction des réseaux 5G privés et de leurs cas d'usage implique une modification des technologies de détection afin de refléter les changements apportés au réseau, aux applications ainsi qu'au stockage de données.

Les entreprises, notamment celles qui opèrent dans des environnements hautement industrialisés, devront veiller à ce que leurs technologies de détection soient capables d'ingérer et de traiter efficacement les données de journaux, souvent créées dans un format propriétaire. Aussi, elles pourront exploiter les technologies d'analyse réseau afin de surveiller la présence d'activités suspectes, y compris les preuves d'exfiltration de données.

Réponse

Ce pilier repose en partie sur les capacités de planification, rouage essentiel à l'efficacité de vos opérations de sécurité. Ceci implique l'organisation régulière d'exercices de mise en situation, ainsi que la démonstration des réponses à différentes menaces. Une évaluation indépendante des systèmes de sécurité est également vivement recommandée.

Sachant que les entreprises répondent différemment aux incidents de sécurité selon leur secteur d'activité, vos partenaires technologiques doivent avoir une bonne maîtrise de l'environnement industriel afin de soutenir votre planification spécifique.

Face à l'introduction de la 5G privée et de ses nouveaux cas d'usage, les entreprises doivent ajuster leurs programmes de protection, de détection mais aussi de planification de la réponse à incident, qui doit être régulièrement testée pour en vérifier l'efficacité.

En cas d'incident, vous devez pouvoir compter sur des renforts d'urgence. Or, la plupart des entreprises ne peuvent pas se permettre d'assigner des collaborateurs entièrement astreints à cette mission dans l'attente d'une éventuelle compromission. La solution consiste donc à attribuer des responsabilités secondaires à certains collaborateurs qui seront mobilisés en cas d'incident, ou bien de faire appel à un prestataire – voire un mélange des deux.

Restauration

Les industriels doivent aborder ce volet en étudiant à nouveau les besoins spécifiques de leur activité, ainsi que les équipements concernés afin de réduire l'impact sur l'entreprise.

L'adoption d'un réseau 5G privé implique également l'introduction de nouveaux fournisseurs technologiques, dont il faudra cerner le rôle dans le processus de restauration afin de bien les intégrer à votre planification.

Conclusion.

L'avènement de la 5G en général, et de la 5G privée en particulier, promet de faire émerger des réseaux de nouvelle génération qui transformeront le monde industriel. Les dirigeants doivent donc travailler main dans la main avec les responsables des départements IT et sécurité pour actionner pleinement les leviers de la quatrième révolution industrielle, tout en maîtrisant parfaitement les risques associés.

En exploitant les contrôles de sécurité natifs des réseaux 5G, ainsi que les recommandations du cadre de cybersécurité du NIST, votre entreprise a toutes les cartes en main pour impulser une innovation continue, en toute sécurité.

Rendez-vous sur verizon.com/business/fr-fr/solutions/5g/ pour savoir comment la 5G Verizon peut changer la donne pour votre entreprise.

verizon