Lignes directrices de STAR relatives à l'infrastructure des concessionnaires

2025

MEILLEURES PRATIQUES ET RECOMMANDATIONS DE L'INDUSTRIE POUR LES TECHNOLOGIES DE L'INFORMATION DANS LE SECTEUR DE LA VENTE AU DÉTAIL DE VÉHICULES AUTOMOBILES

Table des matières

1. Lignes directrices de STAR relatives à l'infrastructure des concessionnaires

1.1 Aperçu

Ce document détaillé – *Lignes directrices de STAR relatives à l'infrastructure des concessionnaires* – décrit les meilleures pratiques de l'industrie et doit être mis à la disposition des concessionnaires pour leur permettre de vérifier leurs besoins en matière de réseau et d'infrastructure. Les concessionnaires, qu'ils soient petits ou grands, doivent pouvoir compter sur des administrateurs de réseau internes, ou des responsables informatiques, chargés d'examiner ces lignes directrices, les listes de contrôle et les conseils, ainsi que le guide de référence rapide, afin de s'assurer que leur concession a mis en œuvre une solution sûre, sécurisée et robuste qui répond aux besoins des clients et des équipes de la concession.

1.2 Groupe de travail sur les lignes directrices relatives à l'infrastructure des concessionnaires

Les lignes directrices relatives à l'infrastructure des concessionnaires sont appuyées par l'un des nombreux groupes de travail de l'organisation STAR. Contrairement à de nombreux groupes de travail qui se concentrent sur les structures de données et les transports, les lignes directrices relatives à l'infrastructure des concessionnaires ont été établies pour aider les concessionnaires, les vendeurs et les fabricants d'équipement d'origine à disposer d'un guide commun pour l'infrastructure informatique nécessaire à la sécurité, à l'efficacité et à la robustesse des concessions automobiles.

1.3 Avantages des lignes directrices relatives à l'infrastructure des concessionnaires – Concessionnaire, fournisseur et fabricant d'équipement d'origine

Comme les autres détaillants, les concessions automobiles doivent disposer de la bonne technologie pour soutenir des processus solides visant à vendre des véhicules et à en assurer l'entretien. Depuis l'avènement d'Internet, de nombreux systèmes différents sont utilisés au sein d'une concession pour répondre aux demandes toujours croissantes des clients. Ces systèmes sont fournis et pris en charge par des fournisseurs de systèmes pour les concessionnaires et comprennent tout, du système principal de gestion des concessions aux nombreuses solutions de soutien, telles que le marketing de la relation client, la gestion des clients potentiels, l'exploitation de l'équité, la gestion de la réputation, les sites Web, le marketing numérique, la gestion des stocks en ligne, les outils d'aire de service, et bien d'autres encore. Avec le besoin sans cesse croissant de fournisseurs de systèmes pour les concessionnaires, il est également nécessaire que les données soient partagées de manière efficace et sécurisée entre ces systèmes et les fabricants d'équipement d'origine. Les présentes lignes directrices relatives à l'infrastructure des concessionnaires constituent un guide destiné à favoriser l'intégration efficace des données, la protection de celles-ci, la fiabilité des systèmes et l'efficacité des processus opérationnels.

1.4 Avis de non-responsabilité

Tout nom d'entreprise, application, lien de site Web ou référence technologique figurant dans le présent document ne doit pas être considéré comme une approbation par les fabricants d'équipement d'origine ou par STAR, à moins que cette approbation ne soit expressément mentionnée.

Le présent document fournit une spécification de base ou une ligne directrice pour les concessionnaires afin de leur permettre d'établir la communication par Internet. Il est important de noter que l'infrastructure du réseau, les données du concessionnaire et la sécurité du système relèvent de la responsabilité de la concession. Des organisations tierces, telles que des prestataires de services et des partenaires, peuvent fournir des conseils et des recommandations. Certaines organisations peuvent fournir des logiciels, du matériel ou des éléments de réseau propriétaires pour aider à simplifier les opérations du réseau. Toutefois, ces applications, recommandations ou outils ne remplacent pas la gestion du réseau.

2. Infrastructure du réseau des concessionnaires

2.1 Aperçu

L'infrastructure réseau d'une concession est constituée des ressources matérielles et logicielles utilisées pour permettre la connectivité, la communication, les opérations et la gestion du réseau local (LAN) du concessionnaire. L'infrastructure de réseau fournit le chemin de communication et les services entre les utilisateurs, les fournisseurs de services, le fabricant d'équipement d'origine et les clients finaux. Une sélection et une mise en œuvre appropriées de l'infrastructure réseau sont essentielles pour garantir l'efficacité du réseau et la compatibilité des applications et des données avec les fabricants d'équipement d'origine, les fournisseurs de systèmes pour les concessionnaires et les concessions.

2.2 Matériel

Le matériel de la concession est un dispositif physique qui sert à capturer les données du concessionnaire (ordinateurs de bureau, ordinateurs portables, appareils portatifs), à acheminer ces données (routeurs, commutateurs, pare-feu) et à les fournir sur demande (serveurs, moniteurs et périphériques).

Le choix du matériel de réseau est un élément essentiel de la gestion du réseau d'une concession. Le nouveau matériel peut représenter une dépense d'investissement très coûteuse, mais le matériel désuet peut, par exemple, entraver les activités de l'entreprise en raison de problèmes de vitesse ou de compatibilité.

La partie suivante explique à quel moment acheter du nouveau matériel et présente les lignes directrices et les recommandations pour l'achat d'ordinateurs de bureau, d'ordinateurs portables et d'équipements de réseau.

2.2.a À quel moment faut-il acheter du matériel neuf?

Du matériel informatique bien entretenu peut durer de trois à cinq ans, voire plus dans certains cas. Cependant, à un certain moment, un concessionnaire doit évaluer les options de mise à niveau ou de remplacement du matériel actuel.

STAR recommande aux concessionnaires d'envisager le remplacement du matériel dans les situations suivantes :

- Le matériel actuel ne répond pas aux exigences de base nécessaires à l'exploitation d'une technologie particulière.
- Le matériel actuel n'est pas conforme aux normes de base fixées par un fabricant d'équipement d'origine, un fournisseur de systèmes pour les concessionnaires ou d'autres partenaires technologiques de la concession.
- Le matériel actuel ne dispose pas des équipements, des accessoires ou du soutien dont les périphériques ont besoin pour exécuter une fonction précise.
- Les performances de l'appareil sont si lentes qu'elles affectent les activités de l'entreprise. *Remarque* : *la lenteur n'est pas nécessairement due à un problème de matériel. Elle peut être attribuable à la configuration, au stockage, à la sécurité ou à une erreur de la part d'un utilisateur.*
- Le matériel actuel n'est pas compatible avec les nouveaux logiciels (tels que les systèmes d'exploitation, les navigateurs ou les applications des concessionnaires).
- Le nouveau matériel pourrait permettre de réaliser des économies intéressantes grâce aux gains de temps, aux fonctionnalités supplémentaires ou à une facilité d'utilisation.
- Les coûts de mise à niveau sont égaux ou proches du coût de remplacement, ou le produit arrive en fin de vie utile ou n'est plus pris en charge.
- Le fabricant ne prend plus en charge le matériel. En d'autres termes, les correctifs, les mises à jour de sécurité et les avancées en matière de logiciels ne sont pas effectués sur les appareils. Lorsque le matériel n'est plus pris en charge, la concession est exposée à des risques de sécurité et de fiabilité.

2.2.b Quoi acheter : matériel destiné aux consommateurs par rapport au matériel de qualité professionnelle

La plupart des fabricants d'ordinateurs proposent deux catégories différentes d'ordinateurs : le matériel destiné au grand public et conçu pour un usage personnel et résidentiel, et le matériel de qualité professionnelle pour les entreprises. Si le prix du matériel grand public peut sembler attractif pour les concessionnaires, le coût total de possession s'avère souvent plus élevé en raison des fonctionnalités limitées, des taux de défaillance plus élevés et du soutien nécessaire plus complexe.

STAR recommande aux concessions d'acheter du matériel de qualité professionnelle pour les raisons suivantes :

- Les systèmes destinés aux consommateurs sont généralement fabriqués avec des pièces plus génériques ou des pièces moins coûteuses fournies en grandes quantités. De plus, les fabricants sont connus pour changer de pièces, de fournisseurs et de composants sans modifier les modèles. En raison de ces facteurs, ces pièces peuvent présenter un taux de défaillance plus élevé. Il en résulte des temps d'arrêt plus importants, des délais d'assistance plus longs et un taux de remplacement des systèmes plus lent.
- Les systèmes de qualité professionnelle sont généralement fabriqués à partir de pièces de marque qui sont normalisées, ce qui facilite la normalisation du réseau et son soutien pour de nombreuses entreprises.
- Les ordinateurs personnels de type grand public sont souvent équipés de systèmes d'exploitation destinés à un usage résidentiel. Il peut en résulter des problèmes de mise en réseau pour les entreprises, comme la connexion à des serveurs ou à d'autres postes de travail.
- Le matériel réseau utilisé par les consommateurs n'est souvent prévu que pour un petit nombre de connexions. Le matériel utilisé par les entreprises est conçu pour prendre en charge le grand nombre de connexions dont les réseaux de concessions ont besoin.
- Le matériel grand public peut être assorti de garanties limitées. Certaines garanties offertes aux consommateurs ne s'étendent pas aux entreprises.
- Les économies initiales peuvent être compensées par des coûts de remplacement et de soutien technique plus élevés, ainsi que par des délais d'exécution plus longs pour obtenir un remplacement.

2.2.c Recommandations matérielles

Matériel de point d'extrémité (ordinateurs de bureau, ordinateurs portables et tablettes)

Les recommandations de STAR pour les ordinateurs de bureau, les ordinateurs portables et les tablettes des concessionnaires ne sont plus axées sur des exigences matérielles globales. Cette évolution s'explique principalement par les progrès de la puissance de traitement du matériel, le passage à l'informatique en nuage et l'omniprésence de la mobilité. STAR recommande que les besoins matériels soient déterminés sur la base d'un scénario d'utilisation fondé sur les tâches à accomplir.
Lors de l'achat de nouveaux appareils, il faut tenir compte des facteurs suivants :

1. **Mobilité :** certaines fonctions au sein d'une concession requièrent de la mobilité. D'autres fonctions sont exercées principalement dans un seul lieu. Tenez compte des besoins en matière de mobilité lors de l'achat d'un nouvel appareil. Gardez également à l'esprit que de nombreux appareils mobiles, tels que les tablettes, fonctionnent avec des logiciels particuliers qui peuvent ne pas être compatibles avec l'ensemble du matériel et des logiciels requis. Il faut tenir compte des exigences matérielles et logicielles avant de décider si une tablette, un ordinateur portable ou un ordinateur de bureau est le meilleur choix pour une fonction donnée.

2. **Exigences logicielles :** les fonctions exercées au sein de la concession nécessitent une interaction avec différents logiciels. Les logiciels sont souvent conçus pour des systèmes d'exploitation et des navigateurs Internet précis. Les applications logicielles peuvent également exiger une configuration matérielle de base. Lors de l'achat d'un nouvel appareil, il faut comprendre le logiciel qu'il utilisera et les exigences requises pour le faire fonctionner.
3. **Exigences relatives aux accessoires matériels :** les concessionnaires ont souvent besoin d'accessoires particuliers pour remplir une fonction. Des outils d'aide à la vente, des diagnostics de service et d'autres adaptateurs physiques sont nécessaires pour des cas d'utilisation précis. Ces accessoires sont souvent conçus en fonction de spécifications logicielles et matérielles particulières. Si la fonction d'antivol nécessite un accessoire particulier, il faut vérifier les exigences auprès du fournisseur avant d'acheter un nouvel équipement.
4. **Exigences des fabricants d'équipement d'origine, des fournisseurs de systèmes pour les concessionnaires et des tiers :** les fabricants d'équipement d'origine, les fournisseurs de services aux concessionnaires et d'autres fournisseurs tiers déploient souvent des technologies propres aux concessions. Ces technologies (matériel ou logiciel) peuvent nécessiter des caractéristiques précises pour fonctionner de manière efficace. Si un appareil de concession utilise des technologies particulières, il faut vérifier auprès du fournisseur de ces technologies.
5. **Fiabilité :** la fiabilité des appareils doit être prise en compte lors de l'achat de matériel. Certaines activités de la concession, telles que l'environnement de service, sont plus sujettes aux défaillances des appareils. Certaines fonctions sont plus sensibles aux temps d'arrêt des appareils. Pour déterminer quoi acheter et à quel moment, il faut tenir compte de la probabilité d'une défaillance de l'appareil et des conséquences qu'une telle défaillance peut avoir sur la fonction concernée et sur les activités de la concession.

Au-delà des recommandations relatives aux cas d'utilisation, STAR peut fournir des conseils sur le choix du matériel à acheter et sur le moment de l'achat. STAR fournit des conseils sur le moment où il convient d'acheter du nouveau matériel à la section 2.2.a du document *Lignes directrices de STAR sur l'infrastructure des concessionnaires*. Pour déterminer ce qu'il convient d'acheter, STAR fournit des conseils sur les achats de matériel destiné aux consommateurs ou aux entreprises à la section 2.2.b. et propose un guide pour les tablettes et les appareils mobiles à la section 2.2.d.

Pour plus de renseignements sur les recommandations relatives au matériel des concessionnaires, y compris les tablettes, la mobilité, la mise hors service et le recyclage du matériel, veuillez consulter la section 2.2.e.

Matériel réseau (routeurs et commutateurs)

Routeurs et commutateurs	
Composant	**Caractéristiques**
Caractéristique de la norme Ethernet	IEEE 802.3 100BASE-T ou 1000BASE-T
Redondance	La connexion entre plusieurs commutateurs doit utiliser des liens redondants de la plus grande vitesse disponible, en utilisant la norme Spanning Tree Protocol (STP) ou la norme Rapid Spanning Tree Protocol (rSTP) pour garantir une topologie sans boucle.
Alimentation électrique	Des sources d'alimentation redondantes sont recommandées pour réduire les temps d'arrêt.
Vitesse	100 ou 1000 Mb/s
Réseau local virtuel (VLAN)	Les commutateurs dotés de la technologie VLAN et 802.1Q (trunk) doivent être utilisés pour les réseaux routés avec plusieurs sous-réseaux ou VLAN.

Protocoles de gestion	Les appareils gérés doivent prendre en charge les normes de l'industrie en matière de gestion à distance, comme le protocole de gestion simple du réseau (SNMP) et la surveillance du réseau distant (technologie RMON).
Commutateurs sans fil	Les appareils sans fil doivent être compatibles avec la norme IEEE 802.11ac/ax.

2.2.d Tablettes et appareils mobiles

Les tablettes sont des appareils portatifs conçus pour la mobilité et l'accessibilité. Les tablettes n'ont souvent pas les mêmes fonctionnalités qu'un ordinateur portable ou de bureau. C'est pourquoi il est fortement recommandé aux concessionnaires de ne pas remplacer les ordinateurs de bureau ou les ordinateurs portables par des tablettes, mais plutôt d'utiliser des tablettes lorsque l'application et la fonction nécessitent une mobilité et une accessibilité accrues.

Certaines applications sont développées spécifiquement pour fonctionner sur des tablettes, telles que les iPad. Lorsque ces applications sont déployées, le fabricant d'équipement d'origine ou le fournisseur de système pour les concessionnaires précise les dispositifs avec lesquels ces applications sont destinées à être utilisées. En fonction de l'évolution de la technologie dans l'espace mobile, la compatibilité de certains programmes peut être limitée à des tablettes particulières ou à des versions précises du système d'exploitation de l'appareil mobile.

2.2.e Mise hors service et recyclage du matériel

Il incombe au propriétaire initial de l'appareil de veiller à ce que tous les appareils électroniques usagés soient éliminés de manière appropriée. Il existe des milliers de recycleurs de matériel électronique aux États-Unis, mais il est important de choisir la bonne entreprise offrant ce type de service. Voici quelques conseils pour bien choisir son recycleur.

Renseignez-vous sur les politiques et les pratiques du recycleur en matière de destruction des données personnelles contenues dans les équipements usagés.

- Les données peuvent être effacées des supports de stockage à l'aide d'une méthode d'effacement magnétique ou d'un programme permettant d'écraser tous les secteurs d'un disque dur. Toute méthode utilisée pour effacer les données doit être appliquée plusieurs fois (multipasse).
- Les supports de stockage peuvent être détruits par déchiquetage, découpage, incinération, perforations multiples ou broyage.
- Le recycleur doit être en mesure de certifier par écrit que les données ont été effacées, ou que les supports de stockage ont été détruits, et de fournir un relevé des méthodes utilisées.

Renseignez-vous sur les certifications de l'entreprise de recyclage.

- Le recycleur doit être certifié. Si l'on vous répond que l'entreprise n'est pas certifiée, qu'il s'agit d'un « secret commercial » ou que la méthode utilisée est « confidentielle », évitez de faire appel à elle.
- Les principales certifications de l'industrie sont les suivantes :
    - E-Stewards – www.e-stewards.org (en anglais)
    - Basel Action Network – www.ban.org (en anglais)
    - R2 – www.sustainableectronics.org (en anglais)
- Les recycleurs et les groupeurs doivent être en mesure de prouver qu'ils disposent des installations, de la formation et de l'équipement adéquats pour effectuer les opérations déclarées en présentant un système de gestion et d'exploitation vérifié, ainsi que des preuves d'audits récents.
- Demandez si l'entreprise de recyclage dispose d'une certification ou d'un système de gestion de l'environnement, soit une certification de gestion de l'environnement ISO 14001, soit des certifications d'organisations telles que l'International Association of Electronics Recyclers (IAER) ou l'Institute of Scrap Recycling Industries (ISRI).
- Pour les entreprises qui ne sont pas certifiées, la prudence est de mise. La concession, en tant que propriétaire initial de l'appareil, a la responsabilité d'assurer un recyclage adéquat.

Vérifiez si le recycleur a commis des infractions en matière d'environnement ou de sécurité (citations, amendes, avis de

violation, ordonnances sur consentement, etc.) ou s'il a déposé une demande d'indemnisation au titre de l'assurance contre les dommages environnementaux au cours des cinq dernières années.

- Il est préférable de favoriser les entreprises qui ont une bonne réputation en matière de respect des exigences environnementales et de sécurité.
- Une entreprise qui est en activité depuis plusieurs années et qui n'a commis que quelques infractions mineures qui ont été rapidement résolues peut être tout aussi fiable qu'une entreprise qui n'est en activité que depuis un an ou deux et qui n'a commis aucune infraction.
- Vérifiez l'existence d'infractions majeures, telles que des rejets de déchets en grandes quantités ou des plaintes importantes de la part des résidents avoisinants.

Vérifiez si le recycleur envoie des équipements usagés ou des déchets à d'autres partenaires d'affaires ou fournisseurs de services; ces derniers sont appelés « partenaires en aval ».

- La bonne tenue des registres est une pratique de gestion exemplaire dans l'industrie. Recherchez des entreprises qui tiennent des registres détaillés, notamment sur les lieux d'expédition des matériaux, les quantités expédiées et les numéros de série des articles à réutiliser.
- Bien qu'il existe plusieurs entreprises de recyclage « à service complet » aux États-Unis, il est probable que l'entreprise de recyclage ne se chargera pas de l'ensemble du traitement de l'appareil.
- L'entreprise de recyclage doit disposer de registres écrits indiquant les opérations de traitement effectuées sur le site (telles que le tri ou le broyage) et les destinataires des matériaux ou des produits après le traitement initial.
- Demandez si les partenaires d'affaires du recycleur (partenaires en aval) sont contractuellement liés aux mêmes normes ou aux mêmes meilleures pratiques de gestion que le recycleur choisi. Une liste complète de tous les partenaires en aval doit être mise à disposition du recycleur choisi.
- Méfiez-vous des recycleurs qui déclarent que leurs processus et leurs partenaires d'affaires sont « confidentiels », « exclusifs » ou qu'ils n'ont pas d'information à ce sujet.
- Toute exportation doit être effectuée conformément aux lois applicables des pays exportateurs et importateurs.

Un recycleur doit détenir une assurance responsabilité civile générale et une assurance responsabilité environnementale.

- Les exigences en matière d'assurance varient d'un État à l'autre. Le montant et le type de couverture nécessaires varient en fonction de la taille de l'établissement et de ses activités.
- Le montant et la couverture dépendent de la portée et de l'ampleur des activités.

2.3 Logiciel

Le logiciel est l'information d'exploitation ou le programme utilisés par le matériel de la concession pour capturer, stocker, manipuler et afficher des données liées au matériel du réseau. Les concessions utilisent des logiciels pour saisir les données relatives aux clients, automatiser les processus de vente et d'entretien des véhicules, et communiquer avec d'autres systèmes ou réseaux.

Pour les concessions, ces programmes ou processus résident souvent dans le système d'exploitation ou le navigateur Internet d'un ordinateur. Les logiciels sont souvent conçus pour des systèmes d'exploitation ou des navigateurs Internet précis. Les logiciels étant essentiels aux communications et aux processus d'entreprise des concessionnaires, il est important que ces derniers utilisent des systèmes d'exploitation et des navigateurs compatibles avec les logiciels de concession.

La section suivante décrit en détail les systèmes d'exploitation et les navigateurs courants. L'objectif de cette section est de fournir des conseils pour comprendre les systèmes d'exploitation et les applications de navigateurs afin de mieux les choisir. Il est fortement recommandé au concessionnaire de vérifier la compatibilité du logiciel avec les applications de la concession auprès du fabricant de l'équipement d'origine et des fournisseurs de services de la concession.

2.3.a Systèmes d'exploitation

Vous trouverez ci-dessous une liste des systèmes d'exploitation les plus courants sur le marché. Certaines applications ne sont pas compatibles avec des systèmes d'exploitation particuliers. Il est recommandé aux concessionnaires de vérifier auprès de leurs fabricants d'équipement d'origine, de leurs fournisseurs de systèmes pour les concessionnaires et auprès d'autres fournisseurs, quel système d'exploitation utiliser. Veuillez noter que Microsoft a mis fin au soutien des systèmes d'exploitation XP, Vista et Windows 7, y compris les mises à jour de sécurité critiques. STAR recommande aux concessions de ne pas utiliser Windows XP, Vista ou Windows 7.

Systèmes d'exploitation clients courants	Dernière mise à jour ou ensemble de modifications provisoires* (Service Pack)	Fin du soutien général	Fin du soutien prolongé
Windows XP	Service pack 3	14 avril 2009	8 avril 2014
Windows Vista	Service pack 2	10 avril 2012	11 avril 2017
Windows 7	Service pack 1	13 janvier 2015	14 janvier 2020
Windows 8	Windows 8.1	9 janvier 2018	10 janvier 2023
Windows 10	22H2	13 octobre 2020	14 octobre 2025
Windows 11	24H2		
MAC OS X	15.1.1	Les versions 14 et inférieures ne sont plus prises en charge	Les versions 14 et inférieures ne sont plus prises en charge
iOS (pour iPad et iPhone)	18.2		
Android	15		

**** Dernières mises à jour/Service Pack en date de janvier 2025***

2.3.b Navigateurs Internet

Vous trouverez ci-dessous une liste des navigateurs Internet les plus courants sur le marché actuellement. Certaines applications ne sont pas compatibles avec des navigateurs spécifiques. D'autres applications nécessitent des paramètres de navigateur précis, tels que le mode de compatibilité. Il est recommandé aux concessionnaires de consulter leurs fabricants d'équipement d'origine, leurs fournisseurs de systèmes pour les concessionnaires et d'autres fournisseurs pour déterminer quel navigateur utiliser.

Navigateur	Dernière mise à jour ou Service Pack*	Remarques
Apple Safari	17	Non recommandé pour les systèmes d'exploitation Microsoft
Google Chrome	131	
Internet Explorer	11	Internet Explorer a été retiré en juin 2022 Microsoft Edge est le navigateur recommandé par Microsoft
Microsoft Edge	1131	
Mozilla Firefox	133	

**** Dernières mises à jour/Service pack en date de janvier 2024***

2.3.c Licences de logiciels

La plupart des concessions négligent la question de la conformité des licences de logiciels. Cependant, cette négligence peut coûter des milliers de dollars à une concession. Voici les erreurs les plus courantes en matière de licences de logiciels pour une concession.

- Partage d'une licence commune plutôt que d'avoir une licence par appareil.
- Partage des identifiants pour les logiciels infonuagiques.
- Installation de copies de logiciels sous licence légale, mais non utilisées.
- Achat de versions de logiciels « pour la maison » plutôt que pour l'entreprise ou le commerce.
- Utilisation de logiciels piratés, téléchargés gratuitement.

Pour résoudre ce problème, les entreprises doivent créer un programme de gestion des biens logiciels. La gestion des biens logiciels consiste à gérer et à optimiser l'achat, le déploiement, la maintenance et le cycle de vie des biens logiciels au sein d'une organisation. Les deux principaux avantages d'un programme de gestion des biens logiciels sont le contrôle des coûts et la réduction des risques.

2.4 Réseau local (LAN)

Un réseau local (LAN) est constitué d'un groupe d'ordinateurs et d'appareils connexes reliés entre eux par des communications communes partagées, telles qu'une ligne câblée ou une liaison sans fil. Les concessions doivent gérer un réseau afin que leurs appareils puissent communiquer et partager des ressources de manière efficace et sécurisée.

La gestion du réseau peut représenter une tâche difficile pour les concessionnaires automobiles. Les concessionnaires doivent rendre le réseau accessible au partage des données et en limiter l'accès à des fins de sécurité. Outre le personnel de la concession, il arrive souvent qu'un fournisseur de services, un fabricant d'équipement d'origine et même des clients aient besoin de partager les ressources du réseau. Fournir un accès sûr et sécurisé au réseau de la concession peut s'avérer difficile.

La section qui suit présente des recommandations pour la configuration et la gestion du réseau local. Il fournit également des conseils sur le réseautage sans fil, la mobilité des concessions et l'accès des clients.

Recommandation	Caractéristiques
Pare-feu	Dispositif de sécurité entièrement géré qui surveille en permanence les menaces par le biais d'un système de détection d'intrusion (SDI) et d'un système de prévention d'intrusion (IPS), et d'autres mécanismes, tels que le filtrage des paquets, l'antivirus et l'inspection dynamique des paquets. - Les pare-feu doivent prendre en charge la traduction d'adresses de réseau (NAT) et la technologie d'analyse de procédé (TAP). Les pare-feu doivent également prendre en charge le routage dynamique à l'aide de RIPv2, OSPF et BGP. - Modifiez le mot de passe de l'appareil au moment de l'installation et de façon régulière. - Conservez une configuration de sauvegarde dans vos dossiers en cas de défaillance du logiciel ou de remplacement du matériel. - Une redondance matérielle supplémentaire peut être obtenue grâce à un pare-feu secondaire à haute disponibilité. - Pour en savoir plus sur les pare-feu et la sécurité du réseau, consultez la section 2.6.
Services de noms de domaine (DNS)	Utilisez le service DNS public, sauf lorsque vous utilisez Windows Active Directory (dans ce cas, il est nécessaire de disposer d'un serveur DNS interne).

2.4.a Configuration et gestion du réseau

Recommandation	Caractéristiques
Réseau local	Gigabit Ethernet
Câblage de données	Le câblage du réseau de données existant doit être de catégorie 5e, au minimum, et être conforme à la norme TIA-568-A. La catégorie 6a doit être utilisée pour le câblage neuf. Les câbles horizontaux ne doivent pas dépasser 90 mètres (295 pieds). Il est fortement recommandé de remplacer les câbles de données par des câbles en fibre optique lorsque la longueur dépasse 295 pieds.
Emplacement de l'équipement	L'équipement utilisé pour le réseau local (commutateurs) doit être installé dans une armoire de câblage ou dans une salle de communication. Tous les équipements doivent être montés ou fixés sur un support ou une étagère. Certains modèles de commutateurs peuvent accueillir une alimentation électrique supplémentaire pour renforcer la tolérance aux pannes.
Adressage IP	Le fournisseur de services Internet de la concession doit fournir un adressage IP pouvant être acheminé (« routable »). Pour le réseau local du concessionnaire, il vaut mieux utiliser l'adressage dynamique (DHCP) pour faciliter le soutien.
Adaptateur de réseau	Gigabit Ethernet
Commutation Ethernet	Commutateur gigabit géré. Étiquetez chaque interface et chaque câble. Vous gagnerez ainsi du temps lorsque vous devrez retrouver des câbles de réseau dans le cadre d'une demande d'assistance ou d'une nouvelle installation.
Routeurs	Routeur professionnel. Les routeurs doivent prendre en charge la traduction d'adresses de réseau (NAT) et la technologie d'analyse de procédé (TAP). Les routeurs doivent également prendre en charge le routage dynamique à l'aide de RIPv2, OSPF et BGP. - Modifiez le mot de passe de l'appareil au moment de l'installation et de façon régulière. - Conservez une configuration de sauvegarde dans vos dossiers en cas de défaillance du logiciel ou de remplacement du matériel. - La mise en œuvre d'un service de réseau étendu défini par logiciel (SD-WAN) est une solution de choix qui offre un basculement, des fonctions optimisées du trafic et des configurations stockées dans le nuage tout en connectant la concession à Internet, aux centres de traitement des données et à d'autres sites de concessionnaires.

2.4.b Infrastructure des concessionnaires et continuité des activités

L'infrastructure des concessionnaires joue un rôle essentiel dans la reprise après sinistre et la capacité de revenir à un fonctionnement normal du réseau.

Les zones critiques du réseau d'une concession doivent être à haute disponibilité, disposer d'une infrastructure redondante ou de solutions de sauvegarde critiques. STAR recommande les considérations suivantes en matière d'infrastructure :

Infrastructure du concessionnaire	Recommandation	Référence
Transport de données/bande passante	Plusieurs technologies et fournisseurs d'accès assurent une connectivité Internet fiable	Section 2.5.c
Réseau étendu	Des technologies comme le service de réseau étendu défini par logiciel (SD-WAN) constituent une solution de choix qui offre un basculement, des fonctions optimisées du trafic et des configurations stockées dans le nuage tout en connectant la concession à Internet, aux centres de traitement des données et à d'autres sites de concessionnaires.	Section 2.4.a
Réseau local	Le matériel à haute disponibilité, les alimentations redondantes et les sauvegardes de configuration garantissent qu'une panne d'équipement n'aura pas d'incidence sur les activités de l'entreprise.	Section 2.4.a
Sauvegarde des données	Les données des serveurs, des points d'extrémité et des équipements de réseau doivent être sauvegardées dans d'autres emplacements.	Sections 2.2.c et 2.4.a

2.4.c Réseau sans fil

Les réseaux locaux sans fil permettent la communication en réseau sans les contraintes physiques du câblage. La technologie sans fil peut s'avérer particulièrement pratique, car elle offre une certaine mobilité au personnel. Elle permet également aux clients d'apporter et d'utiliser leurs propres appareils, et étend le réseau du concessionnaire au-delà des murs physiques de la concession. Les concessionnaires doivent également comprendre que l'omniprésence des réseaux sans fil s'accompagne de défis en matière de conception, d'assistance et de sécurité.

Consultez les lignes directrices suivantes lors de la conception, de la prise en charge et de la sécurisation d'un réseau sans fil de concession.

Conception de réseau sans fil	
Recommandation	**Caractéristiques**
Matériel sans fil	Seuls des points d'accès de qualité professionnelle doivent être utilisés. Les points d'accès de qualité professionnelle sont conçus pour offrir des fonctions d'itinérance et d'autres fonctions professionnelles (telles que les VLAN ou les identifiants SSID multiples) nécessaires à la prise en charge des dispositifs sans fil pour les applications. Les points d'accès sans fil de qualité professionnelle sont également conçus pour accueillir un plus grand nombre de connexions que le matériel de qualité grand public.
Segmentation du réseau	Les concessions doivent s'assurer que le trafic des invités est séparé du réseau de la concession par des VLAN ou une connexion Internet distincte.
Identifiants SSID	Il est recommandé aux concessions d'utiliser des identifiants SSID distincts pour les différentes fonctions de l'entreprise (c.-à-d. ventes, service après-vente et administration). Toutefois, les concessions ne doivent pas confondre les identifiants SSID avec la segmentation du réseau. En général, les identifiants SSID ne séparent pas le trafic du réseau, mais fournissent seulement un moyen différent de se connecter au réseau.
Couverture	Déployez des points d'accès sans fil pour assurer une couverture adéquate. Les outils sans fil peuvent fournir la puissance du signal autour du bâtiment. Faites attention aux structures ou aux objets qui peuvent interférer avec la couverture sans fil (interférences électriques, interférences de fréquence radio ou matériaux physiques, tels que les métaux ou le béton).
Authentification et chiffrement	Liaison WPA2 (Wi-Fi Protected Access II) avec authentification RADIUS et chiffrement AES. Remarque : consultez les recommandations du fabricant d'équipement d'origine pour obtenir des conseils sur la compatibilité avec les technologies propres au fabricant d'équipement d'origine.
Norme de réseau	802.11ax ou 802.11ac
Détection sans fil indésirable	Analysez, identifiez et supprimez tous les points d'accès sans fil indésirables qui pourraient se trouver sur le réseau de la concession. - Un point d'accès sans fil indésirable est défini comme un point d'entrée sans fil dans le réseau de la concession qui n'a pas été autorisé ou sécurisé par le concessionnaire, la direction des TI et le propriétaire. - Tous les réseaux sans fil indésirables doivent être détectés, repérés et supprimés sans délai. - STAR recommande l'utilisation d'un service de détection sans fil géré qui analyse en permanence le réseau pour détecter les menaces liées au réseau sans fil.

Mobilité de la concession	
Recommandations	**Caractéristiques**
Mobilité au sein de la concession	Utilisez un réseau maillé sans fil pour que les utilisateurs finaux puissent se déplacer sur le site sans perdre la connexion et sans avoir à s'authentifier à nouveau.
Contrôleurs sans fil	Un contrôleur de réseau local sans fil peut être utilisé en combinaison avec le protocole LWAPP (Lightweight Access Point Protocol) pour gérer des points d'accès allégés sur le réseau de la concession. La couverture, la fiabilité et l'efficacité du réseau s'en trouveront renforcées.

Accès des clients	
Recommandations	**Caractéristiques**
Priorisation du trafic	Les concessions doivent utiliser un pare-feu ou un autre mécanisme pour limiter la consommation de bande passante des invités. Ainsi, l'accès des visiteurs n'interfère pas avec les activités de l'entreprise en consommant trop de bande passante.
Authentification des invités et conditions d'utilisation	STAR recommande aux concessions d'utiliser un portail captif exigeant des invités qu'ils acceptent les conditions d'utilisation de la concession. Il peut s'agir de restrictions de contenu, de limitations de la bande passante et d'accords d'utilisation.
Bande passante Internet	Pour s'assurer que la concession dispose d'une largeur de bande passante suffisante, le concessionnaire doit choisir la bonne technologie et la bonne vitesse. (Pour en savoir plus sur les technologies et la bande passante Internet, consultez les sections 2.5.a et 2.5.b des *Lignes directrices de STAR relatives à l'infrastructure des concessionnaires*) - STAR recommande également à chaque concession de disposer d'une connexion Internet de secours provenant d'un autre fournisseur et qui utilise une technologie différente. - Voir la section 2.5.c pour des recommandations sur les connexions de sauvegarde Internet.

2.5 Bande passante Internet

La bande passante Internet correspond à la quantité de données pouvant être envoyées vers la concession et en provenance de celle-ci, généralement mesurée en bits par seconde. La plupart des logiciels de concession utilisent l'Internet pour la communication des données. Les informations sur les stocks, les bons de travail, les manuels d'entretien et les données sur les véhicules sont souvent accessibles sur Internet. De plus, la majorité du personnel et des clients utilisent l'accès Internet de la concession pour des raisons personnelles, par exemple pour consulter leurs courriels ou naviguer sur le Web. Étant donné que de nombreux utilisateurs dépendent de l'Internet pour obtenir des informations, il est essentiel que la concession se procure une bande passante suffisamment grande pour fournir à chaque ressource la capacité d'accéder rapidement aux données. Pour s'assurer que la concession dispose d'une largeur de bande passante suffisante, le concessionnaire doit choisir la bonne technologie et la bonne vitesse.

La section suivante détaille les technologies disponibles pour l'accès à Internet et explique comment prévoir une bande passante adéquate pour chaque ressource du réseau local (LAN).

2.5.a Technologies Internet

Technologie	Description	Vitesse	Support physique	Commentaires
Câble	Un modem câble particulier et une ligne de câble sont nécessaires.	Les vitesses peuvent varier, mais elles se situent généralement entre 10 Mb/s et 100 Mb/s.	Câble coaxial	Le service Internet par câble utilise une infrastructure partagée et peut se dégrader en cas d'utilisation intensive. Les concessions doivent s'informer sur les fournisseurs de câbles qui offrent déjà un service dans la région. Le coût de la mise en place du service dans une zone et de l'installation du câble dans une tranchée peut être prohibitif. Ford recommande aux concessions d'acheter un câble de qualité professionnelle et de demander au fournisseur une entente de niveau de service (ENS) ou un objectif de niveau de service (ONS) écrit.

Ligne d'abonné numérique (DSL)	Cette technologie utilise la partie numérique inutilisée d'une ligne téléphonique ordinaire en cuivre pour transmettre et recevoir des informations. La liaison numérique asymétrique (ADSL) signifie que la vitesse de téléversement du service est plus lente que la vitesse de téléchargement. La ligne numérique à paire symétrique (SDSL) offre les mêmes vitesses de téléversement et de téléchargement. La ligne d'abonné numérique à très haut débit (VDSL) est une autre technologie asymétrique qui peut offrir des vitesses allant jusqu'à 52 Mb/s.	De 128 kbit/s à 52 Mb/s	Paire torsadée (utilisée comme support numérique à large bande)	Ford recommande aux concessionnaires d'acheter des lignes DSL de qualité professionnelle offrant une vitesse de téléversement et de téléchargement suffisante pour exécuter les applications des concessionnaires Ford. La VDSL constitue le seul service DSL recommandé, car elle est peut-être la seule à disposer d'une bande passante suffisamment large pour répondre aux exigences recommandées en la matière.
T1	Lignes et équipements particuliers (unité de service de données [DSU] et unité de service de canal [CSU]) nécessaires.	1,544 Mb/s	Paire torsadée, câble coaxial ou fibre optique.	Plusieurs lignes T1 peuvent être reliées entre elles pour atteindre des vitesses plus élevées.

Technologie	Description	Vitesse	Support physique	Commentaires
Satellite		6 Mb/s ou plus	Ondes Possibilité d'utiliser un accès par ligne commutée pour le trafic en amont.	La bande passante n'est pas partagée. De plus, le temps d'attente est généralement élevé. Ce temps d'attente élevé interfère souvent avec les applications des concessionnaires. La technologie satellite n'est pas recommandée pour les concessionnaires.
Fibre	Les types de connectivité Internet du service de fibre optique fonctionnent sur un réseau optique.	Jusqu'à 300 Mb/s	Réseau optique	La fibre offre des vitesses élevées, des coûts réduits et de bonnes ententes de niveaux de service. Toutefois, l'accessibilité est limitée dans certaines régions du pays.

2.5.b Planification de la bande passante

Commencez par comprendre le service Internet actuel de la concession.

De nombreuses concessions ne connaissent pas leur technologie, leur vitesse et leur utilisation actuelles de l'Internet. La compréhension de la technologie peut aider à cerner les limites potentielles et les économies de coûts. Utilisez le tableau ci-dessus pour mieux comprendre les différentes technologies offertes sur le marché. Renseignez-vous sur les vitesses de

téléchargement et de téléversement de la bande passante du service actuel (habituellement en mégaoctet par seconde ou en kilobit par seconde) en consultant le fournisseur de services Internet de la concession. Enfin, connectez-vous au dispositif de passerelle de la concession, demandez au fournisseur d'accès Internet du concessionnaire ou trouvez des tests en ligne pour comprendre l'utilisation actuelle de la bande passante.

Prévoyez les pointes d'utilisation

L'utilisation de la bande passante n'est pas toujours constante. Les concessionnaires peuvent constater des pointes d'utilisation en fonction des processus d'entreprise (périodes d'activité élevée), des processus technologiques (exécution de sauvegardes ou téléchargement de mises à jour) et de l'utilisation par les clients (diffusion vidéo en continu depuis la salle d'attente). Il est recommandé aux concessions d'utiliser en moyenne 60 % de leur capacité pour tenir compte des pointes potentielles.

Planifiez les progrès technologiques

La plupart des fabricants d'équipement d'origine, des fournisseurs de systèmes pour les concessionnaires et des vendeurs de concessions développent des solutions qui exploitent davantage les communications Internet. Les concessions doivent comprendre que leurs besoins en matière de bande passante ne sont pas statiques, mais qu'ils continueront d'augmenter à mesure que la concession, les vendeurs et les partenaires mettront en œuvre de nouvelles technologies.

Planifiez la croissance

L'Institute of Electrical and Electronics Engineers (IEEE) affirme que les réseaux devront être en mesure de supporter un taux de croissance annuel composé de 58 % de la bande passante. Cette croissance est due à l'augmentation simultanée du nombre d'utilisateurs, des méthodes d'accès, des taux d'accès et des services, tels que la vidéo sur demande et les médias sociaux.

Faites preuve de vigilance

L'utilisation de la bande passante n'étant pas statique, la planification doit être une activité permanente. En obtenant une visibilité sur les schémas d'utilisation de la concession, un administrateur TI peut mieux anticiper une limitation potentielle de la bande passante avant qu'elle n'ait une incidence sur le rendement des activités de la concession. Il est recommandé aux concessions de mettre en place des alertes pour les pointes d'utilisation, la consommation moyenne ou les périodes de non-disponibilité de la bande passante. Ainsi, les risques seront atténués, les temps d'arrêt limités et la concession pourra procéder à une mise à niveau avant que l'activité n'en soit affectée de manière significative.

2.5.c Connexion de secours

La disponibilité du service Internet est essentielle pour les activités des concessions. Étant donné que les concessionnaires dépendent d'Internet pour la vente et l'entretien des véhicules, il est recommandé de disposer d'une connexion de secours.

Suivez les recommandations suivantes lors du choix d'une connexion de secours :

- Utilisez un fournisseur d'accès différent et une autre technologie Internet pour la connexion de secours.
- Il faut au minimum disposer d'un service de secours ou un basculement à large bande 5G. Testez le signal sans fil à l'avance pour vous assurer qu'il est suffisamment puissant. Les fournisseurs d'accès Internet, l'emplacement physique et la conception du bâtiment sont des variables qui influent sur la puissance du signal dans une concession donnée.
- STAR recommande un circuit dédié pour assurer une disponibilité élevée.
- STAR recommande aux concessions d'utiliser une passerelle qui prend en charge le basculement automatique pour réduire au minimum les temps d'arrêt.
- Le service de secours n'a pas besoin de disposer de la même vitesse que la connexion principale, mais il doit disposer d'une largeur de bande suffisante pour soutenir les fonctions essentielles de la concession.

2.6 Sécurité

L'objectif de l'infrastructure réseau d'une concession est de partager des données et des ressources avec le personnel, les clients et les fournisseurs ou partenaires tiers. Les concessions doivent également prendre des mesures pour s'assurer que ces données sont partagées en toute sécurité. Les concessions doivent surveiller les connexions connues et inconnues pour détecter les signes possibles d'une perte de données. Une concession doit prendre des mesures pour protéger les données de la passerelle et de chaque point d'extrémité du réseau. Des technologies, des procédures et des processus doivent être utilisés pour s'assurer que les données des concessionnaires ne tombent pas entre de mauvaises mains.

La section qui suit examine la protection du réseau du point de vue de la passerelle, des postes de travail, de la gestion de l'information sur la sécurité et de la sécurité des données, ainsi que du point de vue du client, du gouvernement, du risque et de la conformité. Des renseignements sur les procédures et les processus de sécurité sont également présentés à la section 6 intitulée « Pratiques en matière de formation, de processus et de documentation ».

2.6.a Politiques de sécurité

Le cadre des politiques de sécurité de la concession doit être complet, cohérent et approuvé par l'organe de gestion du concessionnaire. Il est important de s'assurer que toutes les parties prenantes adhèrent aux politiques et acceptent de les mettre en œuvre dans tous les aspects pertinents de la concession.

Les politiques doivent refléter la stratégie de sécurisation de l'information, et non l'inverse. La compréhension des exigences en matière de sécurité constitue le facteur clé à cet égard. L'accent doit être mis sur la confidentialité, l'intégrité et la disponibilité des données sensibles et des ressources, y compris l'environnement physique, l'infrastructure du réseau, les applications et les données (physiques et numériques). Cette liste n'est toutefois pas exhaustive, car il existe de nombreux autres éléments à prendre en considération. Par exemple, la non-répudiation, la traçabilité ou l'authenticité doivent souvent être prises en compte.

Par ailleurs, chaque secteur d'activité a ses propres zones sensibles. Par exemple, nous nous soucions beaucoup plus de l'intégrité – plutôt que de la confidentialité – d'un avion en vol ou d'une voiture sur l'autoroute que de la confidentialité des antécédents médicaux d'un patient (qui peut également dépendre du contexte). Les politiques de sécurité doivent tenir compte de ces considérations.

Il existe de nombreuses politiques ou directives-cadres prêtes à l'emploi en matière de sécurité, qu'il est possible de choisir et d'appliquer dans une entreprise. Cependant, même si ce type de cadre peut fournir une base générale, une entreprise doit adapter et développer ses politiques pour les appliquer dans le contexte de ses activités.

2.6.b Gestion des identités et des accès

La gestion des identités et des accès (IAM) est un cadre essentiel pour s'assurer que les bonnes personnes ont un accès approprié aux informations et aux ressources technologiques. La gestion de l'identité consiste à créer, à maintenir et à gérer les identités des utilisateurs et les autorisations d'accès qui leur sont associées. L'authentification est le processus qui consiste à vérifier qu'un utilisateur est bien celui qu'il prétend être, généralement au moyen de mots de passe, de données biométriques ou d'une authentification multifactorielle (AMF). L'autorisation, quant à elle, détermine ce qu'un utilisateur authentifié est autorisé à faire, en veillant à ce qu'il n'ait accès qu'aux ressources nécessaires à son rôle. Les meilleures pratiques en matière de gestion des accès incluent l'adoption d'une approche à vérification systématique, l'application du principe du droit d'accès minimal et l'audit régulier des contrôles d'accès. Ces pratiques sont essentielles pour protéger les données sensibles, empêcher les accès non autorisés et garantir le respect des normes réglementaires.

- Vérification systématique :
    - Vérification explicite : chaque demande d'accès fait l'objet d'une vérification approfondie. Il s'agit notamment de vérifier l'identité de l'utilisateur, l'état de santé de l'appareil et le contexte de la demande (p. ex. le lieu, l'heure) avant d'accorder l'accès.
    - Droit d'accès minimal : les utilisateurs se voient accorder le niveau d'accès minimal nécessaire à l'accomplissement de leurs tâches. Les risques d'accès non autorisé à des renseignements sensibles sont ainsi réduits.
    - Intrusion présumée : le cadre part du principe qu'une intrusion s'est déjà produite ou pourrait se produire à tout moment. Cet état d'esprit conduit à une surveillance et à une validation continues de toutes les demandes d'accès.
    - Authentification robuste : l'authentification multifactorielle (AMF) est souvent utilisée pour s'assurer que les utilisateurs sont bien ceux qu'ils prétendent être. Cette méthode ajoute une couche supplémentaire de sécurité au-delà du simple nom d'utilisateur et du mot de passe.
    - Surveillance continue : les activités des utilisateurs font l'objet d'une surveillance continue afin de détecter tout signe de comportement suspect. Cette mesure permet de détecter les menaces et d'y répondre en temps réel.
- Gestion de l'identité :
    - Création d'identifiants uniques : chaque membre de l'organisation dispose d'un identifiant unique pour accéder au système et se voit attribuer l'accès aux applications et aux fonctions nécessaires à l'accomplissement de ses tâches.
    - Maintien à jour des listes d'utilisateurs précises : les administrateurs de réseau tiennent à jour les listes d'utilisateurs finaux et suppriment activement les utilisateurs à la cessation d'emploi.
    - Méthodes d'authentification robustes : les utilisateurs doivent être authentifiés en utilisant des mots de passe uniques pour chaque application et chaque système auquel ils ont accès. Les mots de passe ne doivent pas être reproduits ou répétés pour accéder à différentes applications ou fonctions, ou à différents systèmes. L'autorisation multifactorielle (AMF), la biométrie ou la segmentation en unités, ou toute combinaison de ces éléments doivent être mises en œuvre pour valider l'identité des utilisateurs lors d'une demande d'accès.
    - Gestion active des utilisateurs tiers : soumettez les utilisateurs tiers aux mêmes critères que les utilisateurs internes et disposez d'un processus dynamique de suppression des utilisateurs tiers en fonction de l'évolution de leurs besoins d'accès aux systèmes et aux applications.
    - Codifiez par écrit les politiques et procédures de gestion de l'identité.
- Gestion des accès :

- Définissez une politique claire en matière de gestion des accès : établissez et documentez des politiques qui décrivent comment l'accès est accordé, examiné et révoqué. Ces politiques doivent inclure des lignes directrices concernant les rôles, les autorisations et les responsabilités des utilisateurs1.
- Contrôle d'accès basé sur les rôles (RBAC) : attribuez des droits d'accès en fonction des rôles des utilisateurs au sein de l'organisation. Les utilisateurs n'ont ainsi accès qu'aux informations nécessaires à l'exercice de leurs fonctions.
- Méthodes d'authentification robustes : mettez en œuvre l'authentification multifactorielle (AMF) pour ajouter une couche de sécurité supplémentaire. Cette méthode permet de vérifier l'identité des utilisateurs de manière plus robuste qu'en utilisant uniquement des mots de passe.
- Examens réguliers des accès : procédez à des examens périodiques des droits d'accès des utilisateurs pour vous assurer qu'ils sont toujours appropriés. Il est ainsi possible d'identifier et de supprimer les autorisations inutiles ou obsolètes.
- Processus de gestion des départs sécurisés : veillez à ce que les droits d'accès soient rapidement révoqués lorsqu'une personne quitte l'organisation ou change de rôle. Cette démarche permet d'éviter tout accès non autorisé de la part d'anciens membres du personnel.
- Surveillance et audit continus : Surveillez continuellement les activités des utilisateurs et les habitudes d'accès. Utilisez des outils d'audit pour suivre et enregistrer les activités en matière d'accès pour aider à détecter les activités suspectes et à répondre à ces activités.
- Fédération d'identités et authentification unique : mettez en œuvre la fédération d'identités et l'authentification unique pour simplifier la gestion des accès à travers plusieurs systèmes et applications. La gestion de plusieurs données d'identification devient ainsi moins complexe.
- Renforcement de l'environnement : renforcez la sécurité de l'environnement dans lequel fonctionnent les systèmes de gestion des accès. Il s'agit notamment de sécuriser les serveurs, les réseaux et les points d'extrémité. Il s'agit également d'interdire l'accès aux espaces où sont conservés les données et les systèmes aux personnes qui n'ont pas un besoin valable d'accéder à l'espace physique. Ne conservez aucune données dans des espaces dont l'accès n'est pas contrôlé.

L'intégration de pratiques robustes de gestion des identités et des accès (IAM) est essentielle pour franchir les trois niveaux de maturité de la sécurité de l'information. Au niveau **initial (ad hoc)**, les organisations sont souvent confrontées à des processus de gestion des identités et à des accès incohérents et réactifs, ce qui les rend vulnérables aux menaces de sécurité. Au fur et à mesure que la gestion des identités et des accès progresse vers le niveau **géré (défini)**, elle devient plus structurée et proactive, et s'accompagne de politiques et de procédures clairement définies qui renforcent la capacité de l'organisation à gérer et à atténuer les risques. Enfin, au niveau **optimal (avancé)**, la gestion des identités et des accès est intégrée de manière transparente dans les opérations de l'organisation, ce qui favorise une culture de sécurité mature qui évolue en permanence pour faire face aux menaces émergentes. En harmonisant les pratiques de gestion des identités et des accès à ces niveaux de maturité, les organisations peuvent renforcer de manière considérable leur posture de sécurité globale et leur résilience.

2.6.c Gestion des correctifs

Les systèmes d'exploitation des serveurs et des ordinateurs locaux nécessitent de temps à autre des mises à jour, pour la plupart liées à des risques de sécurité. Les correctifs fournis par le fabricant offrent souvent une protection contre des exploits nouveaux ou inconnus jusqu'alors. Il est essentiel que ces correctifs soient gérés, mis en œuvre et vérifiés pour assurer la fiabilité et la sécurité des applications. De plus, les concessions doivent porter une attention particulière aux éléments suivants :

- Systèmes en fin de vie
  - Se tenir au courant des systèmes d'exploitation en fin de vie permet de s'assurer que l'emplacement n'utilise pas de systèmes d'exploitation qui ne reçoivent plus de mises à jour de sécurité ou d'autres types de mises à jour parce que le fournisseur a cessé d'en assurer le soutien.
  - En général, les fournisseurs annoncent la date de fin de vie de leurs produits, qui peut toujours être vérifiée sur leurs sites Web respectifs.
- Appareils mobiles
  - Les appareils mobiles quittent souvent la protection du réseau de la concession et se connectent à d'autres réseaux qui sont, la plupart du temps, moins sécurisés. Pour cette raison, ces appareils peuvent être considérés comme plus vulnérables. Il est important que les correctifs soient rapidement apportés aux appareils mobiles afin de limiter les risques et l'exposition aux menaces et aux vulnérabilités.

2.6.d Formation sur la sensibilisation à la sécurité

La grande majorité des incidents de sécurité, y compris les violations de données, sont le résultat d'une erreur humaine, comme le fait de cliquer sur un courriel d'hameçonnage, par exemple. Tous les membres du personnel doivent être formés sur la manière de protéger l'entreprise contre le vol, les violations de données et tout autre problème de sécurité, au même titre que les techniciens sont formés aux dernières évolutions des véhicules et les vendeurs aux nouvelles caractéristiques des véhicules et aux nouvelles techniques de vente.

L'objectif du programme de formation n'est pas seulement de former les membres du personnel, mais aussi d'influencer leur comportement. Le personnel doit servir de pare-feu humain à l'entreprise.

La sécurité ne doit pas être perçue comme un sujet ennuyeux; si les gens n'y prêtent pas attention, le message ne passera pas. Il ne faut donc pas hésiter à faire preuve de créativité dans le cadre du programme de formation et de sensibilisation. L'humour, les exemples de la vie réelle, les concours et les jeux sont autant de moyens de maintenir l'intérêt et d'obtenir l'implication du personnel.

Pour maintenir l'implication des employés, envisagez d'utiliser plus fréquemment des modules de formation à la sécurité en ligne plus courts plutôt que des séances de formation uniques et longues. Cette approche permet de maintenir la formation à jour sur les derniers développements en matière de logiciels malveillants et d'attaques.

- La formation doit avoir lieu au moins une fois par année et porter sur les sujets suivants, notamment :
  - la sensibilisation à la fraude psychologique (hameçonnage, fraude du président, hameçonnage vocal, rançongiciel, navigation Internet sécurisée);
  - les mots de passe;
  - les données sensibles (renseignements permettant d'identifier une personne, information de contrôle du protocole, renseignements personnels sur la santé, etc.) et traitement des données;
  - le partage des données et les politiques d'utilisation acceptable;
  - la protection et la destruction des données;
  - la sécurité des appareils mobiles;
  - le réseautage social sécuritaire;
  - La violence au travail;

- Les politiques de l'entreprise en matière de sécurité.

- Une formation supplémentaire peut être nécessaire en fonction du rôle des membres du personnel au sein de l'entreprise. Par exemple, le personnel qui s'occupe des finances de l'entreprise peut avoir intérêt à comprendre comment les cybercriminels les ciblent en raison de l'accès qu'ils ont aux comptes bancaires. La formation axée sur les fonctions permet au personnel de comprendre le rôle que joue chaque membre dans la protection de l'entreprise au quotidien.
    - Utilisez du matériel de sensibilisation à la sécurité dans les salles de pause et autres espaces réservés aux membres du personnel, par exemple des rappels de formation, des affiches ou des dépliants leur rappelant de traiter les données des clients avec précaution, de se familiariser avec la sensibilisation à la fraude psychologique, etc.
    - Utilisez les bulletins d'information de l'entreprise, les courriels, les séances de formation en direct et d'autres fonctions de l'entreprise pour renforcer continuellement le message concernant la sécurité.
- Passez régulièrement en revue les programmes de formation et adaptez-les aux nouvelles technologies, à l'évolution de l'activité des concessionnaires et aux commentaires du personnel.

- Les ressources : elles sont parfois gratuites ou payantes, mais certains partenaires d'affaires peuvent proposer des formations sur la sécurité en ligne à l'intention du personnel.

    - Fournisseur de systèmes de gestion des concessions;
    - Fournisseur d'assurance;
    - Cabinet comptable;
    - Bureau de consultation juridique.
- Autres ressources :
    - Comment rendre la formation sur la cybersécurité accessible :
        - https://www.staysafeonline.org/articles/how-to-make-cybersecurity-training-accessible?utm_source=chatgpt.com
    - SANS Ouch : bulletin mensuel gratuit sur la sécurité pour le personnel (en anglais) :
        - https://securingthehuman.sans.org/resources/newsletters/ouch/2016

2.6.e Conformité aux lois fédérales

Faites en sorte que le concessionnaire respecte tous les règlements fédéraux, provinciaux, locaux et sectoriels applicables aux établissements financiers et de détail, tels que la loi Gramm-Leach-Bliley Act, la Safeguards Rule, la norme PCI DDS, etc.

- La Gramm-Leach-Bliley (GLB) Act et la Safeguards Rule :
    - La Financial Modernization Act of 1999, également connue sous le nom de Gramm-Leach-Bliley Act ou GLB Act, comprend des dispositions visant à protéger les renseignements financiers personnels des consommateurs détenus par les institutions financières. La Gramm-Leach-Bliley (GLB) Act exige que les entreprises définies comme des « institutions financières » assurent la sécurité et la confidentialité des renseignements sensibles. Étant donné que les concessionnaires louent et prêtent (même par l'intermédiaire d'un tiers), ils doivent se conformer à la GLB Act.

    - La Safeguards Rule a été émise par la Federal Trade Commission (FTC), dans le cadre de la GLB Act. La Safeguards Rule exige que les institutions financières mettent en place des mesures pour assurer la sécurité des renseignements sur les clients.

    - Pour obtenir de plus amples renseignements sur ces lois et les exigences, veuillez consulter les sites suivants (en anglais) : http://www.ftc.gov/privacy/privacyinitiatives/glbact.html https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

- La Payment Card Industry Data Security Standard (norme de sécurité sur les données de l'industrie des cartes de paiement [PCI DSS]) :
    - La norme PCI DSS est une norme mondiale de sécurité de l'information élaborée par le PCI Security Standards Council. La norme a été créée pour aider les organisations qui traitent les paiements par carte à prévenir la fraude par carte de crédit en renforçant les contrôles sur les données et leur exposition au risque de compromission.
    - Tous les commerçants qui stockent, acceptent, traitent ou transmettent des données relatives aux titulaires de cartes doivent se conformer aux exigences techniques et opérationnelles définies par la norme PCI DSS. Toutes les concessions doivent respecter la norme PCI-DSS. Toutefois, les exigences en matière de rapports et d'audits pour les concessions varient en fonction du niveau du commerçant. Le niveau du commerçant est déterminé par le nombre de transactions par carte de crédit effectuées en concession. Pour en savoir plus sur la norme PCI DSS et ses exigences, visitez le site https://www.pcisecuritystandards.org/lang/fr-fr/
- Ressources supplémentaires :
    - Les organismes suivants disposent d'informations pour la mise en œuvre de mesures de protection appropriées pour les données :
        - La National Institute for Standards and Technology (NIST) du Computer Security Resource Center (en anglais) : http://csrc.nist.gov
        - La National Strategy to Secure Cyberspace du Department of Homeland Security (en anglais) : http://www.dhs.gov/files/publications/editorial_0329.shtm
        - Le document intitulé *Twenty Most Critical Internet Security Vulnerabilities* (les vingt vulnérabilités les plus critiques en matière de sécurité Internet) de la SysAdmin, Audit, Network, Security (SANS) Institute (en anglais) : www.sans.org/top20
        - Ressources et outils (en anglais) de la Cybersecurity and Infrastructure Security Agency (CISA) :
            - https://www.cisa.gov/resources-tools
        - Le CERT Coordination Center de la Carnegie Mellon Software Engineering Institute (en anglais) : www.cert.org
        - Le Risk Assessment Questionnaire de STAR (questionnaire d'évaluation des risques [en anglais]) : https://www.starstandard.org/index.php/risk-assessment- questionnaire-2/

2.6.f Sécurité du réseau

Les concessions doivent mettre l'accent sur la sécurité et l'intégrité des données de leur réseau local (LAN). Il s'agit tout d'abord de définir des politiques d'utilisation du réseau pour le personnel et les invités. Ces politiques doivent préciser les données auxquelles chaque personne a accès, les ressources du réseau auxquelles cette personne peut accéder et l'endroit où les données sont stockées sur le réseau. Les politiques doivent également indiquer clairement sur quels appareils les données de l'entreprise sont stockées. Voir la section 2.6.a pour en savoir plus sur les politiques et les pratiques en matière de sécurité.

Au-delà des politiques, le réseau doit être configuré et segmenté de la façon la plus sécuritaire possible afin d'éviter tout accès indésirable. Suivez les recommandations suivantes lors de la configuration et de la sécurisation du réseau de la concession.

Recommandation	Caractéristiques
Pare-feu/UTM (gestion unifiée des menaces)	Dispositif de sécurité entièrement géré qui surveille en permanence les menaces par le biais d'un système de détection d'intrusion (SDI), d'un système de prévention d'intrusion (IPS) et d'autres mécanismes. L'appareil doit également présenter les caractéristiques suivantes : • Des mécanismes, comme le filtrage de paquets, l'antivirus et l'inspection dynamique de paquets; • Le filtrage des paquets et des protocoles (p. ex. IP, ICMP); • L'analyse de l'antivirus; • L'inspection des connexions en fonction de leur état; • L'exécution d'opérations mandataires sur les applications sélectionnées; • Rapport sur le trafic autorisé et refusé par le dispositif de sécurité sur une base régulière (c.-à-d. mensuellement). En raison de l'importance du pare-feu et du fait qu'il se trouve souvent sur le chemin des données pour la plupart du trafic de la concession, STAR recommande l'utilisation d'un dispositif de secours en cas de défaillance. Pour limiter les temps d'arrêt, les concessionnaires doivent envisager une solution de basculement automatique vers le dispositif de secours en cas de défaillance matérielle.
Segmentation du réseau	Les informations relatives aux cartes de paiement, aux clients, au trafic de la concession et au trafic des clients doivent être séparées par le biais d'une segmentation du réseau (telle que le VLAN) ou d'un réseau différent (comme un circuit dédié pour les invités) afin de garantir la sécurité des données.
Filtrage de contenu	La perte de données peut résulter du fait que les membres du personnel naviguent sur Internet pour des activités non liées à l'entreprise. STAR recommande aux concessions de filtrer le contenu du réseau afin d'éliminer tout trafic potentiellement nuisible, inapproprié ou non lié aux activités de l'entreprise.

Gestion des informations et des événements de sécurité (GIES)	Une solution de GIES offre une visibilité qui va au-delà de la protection par un antivirus ou un pare-feu. L'objectif ultime d'une solution de GIES est de recueillir les données relatives au trafic de sécurité du réseau et de les inspecter afin de détecter les signes de compromission. Cette indication doit être transmise, sous forme d'alerte, à une personne qualifiée afin qu'elle procède immédiatement à une enquête et à d'éventuelles mesures correctives. Il est important de noter que l'adoption d'un logiciel de GIES ne suffit pas à protéger le réseau d'un concessionnaire. Les concessions doivent disposer de processus et de ressources pour répondre aux informations générées par la technologie de GIES. Voici un conseil général pour la gestion des informations relatives à la sécurité des concessions : Les concessions doivent disposer des éléments suivants : • Une surveillance proactive et en temps réel des événements à l'aide d'un service GIES. • La GIES doit être en mesure de recueillir des données et avoir la capacité d'agréger et de mettre en corrélation des données de sécurité variables provenant du réseau en temps réel. • Le fournisseur de services de GIES doit être en mesure d'avertir l'administrateur du réseau en cas d'événement de sécurité et de fournir la documentation appropriée à des fins de conformité. • L'objectif fondamental d'un service de GIES est de contribuer à l'identification ou à la prévention d'une intrusion dans un réseau. Une réponse immédiate à une violation peut réduire ou prévenir la perte de données de manière significative. **Remarque :** il ne faut pas confondre un logiciel de gestion réactive (c.-à-d. un pare-feu sur un ordinateur de bureau, ou un antivirus) avec un service de GIES proactif.

Tests d'intrusion et analyse des vulnérabilités	Il est vivement recommandé d'effectuer chaque année des tests d'intrusion internes et externes sur le réseau des concessionnaires. Un test d'intrusion est une méthode d'évaluation de la sécurité d'un système informatique ou d'un réseau qui consiste à simuler une attaque provenant d'une source malveillante. Un test d'intrusion doit être effectué sur tout système informatique destiné à être déployé dans un environnement en réseau, en particulier ceux qui possèdent un accès à Internet ou qui sont exposés. Les activités de test d'intrusion peuvent être réalisées en externe (simulation d'une attaque depuis l'extérieur de votre réseau, exactement comme une tentative de piratage lancée depuis un pays étranger), ou en interne (depuis l'intérieur de votre réseau pour voir quels sont les accès et les vulnérabilités).
Partenaires d'intégration certifiés	Assurez-vous que les intégrateurs de données des concessionnaires sont certifiés pour les systèmes de gestion des concessions et les applications des fabricants d'équipement d'origine. Les points d'intégration non autorisés ou hostiles sont souvent moins sûrs et exigent parfois que la concession partage les informations relatives à l'utilisateur et au mot de passe.
Système de détection sans fil	Analysez, identifiez et supprimez les points d'accès sans fil indésirables qui pourraient se trouver sur le réseau du détaillant. Un point d'accès sans fil indésirable est défini comme un point d'entrée sans fil dans le réseau de la concession qui n'est pas autorisé, sécurisé ou connu des services informatiques, de la direction et des propriétaires du concessionnaire. Tous les réseaux sans fil indésirables doivent être détectés, trouvés et supprimés immédiatement. STAR recommande l'utilisation d'un service de détection sans fil géré qui analyse en permanence le réseau pour détecter les menaces liées au réseau sans fil.
Surveillance continue	La surveillance continue offre une visibilité en temps réel et démontre que les contrôles de sécurité et les mesures de protection des données sont efficaces pour détecter et prévenir les menaces. Utilisez des technologies, des processus et des procédures de surveillance continue pour vous assurer que la concession a la capacité de lancer des alertes en cas d'attaques et de vulnérabilités et d'y répondre.

Authentification multifactorielle	Mettez en œuvre l'authentification multifactorielle (AMF) pour tous les comptes privilégiés et les utilisateurs ayant besoin d'un accès à distance. Utilisez l'AMF pour toute personne (membre du personnel, fournisseur ou client) qui doit accéder à des systèmes contenant des informations sur les clients.

2.6.g Sécurité des ordinateurs de bureau

Recommandation	Caractéristiques
Surveillance des virus sur les ordinateurs	Des produits antivirus de qualité professionnelle doivent être installés sur tous les ordinateurs et configurés pour effectuer automatiquement les opérations suivantes : • Téléchargement et installation des mises à jour les plus récentes des signatures de virus; • Surveillance active des virus; • Mise en quarantaine et suppression des fichiers infectés; • La solution d'antivirus doit comprendre un antivirus, un logiciel anti-espion, une prévention d'intrusion, un contrôle d'application, un antipourriel et une détection de trousse administrateur pirate.

Gestion des correctifs	STAR recommande que la gestion des correctifs soit effectuée sur chaque ordinateur afin de s'assurer que tous les postes de travail disposent des correctifs Microsoft les plus récents. La gestion des postes de travail doit inclure la surveillance à distance des défaillances matérielles et logicielles, des pannes de serveurs, du manque d'espace disque, de l'utilisation excessive de l'unité centrale et de la mémoire.
Protection par mot de passe	Les mots de passe doivent expirer tous les 60 jours ou moins. Les concessions doivent au moins utiliser des « mots de passe forts » contenant un minimum de huit caractères et comprenant trois des quatre exigences suivantes : 1) Une majuscule; 2) Une minuscule; 3) Un caractère numérique; 4) Des caractères spéciaux.
Détection des points d'extrémité et plateforme d'intervention	• Une plateforme de protection des points d'extrémité et une solution de détection et d'intervention sur les terminaux doivent être déployées sur les points d'extrémité afin de prévenir les attaques de logiciels malveillants à partir de fichiers, de détecter les activités malveillantes et de fournir les capacités d'investigation et de remise en état nécessaires pour répondre aux incidents et aux alertes de sécurité actives. Les alertes émises par ce service doivent être traitées immédiatement afin de limiter les risques et les pertes potentielles de données. L'offre de services doit permettre une visibilité multiplateforme des activités des points d'extrémité et des serveurs, ainsi que des activités suivantes : une détection des menaces grâce à des moteurs d'IA statiques et comportementaux, et un système de détection des intrusions sur l'hôte (SDIH) au sein de l'agent du point d'extrémité; • Le confinement des menaces et les conseils en matière de remédiation; • Les rapports sur les activités et la chasse aux menaces; • La visibilité multiplateforme sur l'exécution des processus, les communications réseau, l'accès aux fichiers, les applications, les requêtes DNS et le trafic Web chiffré.

2.6.h Sécurité des courriels

Aperçu : La sécurité des courriels est un risque critique pour de nombreuses organisations parmi les plus importantes au monde. Aujourd'hui, 91 % des attaques réussies sur les réseaux d'entreprise impliquent l'utilisation du courrier électronique. Une solution de sécurité des courriels permet d'inspecter le contenu entrant et sortant, de le chiffrer et d'émettre des alertes de sécurité afin d'atténuer la plupart de ces risques.

Sécurité des courriels sortants : Identifiez les logiciels malveillants, les courriels inappropriés, les contenus non autorisés et les renseignements confidentiels de l'entreprise avant qu'ils ne quittent le réseau, et intervenez en conséquence.

Sécurité des courriels entrants : Appliquez des filtres pour bloquer les logiciels malveillants, l'hameçonnage ou les courriels malveillants avant qu'ils ne s'introduisent dans le réseau.

Chiffrement : Le chiffrement des courriels par le protocole TLS (Transport Layer Security) est recommandé pour rendre plus difficile la lecture du courrier électronique par des tiers pendant son acheminement.

2.6.i Sécurité des applications

Pour la présente section, supposons que toutes les applications ont été acquises auprès de fournisseurs externes et déployées soit sans aucune modification, soit avec un minimum de personnalisation. On entend également, par application, toutes celles qui concernent les entreprises. La sécurité des applications consiste à s'assurer que toutes les données traitées et toutes les fonctions d'affaires offertes par l'application sont protégées de manière appropriée.

- Domaines et activités principales
    - Effectuez un inventaire des applications. Documentez les applications présentes sur le réseau de la concession, quels sont leurs objectifs, qui en est responsable et comment obtenir du soutien. Effectuez une analyse des répercussions sur les activités (ARA), y compris la classification des informations, afin de comprendre la criticité opérationnelle et d'appliquer un ordre de priorité approprié. Ce registre permettra également de repérer et d'éliminer les applications malveillantes qui peuvent constituer une menace pour le réseau des concessionnaires et la sécurité des données.
    - Protégez les informations traitées lors de leur transmission et de leur stockage. Veillez à ce que les données sensibles et critiques soient bien protégées, tant du point de vue de la confidentialité que de l'intégrité. Examinez l'intégration des applications entre elles ainsi que les applications de communication interne, en particulier les connexions aux bases de données, qui sont très souvent oubliées. Si nécessaire, assurez-vous que la méthode de cryptographie utilisée pour la protection du stockage est appropriée. Enfin, assurez-vous que les flux d'informations sont protégés de bout en bout.
    - Tenez compte des exigences opérationnelles supplémentaires, telles que l'authenticité, la non-répudiation ou la traçabilité, souvent requises pour respecter les réglementations en matière de protection des données personnelles (p. ex. le Règlement général sur la protection des données [RGPD]).
    - Appliquez le principe de la défense en profondeur en mettant en œuvre une configuration précise des zones de sécurité et des composants d'application, des services d'infrastructure supplémentaires, comme des mandataires inverses ou des pare-feu d'application Web, et des couches de contrôle d'accès telles que l'authentification multifactorielle, etc.
    - Mettez en place une stratégie appropriée de gestion des identités et de gestion des accès (voir la section IAM pour plus de détails). Appliquez les principes du droit d'accès minimal et du besoin de connaître.
    - Exigez d'un fournisseur les résultats d'une analyse de la vulnérabilité des applications réalisée par une

entreprise tierce indépendante. Veillez à ce que tous les risques de niveau moyen et élevé identifiés soient pris en compte.

- Une partie de la stratégie de sécurité consiste également à s'assurer que les transactions commerciales sont traitées sans erreur et en respectant le niveau de qualité attendu. On peut donc s'attendre à ce qu'un fournisseur produise des résultats de tests ou des rapports d'audit.
- Mettez en place des procédures de traitement des incidents, des demandes d'accès, etc. Envisagez de mettre en place une surveillance des applications d'affaires afin de repérer, voire de prévenir, les événements indésirables. Généralement, cette démarche s'inscrit dans le cadre de la mise en œuvre d'une gestion des services informatiques.
- Exécutez régulièrement des activités de modélisation des menaces afin de vous assurer que les risques liés à l'environnement applicatif sont documentés, atténués et maintenus sous contrôle.
- Appliquez les mises à jour et les correctifs des applications dès que possible afin de limiter les risques d'exploitation.

2.6.j Mobilité

Ce domaine est étroitement lié à d'autres domaines, tels que la sécurité des applications ou la sécurité des courriels. Toutefois, il est traité séparément en raison des risques supplémentaires qu'il introduit à cause du contrôle beaucoup plus limité des types d'appareils visés. Les appareils mobiles sont définis ici comme des téléphones intelligents, des tablettes, des ordinateurs portables et tout autre appareil spécialisé qui traite ou contient des données de l'entreprise.

- Domaines et activités principales
  - Créez des politiques et des procédures pour savoir qui peut accéder à distance à l'environnement de l'entreprise, quand et comment, et à quelles parties (réseau, serveurs, applications, etc.). Par exemple, une politique peut autoriser les téléphones intelligents et les tablettes à accéder au réseau externe de l'entreprise et restreindre l'accès à son réseau interne; elle peut également autoriser l'accès au réseau interne de l'entreprise pour les ordinateurs portables gérés au moyen d'un réseau privé virtuel (RPV). Déployez une solution technique appropriée pour soutenir l'approche établie.
  - Définissez les informations qui peuvent être traitées et stockées sur les appareils mobiles; veillez à inclure les considérations relatives aux appareils gérés et non gérés.
  - Mettez en place des politiques, des procédures et des capacités techniques pour définir les logiciels qui peuvent être installés et exécutés sur tous les types d'appareils mobiles. Dans le cas d'appareils non gérés, établissez des conditions dans lesquelles les données de l'entreprise ne sont pas exposées à des risques inacceptables (p. ex. en installant des solutions telles que MobileIron ou Microsoft Intune pour les téléphones intelligents).
  - L'accès aux appareils doit être restreint, nécessitant l'authentification de l'utilisateur. La plupart des appareils peuvent être verrouillés au moyen d'un verrouillage d'écran, d'un mot de passe ou d'un numéro d'identification personnel (NIP).
  - Appliquez la stratégie appropriée de gestion des identités et des accès.
  - Assurez-vous de la bonne configuration et du renforcement des appareils et du système d'exploitation (p. ex. mot de passe du BIOS, chiffrement au niveau de l'appareil, disponibilité des ports USB et SD). Assurez-vous que l'appareil n'est pas débloqué ou débridé (en particulier dans le cas des appareils Android et iOS).

- Maintenez à jour un logiciel antimaliciel et, de préférence, gérez-le de manière centralisée, à la fois sur les ordinateurs portables et les téléphones intelligents.
- Mettez à jour le système d'exploitation mobile avec les correctifs de sécurité. De plus amples informations sur la gestion des correctifs sont disponibles à la section 2.6.c.
- Appliquez un chiffrement approprié des données à la fois sur les ordinateurs portables et les appareils mobiles, en accordant une attention particulière à la gestion des clés de déchiffrement.
- Passez en revue toutes les méthodes de connectivité, en accordant une attention particulière à la connectivité sans fil automatisée, car les mots de passe peuvent être exposés et des attaques par interception peuvent être exécutées.
- Activez l'option d'effacement des données à distance si elle est disponible.
- Sauvegardez régulièrement le contenu de l'appareil mobile.

- Considérations relatives à la politique « apportez votre appareil personnel de communication (AVEC) »
  - Lorsque les appareils mobiles utilisés par le personnel ou les sous-traitants à des fins professionnelles ne sont pas fournis par la concession, une politique AVEC détaillée est nécessaire et doit aborder les principaux aspects décrits ci-dessous, en plus des activités et des domaines clés déjà mentionnés :
    - Indiquez quelles tablettes, quels téléphones portables, etc., sont autorisés. Les anciens appareils peuvent ne pas être dotés d'un niveau de sécurité nécessaire pour protéger de manière adéquate les données privées de l'entreprise.
    - Veillez à ce qu'il soit clair que TOUTES les données recueillies dans le cadre des activités professionnelles appartiennent à l'entreprise.
    - Identifiez les applications qui ne sont pas autorisées sur les appareils.
    - Utilisez des gestionnaires de mots de passe chiffrés plutôt que d'utiliser ceux qui sont basés sur un navigateur et qui ne sont pas chiffrés, en particulier pour l'accès aux applications d'entreprise.
    - Exigez l'authentification multifactorielle (AMF) pour l'accès aux réseaux d'entreprise.
    - Mettez en œuvre des logiciels et des applications qui séparent l'utilisation personnelle de l'utilisation professionnelle, comme une application de navigation contrôlée par l'équipe informatique de l'entreprise.
    - Déterminez les limites de l'utilisation des données professionnelles et leur suppression lorsqu'elles ne sont plus nécessaires aux activités de l'entreprise.
    - Précisez la politique d'effacement des appareils en cas d'incident lié à la sécurité de l'information. L'effacement peut entraîner la perte de données personnelles comme des photos et des coordonnées.
    - Définissez les exigences relatives au signalement des appareils perdus et à la capacité d'effacement à distance en cas de perte ou de vol d'un appareil.
    - Veillez à ce que la politique AVEC fasse l'objet d'une surveillance et que les utilisateurs n'aient aucune attente en matière de respect de la vie privée en ce qui concerne l'utilisation professionnelle ou les données d'entreprise.
    - Toutes les données commerciales sont la propriété de l'entreprise et sont accessibles à la demande de l'entreprise.

- Le nettoyage des données relatives aux appareils personnels doit faire partie de la procédure de gestion des départs lors d'une cessation d'emploi. Les entreprises doivent disposer d'une capacité d'accès à distance permettant d'effacer les données privées de l'entreprise d'un appareil dans le cas où un membre du personnel quitterait l'entreprise sans préavis.
- Exigez le chiffrement des appareils et l'utilisation d'un réseau privé virtuel (RPV) pour l'usage professionnel.
- Mettez en place une formation sur l'utilisation correcte des appareils personnels à des fins professionnelles, ainsi que des politiques définissant l'utilisation correcte des applications et des données professionnelles sur les appareils personnels.

2.7 Fournisseurs de services gérés

Les concessionnaires se tournent souvent vers des fournisseurs ou des partenaires pour les aider à gérer, à entretenir et à sécuriser l'infrastructure de la concession. Un fournisseur de services peut disposer de la technologie ou de l'expertise nécessaire pour fournir à la concession une solution permettant de gérer plus efficacement les différents aspects du réseau des concessionnaires. Les concessionnaires ne disposent souvent pas du temps, des ressources ou de l'expertise nécessaires pour gérer seuls un réseau d'entreprise. Le recours à un fournisseur de services peut donc s'avérer un choix logique.

Une entente de niveau de service (ENS) est très importante lors de la sélection d'un tiers responsable du soutien de l'infrastructure du réseau. Le fournisseur doit s'engager sur le niveau de service à fournir, sur l'étendue du ou des services et sur les éventuels remboursements ou frais de compensation pour les obligations non respectées.

La section suivante fournit des conseils pour déterminer les ententes de niveau de service et les comprendre.

2.7.a Ententes de niveau de service (ENS)

Les concessions qui bénéficient de services informatiques accordent une grande confiance à l'entente de niveau de service (ENS) qu'elles choisissent. L'entente de niveau de service détaille la qualité de service (QOS) que le fournisseur offre avec son service. En d'autres termes, il s'agit d'une garantie que le service sera fourni comme convenu.

Les ententes de niveau de service sont utilisées dans une grande variété de services de TI des concessionnaires qui comprennent notamment, mais pas exclusivement, les suivants :

- Les services Internet;
- Les services d'intégration de réseau;
- Les services de soutien matériel et logiciel;
- Le soutien sur place;
- Le soutien du centre d'assistance et du centre d'appel.

Lorsque vous choisissez un fournisseur de services, assurez-vous de poser les questions suivantes au sujet des ententes de niveau de service :

- Existe-t-il une entente de niveau de service écrite?
- Quels sont les contretemps, les remboursements ou les autres conséquences si le fournisseur ne respecte pas son entente de niveau de service?
- Existe-t-il des rapports sur l'entente de niveau de service?
- Le service peut-il être annulé si l'entente de niveau de service n'est pas respectée?

Les ententes de niveau de service les plus courantes sont notamment, mais pas exclusivement, les suivantes :

- La disponibilité du réseau;
- La vitesse du réseau;

- La latence du réseau;
- Les délais de remplacement du matériel;
- Les heures de soutien offertes;
- Les engagements en matière de services sur place;
- Les ententes de maintenance du matériel ou des logiciels.

2.8 Gestion des données

2.8.a Sauvegarde des données

Il est essentiel de disposer d'une sauvegarde des données de la concession pour assurer la continuité des activités. Il est fréquent que la disponibilité des données devienne un problème grave en raison d'incidents de cybersécurité, d'incidents physiques ou d'erreurs humaines. Lorsque ces incidents se produisent, il est important que les concessions disposent d'une lecture de sauvegarde et d'un plan de remise en état. STAR recommande aux concessions d'effectuer une sauvegarde complète et incrémentale à intervalles réguliers afin d'assurer la disponibilité et la redondance des données.

Sauvegarde des données	Les données des serveurs, des points d'extrémité et des équipements de réseau doivent être sauvegardées dans d'autres emplacements.	Pour plus d'informations, voir Sections 2.2.c et 2.4.a

2.8.b Sécurité des données (chiffrement)

Le chiffrement dans les réseaux informatiques est le processus de conversion des données dans un format sécurisé qui ne peut être consulté ou décodé que par des parties autorisées. Le chiffrement des données garantit que les informations ne demeurent accessibles qu'en cas de nécessité et aux destinataires désignés. STAR conseille aux concessions de mettre en place un système de chiffrement pour les réseaux sans fil, les communications par courriel, les terminaux et les connexions à distance (RPV).

Suivez les lignes directrices suivantes lorsque vous utilisez le chiffrement dans l'architecture de votre concession.

Chiffrement sans fil	Liaison WPA2 (Wi-Fi Protected Access II) avec authentification RADIUS et chiffrement AES. Remarque : consultez les recommandations du fabricant d'équipement d'origine pour obtenir des conseils sur la compatibilité avec les technologies propres au fabricant d'équipement d'origine.
Chiffrement des courriels	Le chiffrement des courriels par le protocole TLS (Transport Layer Security) est recommandé pour rendre plus difficile la lecture du courrier électronique par des tiers pendant son acheminement.
Chiffrement des points d'extrémité	Appliquez un chiffrement approprié des données à la fois sur les ordinateurs portables et les appareils mobiles, en accordant une attention particulière à la gestion des clés de déchiffrement.
Chiffrement du RPV	Exigez le chiffrement des appareils et l'utilisation d'un réseau privé virtuel (RPV) pour l'usage professionnel.

2.8.c Gouvernance de l'intelligence artificielle (IA)

L'IA est un outil précieux pour améliorer l'efficacité des concessions, acquérir des renseignements supplémentaires et effectuer des analyses de données avancées. Cependant, l'utilisation de l'IA dans le domaine de la concession soulève des inquiétudes quant à la sécurité des données des concessionnaires, des clients et des fabricants d'équipement d'origine. Lorsque vous utilisez des outils d'IA, tenez compte des considérations suivantes :

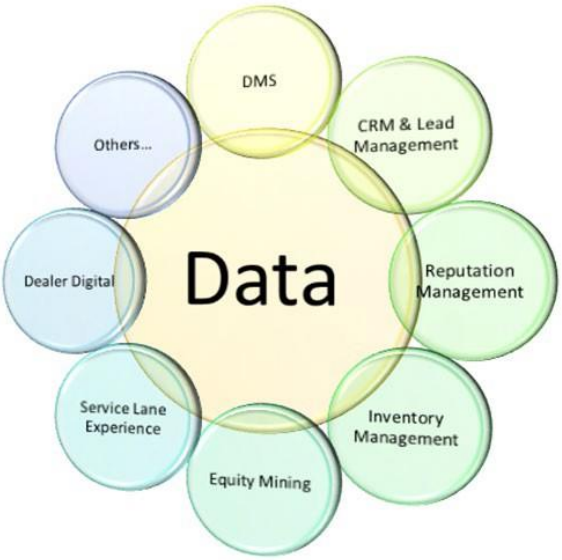
- L'anonymisation et la minimisation des données : anonymisez les données personnelles, ne recueillez que les renseignements nécessaires et mettez en œuvre des politiques de conservation des données afin de réduire les risques.
- La gestion sécurisée du modèle d'IA : séparez les modèles des systèmes de production, mettez en place un contrôle des versions et testez régulièrement la présence de vulnérabilités.

- L’évaluation de la sécurité des fournisseurs : examinez minutieusement les fournisseurs d’IA, assurez-vous de leur conformité à la réglementation et vérifiez régulièrement leurs mesures de sécurité. Veillez également à ce que les exigences de tous les fournisseurs en matière de gouvernance et de sécurité des données soient conformes à vos propres politiques et exigences réglementaires.
- La formation et la sensibilisation du personnel : offrez des formations régulières en matière de sécurité, informez le personnel sur les menaces et encouragez une culture de la sensibilisation à la sécurité.
- Les considérations relatives au partage, à la propriété et à l’utilisation des données : assurez-vous que les données fournies ou partagées avec un modèle d’IA ne sont pas partagées, vendues ou utilisées à d’autres fins que le cas d’utilisation prévu par la concession.

3. Fournisseurs de systèmes pour les concessionnaires

3.1 Aperçu

La complexité d'une concession et de sa technologie connexe a beaucoup évolué depuis la création de STAR. Cette technologie en constante évolution a continué à améliorer la valeur commerciale globale de STAR et les normes d'intégration utilisées pour harmoniser les données entre les systèmes et les processus.



Alors que le système de gestion des concessions a toujours été au cœur de l'écosystème technologique des concessionnaires, il existe aujourd'hui de nombreux systèmes différents qui doivent tous partager des données pour garantir une gestion efficace des clients, des véhicules et des pièces tout au long du parcours en ligne et hors ligne. L'écosystème des fournisseurs de systèmes pour les concessionnaires est en constante évolution, et il est absolument essentiel de veiller à ce que des processus soient mis en œuvre pour assurer une intégration sécurisée et efficace des données.

Les choix de fournisseurs de systèmes pour les concessionnaires changent de jour en jour, et il est essentiel pour les concessionnaires de comprendre l'importance d'une intégration des données sécurisée et efficace.
Il existe des solutions de fournisseur de systèmes pour les concessionnaires qui se concentrent sur la partie frontale de la concession et d'autres qui se concentrent sur la partie dorsale. D'autres solutions visent à gérer les clients en ligne et hors ligne et certaines cherchent spécifiquement à aider les concessions à commercialiser les stocks de véhicules neufs et d'occasions, à gérer et à distribuer le contenu ou à maintenir une image positive dans les médias sociaux et le monde en ligne.

Que ce soit avec un fournisseur qui propose de nombreux produits ou avec un fournisseur spécialisé dans une fonction précise, il est important de comprendre comment les données sont intégrées et gérées dans l'ensemble de l'écosystème.

Il n'existe pas d'approche unique pour la mise en œuvre d'une solution de fournisseur de systèmes pour les concessionnaires, mais il est essentiel d'aligner les technologies sur les priorités de l'entreprise et de mettre en œuvre des processus de gouvernance des données qui soutiennent l'expérience client souhaitée. Les clients recherchent de plus en plus une expérience en ligne et hors ligne transparente, ce qui est possible uniquement grâce à l'intégration des données.

La concession dispose d'un grand nombre de choix lorsqu'elle décide quels fournisseurs de systèmes pour les concessionnaires doivent être utilisés au sein de leur réseau. Les fournisseurs de systèmes pour les concessionnaires servent souvent de « centre » pour les données, les communications et les opérations commerciales des concessionnaires. Lors de l'examen des différentes offres des fournisseurs de systèmes pour les concessionnaires, la section sur l'infrastructure du réseau des concessionnaires des *Lignes directrices de STAR relatives à l'infrastructure des concessionnaires* peut fournir des indications sur les différentes fonctions qu'un fournisseur de services de systèmes peut offrir aux concessionnaires.

3.2 Normes et intégration des données : l'avantage STAR

L'organisation STAR et les normes d'intégration qu'elle contient ont été créées pour optimiser les activités d'intégration des données des concessionnaires entre le fabricant d'équipement d'origine et le fournisseur de système pour les concessionnaires (principalement le système de gestion des concessionnaires au début) en utilisant l'Internet comme moyen principal.

Comme toute autre technologie, l'Internet n'a cessé d'évoluer et l'infrastructure utilisée pour faire fonctionner les entreprises qui l'utilisent a fait l'objet d'un nombre considérable d'innovations. Ces améliorations ont permis de mettre au point une méthode particulièrement fiable pour intégrer les processus d'affaires et les systèmes connexes.

Au cœur de tous ces systèmes se trouvent les données nécessaires pour soutenir le processus opérationnel souhaité. Les données relatives aux véhicules, aux pièces, aux clients, aux services, aux finances et à de nombreux autres groupes de données doivent circuler d'un système à l'autre, et entre le concessionnaire (au moyen du fournisseur de systèmes pour les concessionnaires) et le fabricant d'équipement d'origine, de manière transparente et sécurisée. Les normes d'intégration des données STAR sont des normes ouvertes qui permettent aux fournisseurs et aux fabricants d'équipements d'origine de réduire le temps de développement global et de simplifier les déploiements grâce à un ensemble de documents décrivant les éléments de données nécessaires pour soutenir les objectifs commerciaux (Business Object Documents [BOD]).

Au fil du temps, ces BOD peuvent être enrichis de définitions ou de règles d'affaires et alignés sur diverses méthodologies de transport de données afin de fournir des intégrations de données efficaces et reproductibles. Lorsque STAR a démarré cet important parcours, l'écosystème était beaucoup plus simple. En devenant de plus en plus complexe chaque année, le paysage technologique des concessionnaires permettra réellement aux normes d'afficher les avantages de STAR!

3.3 Paysage technologique des concessionnaires (choix de fournisseurs de systèmes pour les concessionnaires [DSP Choices])

Il semble que le paysage technologique des concessionnaires sera en constante évolution dans un avenir prévisible. Prendre le temps de définir ce paysage ne ferait que produire un document qui deviendrait désuet peu de temps après sa publication.

Ces dernières années, plusieurs catégories de produits de fournisseurs de systèmes pour les concessionnaires nouveaux et importants ont rejoint les systèmes traditionnels de gestion des concessionnaires et ont laissé une marque permanente dans l'écosystème de la vente au détail de véhicules automobiles, c'est pourquoi il est utile de fournir quelques renseignements généraux à leur sujet. Comme pour tous les choix de fournisseurs de systèmes pour les concessions, il convient de prendre le temps de comparer les capacités et de s'assurer que la solution est conforme aux lignes directrices de STAR relatives à l'infrastructure.

Outre la comparaison des capacités et la compréhension de l'intégration globale, il est extrêmement important de comprendre la gestion des données et les éléments à option d'adhésion ou de retraite associés à la solution. Une gouvernance complète des données et une transparence de l'utilisation sont cruciales pour toute solution en matière de fournisseurs de systèmes pour les concessionnaires et les fabricants d'équipements d'origine.

3.3.a DMS (système de gestion des concessions)

Le système de gestion des concessions est un système d'information de gestion groupé créé spécialement pour les concessions de l'industrie automobile. Il a été adapté (généralement sous la forme d'un produit de gestion des concessions spécialisé) pour les concessionnaires d'équipements lourds, de bateaux, de vélos, de véhicules récréatifs et d'équipements de sports motorisés. Le système de gestion des concessions contient des fonctionnalités permettant de gérer les finances, les ventes, l'inventaire, les pièces, le service et les composants de comptabilité et de bureau d'affaires pour le fonctionnement de la concession.

Certaines solutions de système de gestion des concessions sont proposées avec des serveurs centraux sur site, tandis que d'autres tirent parti de l'infonuagique en utilisant un modèle de logiciel-service (SaaS); une solution sur site ou basée sur le SaaS peut convenir, en fonction des besoins de la concession. Il est important de tenir compte de la maintenance du matériel utilisé pour répondre aux besoins des applications. Les services SaaS sont générés dans le nuage et nécessitent peu de maintenance, tandis que les solutions sur site requièrent souvent une gestion des correctifs, des mises à niveau et une maintenance générale des serveurs.

Bien que les fonctionnalités générales des deux solutions soient semblables d'un système de gestion des concessions à l'autre, les capacités de chacun peuvent varier. Dans tous les cas, il est essentiel de veiller à ce que la solution prenne en charge les réglementations nationales, locales, du marché et régionales, ainsi que les marques des fabricants d'équipement d'origine pour le groupe de concessions concerné.

3.3.b Gestion de la relation client et gestion des clients potentiels

Les systèmes de gestion de la relation client et de gestion des clients potentiels permettent de capturer, de suivre et de gérer efficacement les communications en ligne et hors ligne avec les clients actuels et potentiels.

Les solutions de gestion de la relation client et de gestion des clients potentiels nécessitent une intégration avec les données du système de gestion des concessions (clients) et toutes les sources de clients potentiels.

Le système de gestion de la relation client offre des fonctionnalités qui aident le personnel des concessions à gérer les relations avec les clients tout au long du cycle de vie de ces derniers. Les dates importantes relatives aux clients et aux véhicules, les rendez-vous d'entretien et bien d'autres aspects peuvent tous être gérés.

Le système de gestion des clients potentiels offre une fonctionnalité permettant d'attribuer les clients potentiels au personnel des ventes et des services (ou par l'intermédiaire d'un centre de développement commercial défini) pour en assurer le suivi. Ces activités de suivi des clients potentiels visent toutes à augmenter les ventes et le chiffre d'affaires.

Les clients potentiels (demandes de renseignements) sont regroupés et stockés à partir de nombreuses sources différentes, notamment, mais pas exclusivement, les suivantes :

- Visites sans rendez-vous;
- Achats en ligne;
- Clients fournis par le fabricant d'équipement d'origine;
- Contacts téléphoniques;
- Clients saisis lors d'événements.

Les solutions de gestion de la relation client et de gestion des clients potentiels sont également utilisées pour générer de nouvelles occasions d'affaires. En harmonisant les solutions des concessionnaires aux manifestes des fabricants d'équipement d'origine, à d'autres solutions des fournisseurs de systèmes pour les concessionnaires (p. ex. l'exploitation de l'équité) et aux besoins en matière de voitures d'occasion, il est possible de joindre efficacement les clients existants et de créer des occasions d'affaires supplémentaires.

Les concessions ont besoin d'une infrastructure en place pour prendre en charge les clients potentiels provenant des entreprises de niveau 3. Une solution efficace de gestion des clients potentiels doit également prendre en considération les organisations de niveau 3 (telles que cars.com et truecar.com).

3.3.c Gestion de la réputation

Une solution de gestion de la réputation offre des fonctionnalités qui vous aident à surveiller, à comprendre, à identifier et à traiter ce que les gens écrivent en ligne au sujet de votre concession.

Une solution de gestion de la réputation nécessite une intégration avec les sources de données des fournisseurs de systèmes pour les concessions et les fabricants d'équipements d'origine.

La réputation en ligne d'une concession se définit par les commentaires publiés sur les sites d'avis de clients, les blogues, les sites Web et les réseaux sociaux. Internet permet de trouver facilement et sans effort des renseignements sur une concession. En quelques clics, un client peut obtenir un aperçu d'une concession, de son emplacement et de l'opinion générale des clients à son sujet. Dans la plupart des cas, les résultats de recherche incluent des avis et des classements par étoiles. Ces évaluations et avis influencent la décision d'un client d'acheter un véhicule dans une concession donnée.

3.3.d Gestion des stocks en ligne

Une solution de gestion des stocks des concessionnaires offre des fonctionnalités permettant la commercialisation, la gestion du contenu et la distribution des stocks de véhicules. Il s'agit notamment de la distribution par les concessionnaires de leur stock de véhicules neufs et d'occasions dans des publications en ligne ou imprimées, accompagnée de photos des véhicules, de vidéos de présentation, des prix, des offres promotionnelles, etc.

Une solution de gestion des stocks pour les concessions nécessite des intégrations avec le système de gestion des stocks, des outils d'établissement de prix tiers, des fournisseurs de services pour les terrains, des fournisseurs de services de description des véhicules (validation du numéro d'identification du véhicule et données sur la fabrication), et des fabricants d'équipement d'origine.

3.3.e Exploitation de l'équité

Une solution d'exploitation de l'équité permet d'identifier les consommateurs qui disposent d'une équité sur leur véhicule et de les présenter comme des ventes potentielles par l'intermédiaire d'un centre de développement des affaires, d'un responsable Internet, d'une équipe de vente ou d'autres représentants compétents d'un concessionnaire.

Une solution d'exploration de l'équité nécessite une intégration avec les données des fournisseurs de systèmes pour les concessions (clients), la gestion de la relation client ou des clients potentiels, les sources de reprise, les données bancaires (financement et location) et les incitatifs.

3.3.f Outils d'aire de service

Les outils d'aire de service sont une solution basée sur un processus ou un flux de travail qui englobe des fonctionnalités que l'on trouve traditionnellement dans des solutions distinctes liées aux services (c.-à-d. système de gestion des concessions, programmation des services en ligne, menus de service, contrôles de l'état des véhicules, etc.). Elle permet d'offrir au client une expérience cohérente et homogène tout au long des étapes suivantes : 1) prise de rendez-vous, 2) rédaction du rapport d'entretien, 3) entretien du véhicule et 4) remise en service du véhicule.

Les outils d'aire de service requièrent une intégration avec les sources de données du système de gestion des concessions et des fabricants d'équipement d'origine.

3.3.g Marketing numérique pour les concessionnaires

Une trousse de marketing numérique pour les concessionnaires est une suite de services de marketing de détail qui permet aux concessionnaires de diffuser des messages cohérents et synchronisés aux consommateurs en utilisant des canaux numériques et émergents. Il s'agit d'une plateforme intelligente de marketing de réseau qui permet d'aligner le marketing des marques et des concessionnaires. Elle fournit également des analyses permettant d'optimiser les dépenses de marketing à plusieurs niveaux et d'améliorer les performances du réseau des concessionnaires dans les processus de marketing et de vente.

Les solutions numériques pour les concessionnaires nécessitent une intégration avec les sources de données des systèmes de gestion des concessions, de gestion de la relation client et des fabricants d'équipement d'origine.

Les composants de base d'une solution numérique pour les concessionnaires peuvent comprendre les éléments suivants :

- Site Web du concessionnaire (Web et mobile);
- Optimisation pour les moteurs de recherche (SEO);
- Gestion du public cible;
- Perspectives et analyses;
- Gestion des actifs (images, vidéos, ,etc.);
- Clavardage;
- Prise de rendez-vous.

4. Reprise après sinistre et continuité des activités

4.1 Aperçu

La reprise après sinistre et la continuité des activités sont la capacité d'une organisation à se remettre d'un sinistre et à rétablir le fonctionnement normal du réseau. Les concessions doivent disposer d'un plan qui détaille la technologie utilisée, les processus à suivre et les mesures procédurales à prendre en cas de défaillance. La clé d'une reprise après sinistre réussie est d'avoir un plan bien avant qu'une panne ne se produise.

La planification de la reprise après sinistre et de la continuité des activités est un processus qui aide les organisations à se préparer à des événements perturbateurs, qu'il s'agisse d'une tornade dévastatrice ou d'une simple rupture de ligne Internet causée par des gels et des dégels répétés.

Pour comprendre ce qui pourrait se produire en cas de défaillance du réseau, une concession doit d'abord comprendre la nature des données qui sont à risque. Pendant combien de temps ces données peuvent-elles être indisponibles? Que se passe-t-il lorsqu'elles ne sont pas disponibles? Quelles mesures peuvent être prises pour s'assurer que le risque est atténué? La présente section apporte des réponses de base à ces questions, ainsi que des recommandations pour planifier les défaillances et rétablir le fonctionnement du réseau.

4.2 Analyse et atténuation des risques

L'objectif principal de l'analyse des risques est d'aider la concession à identifier toutes les zones pour lesquelles il peut y avoir un risque de perte. Il peut s'agir de matériel, de logiciels, de bâtiments, de personnel, etc. Une fois les différents éléments identifiés, la concession peut classer le niveau de chaque risque et déterminer comment ces risques peuvent l'affecter.

Certaines des différentes catégories de risques auxquelles une concession peut être confrontée sont énumérées ci-dessous :

- Le personnel essentiel;
- Le bâtiment;
- Une perturbation ou une défaillance d'Internet;
- Une défaillance du système principal;
- Une défaillance totale du système;
- La perte de données.

Une organisation peut atténuer les risques de diverses façons. Les solutions ou les plans ci-dessous peuvent être mis en œuvre sur place ou hors site. Voici quelques exemples.

Options d'atténuation des risques sur place	Options d'atténuation des risques hors site
Matériel redondant	Logiciel de sauvegarde à distance
Logiciel et serveurs de sauvegarde de données sur place	Stockage infonuagique
Alimentation sans interruption (ASI)	Contrats de services des équipements de technologie RMA
Génératrices	

5. Informatique en nuage et virtualisation

5.1 Aperçu

Les grandes tendances émergentes dans le domaine des technologies de l'information peuvent être résumées comme étant un paradigme basé sur les services et la virtualisation. Avec un « paradigme basé sur les services », nous condensons différents acronymes, tels que l'architecture axée sur le service (AOS) et le concept populaire d'informatique en nuage (qui a des implications commerciales pertinentes). *Selon les informations de Wikipédia, la principale technologie qui permet l'informatique en nuage est la virtualisation. La virtualisation apporte l'agilité nécessaire pour accélérer les opérations informatiques et réduit les coûts en améliorant l'utilisation de l'infrastructure.*

5.2 Virtualisation client/serveur

La virtualisation, en informatique, consiste à créer une version virtuelle d'un appareil ou d'une ressource, comme un serveur, une unité de stockage, un réseau, etc., où le « cadre » divise la ressource en un ou plusieurs environnements d'exécution. Les applications et les utilisateurs humains peuvent interagir avec la ressource virtuelle comme s'il s'agissait d'une ressource physique unique et réelle. Dans l'environnement d'un concessionnaire, les domaines les plus pertinents pour la virtualisation sont la virtualisation des serveurs et la virtualisation des clients. Ces deux domaines sont intéressants et garantissent des économies constantes.

5.3 Informatique en nuage

Selon la définition du National Institute of Standards and Technology (NIST), l'informatique en nuage est un modèle qui permet un accès omniprésent, pratique et à la demande à un ensemble partagé de ressources informatiques configurables (par exemple, réseaux, serveurs, espaces de stockage, applications et services) qui peuvent être rapidement fournies et restituées avec un minimum d'efforts de gestion ou d'interaction avec le fournisseur de services.

L'informatique en nuage repose sur le partage des ressources afin de réaliser des économies d'échelle, à l'instar d'un service public (comme le réseau électrique), sur un réseau. Le concept plus large de services partagés et normalisés, exploités selon un modèle de consommation, est à la base de l'informatique en nuage.

Selon le NIST, le modèle infonuagique est composé de trois modèles de services de base :

- Le logiciel-service (SaaS) offre au consommateur la possibilité d'utiliser les applications du fournisseur fonctionnant sur une infrastructure infonuagique.
- La plateforme-service (PaaS) offre au consommateur la capacité de déployer sur l'infrastructure infonuagique des applications créées par le consommateur, ou des applications acquises à l'aide de langages de programmation, de bibliothèques, de services et d'outils pris en charge par le fournisseur.
- L'infrastructure-service (IaaS) offre au consommateur la capacité de fournir des ressources de traitement, de stockage, de réseau et d'autres ressources informatiques fondamentales où le consommateur peut déployer et exécuter des logiciels arbitraires, qui peuvent inclure des systèmes d'exploitation et des applications.

Le courrier électronique et la gestion de la relation client sont déjà utilisés par de nombreux concessionnaires dans le cadre d'un modèle SaaS. De nombreux fournisseurs de systèmes de gestion des concessions proposent déjà un modèle semblable au modèle SaaS pour leur système de gestion des concessions. Les deux autres modèles sont rarement adoptés par les concessionnaires, à quelques exceptions près (p. ex. IaaS pour la reprise après sinistre est une option intéressante).

6. Pratiques en matière de formation, de processus et de documentation

De nombreux experts affirment que la plupart des violations de données sont dues à une erreur humaine. Ces dernières années, des études menées par Nuspire Networks, IBM, Verizon et The Ponemon Institute ont toutes conclu que la plus grande menace pour les données des concessionnaires pourrait être le personnel. Au-delà de la sécurité, les membres du personnel sont souvent à l'origine des pannes de réseau, des défaillances des appareils et du ralentissement des activités de l'entreprise. La plupart du temps, la cause première n'est pas le manque de compétences du personnel, mais plutôt la qualité inadéquate de la formation et de la documentation. Le personnel est souvent à l'origine d'un incident de sécurité, ne sait pas comment utiliser les systèmes ou provoque une panne de réseau parce qu'il n'a pas été formé à ce qu'il faut faire ou ne pas faire. Ce manque de formation du personnel peut souvent être lié à un manque de documentation.

La section suivante présente des conseils et des lignes directrices en matière de formation, tant du point de vue de la technologie que de la sécurité des données. Les concessions sont encouragées à adopter des politiques et des procédures de formation. Ces politiques doivent être bien documentées et utilisées dans le cadre de la formation du personnel. La documentation, les

procédures et les processus peuvent à eux seuls avoir une incidence positive sur les opérations du réseau et la sécurité des données des concessionnaires.

6.1 Formation du personnel

Recommandation	Caractéristiques
Formation sur la sécurité	Ayez un programme de formation à la sécurité officiel et écrit pour chaque membre du personnel. La formation doit couvrir des aspects comme la sensibilisation à la fraude psychologique, la gestion des mots de passe, les politiques de partage des données et les procédures de traitement des données sensibles. Révisez régulièrement les programmes de formation et adaptez-les aux nouvelles technologies, à l'évolution des activités des concessionnaires et à la rétroaction du personnel.
Responsabilité en matière de sécurité	Désignez un membre du personnel comme coordonnateur ou coordonnatrice de votre programme de sécurité de l'information.
Formation aux systèmes informatiques des concessionnaires	Offrez une formation officielle pour les applications critiques, le matériel et les autres systèmes informatiques des concessionnaires. Une personne bien informée peut accroître la productivité, réduire les coûts de soutien et améliorer la satisfaction de la clientèle.

6.2 Processus

Recommandation	Caractéristiques
Accès pour les nouveaux membres du personnel	Instaurez une procédure écrite et officielle pour accorder aux nouveaux membres du personnel l'accès aux systèmes. Celle-ci doit comprendre des noms d'utilisateur et des mots de passe uniques.
Accès pour les membres du personnel ayant quitté l'entreprise	Mettez en place une procédure écrite et officielle pour supprimer les membres du personnel du réseau informatique du concessionnaire, récupérer le matériel appartenant à la concession et désactiver tous les comptes des membres du personnel avant leur départ.
Formation aux systèmes informatiques	Mettez en place un programme officiel de formation aux technologies, aux applications et au matériel des concessions. Un personnel bien informé peut accroître la productivité, réduire les coûts de soutien et améliorer la satisfaction de la clientèle.
Évaluation des risques	Identifiez les risques internes et externes qui pourraient vraisemblablement menacer la sécurité, la confidentialité et l'intégrité des informations relatives aux clients. Concevez et mettez en œuvre des mesures de protection des clients afin de contrôler les risques identifiés au moyen de l'évaluation des risques.
Contrôles de sécurité des tiers (fournisseurs)	Il est très important de sélectionner des fournisseurs de services dignes de confiance. Choisissez des fournisseurs de services expérimentés en matière de protection des informations relatives aux clients d'un concessionnaire.
Traitement et intervention en cas d'incident de sécurité	Mettez en place une procédure officielle pour répondre aux incidents de sécurité sur le réseau. Couvrez les aspects liés à l'identification des failles de sécurité, à l'intervention, à la communication et à la documentation.

6.3 Documentation

Recommandation	Caractéristiques
Documentation sur la sécurité	Créez une politique de sécurité écrite qui aborde les normes administratives, techniques et de processus relatifs à la sécurité des données des clients. La documentation doit comprendre les éléments suivants : • La formation du personnel; • L'intervention et la gestion en cas d'incident ou de violation; • Les ententes relatives à l'utilisation d'Internet par le personnel; • Les politiques et les procédures liées à la surveillance et à la gestion du réseau.
Documentation pour les nouveaux membres du personnel	Ayez un programme écrit pour les nouveaux membres du personnel. Ce programme doit comprendre une formation sur la sécurité et sur les systèmes, ainsi qu'une procédure documentée pour la demande de soutien technique en TI.
Documentation des systèmes	Offrez une formation sur les applications essentielles, le matériel et les autres systèmes de TI des concessionnaires. Une personne bien informée peut accroître la productivité, réduire les coûts de soutien et améliorer la satisfaction de la clientèle.

7. Annexes

7.1 Guide sur la politique de sécurité des concessionnaires

Le cadre des politiques de sécurité de la concession doit être complet, cohérent et approuvé par l'organe de gestion du concessionnaire. Il est important de s'assurer que toutes les parties prenantes adhèrent aux politiques et acceptent de les mettre en œuvre dans tous les aspects pertinents de la concession.

Les politiques doivent refléter la stratégie de sécurisation de l'information, et non l'inverse. La compréhension des exigences en matière de sécurité constitue le facteur clé à cet égard. L'accent doit être mis sur la confidentialité, l'intégrité et la disponibilité des données sensibles et des ressources, y compris l'environnement physique, l'infrastructure du réseau, les applications et les données (physiques et numériques). Cette liste n'est toutefois pas exhaustive, car il existe de nombreux autres éléments à prendre en considération. Par exemple, la non-répudiation, la traçabilité ou l'authenticité doivent souvent être prises en compte.

Par ailleurs, chaque secteur d'activité a ses propres zones sensibles. Par exemple, nous nous soucions beaucoup plus de l'intégrité – plutôt que de la confidentialité – d'un avion en vol ou d'une voiture sur l'autoroute que de la confidentialité des antécédents médicaux d'un patient (qui peut également dépendre du contexte). Les politiques de sécurité doivent tenir compte de ces considérations.

Il existe de nombreuses politiques ou directives-cadres prêtes à l'emploi en matière de sécurité, qu'il est possible de choisir et d'appliquer dans une entreprise. Cependant, même si ce type de cadre peut fournir une base générale, une entreprise doit adapter et développer ses politiques pour les appliquer dans le contexte de ses activités.

Lignes directrices générales

- Veillez à ce que la direction comprenne bien les éléments qui doivent être protégés et le niveau d'ambition escompté en matière de protection des données. D'une part, il est important que les politiques assurent le niveau de protection attendu. D'autre part, il est particulièrement important que les politiques ne soient pas restrictives au point d'empêcher l'entreprise d'exercer les activités dont elle a besoin.
- Veillez à ce que les politiques soient alignées sur les lois et les règlements (p. ex. dans le domaine de la protection des données personnelles ou des règlements propres au secteur d'activité).
- Mettez en place des politiques qui reflètent les pratiques réelles et réalisables en matière de sécurité. Il est préférable de disposer d'un petit ensemble de règles plutôt que d'un document exhaustif difficile à suivre. Si la situation réelle est loin d'être à la hauteur des ambitions, il convient d'élaborer un plan de transition approuvé par toutes les parties prenantes afin de faire évoluer l'organisation depuis sa situation actuelle jusqu'à la situation souhaitée. Il est particulièrement important d'élaborer un plan de communication efficace dans le cadre du programme de sécurité global.
- Les politiques ne doivent pas faire l'objet de modifications trop fréquentes (y compris la manière dont elles sont exprimées et la langue dans laquelle elles sont formulées). Toutefois, si nécessaire, des modifications appropriées doivent être apportées, car les politiques doivent toujours refléter les exigences en matière de sécurité et les stratégies de sécurité de l'information en vigueur.
- Les politiques doivent être exprimées de manière à ne laisser aucune place aux exceptions. Cet aspect est lié à la fois à la langue et à l'engagement de toutes les parties prenantes à respecter les politiques. Dans le cas contraire, en particulier lorsque de nombreuses exceptions sont autorisées, l'engagement réel de la direction à l'égard de la politique ou le fait que la politique reflète véritablement la stratégie de l'entreprise en matière de protection de l'information peuvent être remis en cause.
- Les politiques doivent être exprimées de manière à ne laisser aucune place à l'interprétation. De plus, les politiques doivent être accompagnées de lignes directrices, de processus, de procédures, de rôles et de responsabilités, ainsi que d'interprétations, afin que l'on sache clairement ce qu'il convient de faire dans des cas précis. Il faut également savoir à qui s'adresser si une interprétation ou une décision est nécessaire. La mise à jour des articles de la base de connaissances est également une bonne pratique.
- Veillez à ce que des solutions et des technologies appropriées soient accessibles pour répondre aux attentes des politiques. Par exemple, lorsqu'une politique exige une authentification à deux facteurs dans des circonstances particulières, il est important que l'environnement informatique existant permette la mise en œuvre de ce niveau de protection supplémentaire.
- Mettez en place un tableau de bord pour suivre le niveau de mise en œuvre des politiques, ce qui permettra une gestion fiable des risques ainsi qu'une hiérarchisation des efforts.

Des lignes directrices et des exemples de politiques jugées particulièrement valables du point de vue des concessions sont présentés ci-dessous.

7.1.1 Politique d'utilisation acceptable

Elle décrit l'utilisation acceptable des ressources physiques et numériques d'une entreprise. Elle couvre également la propriété et le contrôle. Elle met l'accent sur des exemples d'activités interdites.

7.1.2 Politique de gestion des actifs

Les actifs représentent tous les éléments qui ont une valeur pour une organisation. Les actifs d'une entreprise sont considérés comme des aspects à la fois physiques et logiques.

Aspects physiques. Les serveurs, disques durs, routeurs, téléphones mobiles et les supports amovibles, comme les DVD ou les clés USB, par exemple. Il est important de suivre le cycle de vie des actifs, en accordant une attention particulière à leur cession et à leur réutilisation.

Aspects logiques. Il est important qu'une entreprise élabore des normes régissant la collecte, la conservation et l'utilisation appropriées des données. Ces normes doivent tenir compte de la nature des informations recueillies, de leur durée de conservation, de la manière dont elles sont stockées, des personnes qui peuvent y avoir accès et de la manière dont l'accès est assuré. Ces mesures sont étroitement liées au rôle accru de la réglementation en matière de protection de la vie privée dans différents pays.

Par ailleurs, il convient d'élaborer une politique de classification de l'information qui précise clairement les exigences en matière de propriété et de protection de l'information à différents niveaux. Cette politique est si importante qu'elle fait parfois l'objet d'une politique distincte et identifiable.

7.1.3 Politique sur les applications d'entreprise

Mettez en place une politique de classification des applications d'entreprise. Décrivez les exigences en matière de protection liée aux applications pour différents niveaux de criticité (p. ex. emplacement des zones de sécurité, méthodes de connectivité, contrôle de l'identité et de l'accès, application de la défense en profondeur, de la sécurité en cas d'échec, du droit d'accès minimal et d'autres principes semblables). Incluez les attentes concernant l'architecture de l'application, la communication avec d'autres systèmes et le tri des données entre les clients. Déterminez les attentes à l'égard des solutions basées sur l'informatique en nuage (qui deviennent de plus en plus répandues).

Les autres aspects à préciser incluent la manière dont une application est acquise par l'entreprise, les étapes obligatoires, les exigences communes à l'égard des fournisseurs, tant fonctionnelles que non fonctionnelles (p. ex. les ENS, la sécurité, la gestion de l'identité, les intégrations). Définissez les audits attendus de l'application acquise (p. ex. rapports de test d'intrusion ou d'analyse de vulnérabilité). Appuyez les politiques sur des modèles et des lignes directrices à partager avec les fournisseurs.

7.1.4 Politique sur les communications électroniques

À l'ère technologique actuelle, les entreprises disposent de nombreuses possibilités de communication et d'échange d'informations. Toutefois, ces possibilités comportent des risques. Par exemple, on peut utiliser un service infonuagique pour communiquer, mais celui-ci peut néanmoins recueillir des données à des fins malveillantes. Il est important de réglementer les communications électroniques, telles que les courriels et les messageries instantanées, l'utilisation de tableaux comme Trello, l'échange de fichiers au moyen de Dropbox et d'autres solutions et plateformes semblables.

7.1.5 Politique de gestion des identités et des accès

Il s'agit de l'un des domaines les plus critiques. Vous trouverez de plus amples renseignements à ce sujet à la section pertinente des présentes lignes directrices. La politique relative aux mots de passe doit être incluse dans cette section.

7.1.6 Politique de gestion des incidents de sécurité

Aucun environnement informatique ne peut être sécurisé à 100 %. Une entreprise doit être prête à faire face à un incident de sécurité. La politique de gestion des incidents de sécurité doit faire partie de la gestion globale des incidents ou y contribuer. Fournissez la définition d'un incident de sécurité, présentez les processus et les procédures (c.-à-d. le

plan d'intervention) pour savoir ce qu'il faut faire en cas d'incident de sécurité (en fonction de la catégorie d'incident, par exemple piratage informatique, comportement répréhensible, défaillance de l'équipement) et la criticité.
Définissez les procédures exactes de réaction et d'action. Par exemple :

- Si un ordinateur est compromis, déconnectez-le immédiatement du réseau;
- Si une personne entre sans carte d'accès, demandez-lui une pièce d'identité;
- Envisagez une enquête judiciaire plus approfondie;
- Considérez la mise en place de correctifs d'urgence pour soutenir les plans de continuité des services et des activités;
- Identifiez les personnes à prévenir en cas d'incident, tant à l'intérieur qu'à l'extérieur de l'organisation. Les parties suivantes peuvent devoir être informées : les consommateurs, les forces de l'ordre, les clients, les agences d'évaluation du crédit et les autres entreprises susceptibles d'être affectées par la violation;
- Très souvent, il existe également des lois et des règlements qui dépendent du pays, de l'État et du secteur d'activité et qui exigent un comportement particulier en cas d'atteinte à la protection des données.

On peut également s'attendre à ce que la politique introduise des solutions techniques appropriées pour soutenir sa mise en œuvre.

De plus amples renseignements sur les interventions en cas d'incident sont accessibles à l'adresse suivante (en anglais) : https://www.sans.org/reading- room/whitepapers/incident.

Des exemples de formulaires de traitement des incidents et de documentation sont disponibles à l'adresse suivante (en anglais) : https://www.sans.org/score/incident-forms.

7.1.7 Politique de réseau

La politique de réseau est un autre aspect très important de la sécurité globale. Lors de l'élaboration d'une politique de réseau, il est recommandé de tenir compte des aspects suivants :

- Des classes de zones de réseau définies avec l'organisation correspondante (propriétaire de la zone, opérateur de la zone, etc.), un niveau de confiance attribué à chaque classe, des connexions autorisées définies entre les différents niveaux de confiance. Introduire des segments de réseau plus restreints pour les applications et les données plus sensibles;
- Une liste des appareils du réseau et des configurations associées, et une indication de ce qui doit être autorisé à se connecter et à quel endroit;
- Des connexions réseau externes et des réseaux privés virtuels (pour le personnel et les partenaires externes);
- Un système de noms de domaine (DNS), y compris la structure de dénomination, ainsi que l'infrastructure et le champ d'application correspondants;
- Des pare-feu, des serveurs mandataires d'entrées et des configurations de serveurs mandataires (p. ex. tout le trafic sortant doit passer par un serveur mandataire, tout le trafic entrant sensible doit passer par le serveur mandataire d'entrées);
- Des classes et des normes sans fil sur l'authentification et la protection en transit. Des segments distincts, précis et très limités pour les clients;
- La maintenance à distance;

- La voix par protocole Internet (VoIP), la téléphonie et la téléconférence.

7.1.8 Gestion des risques et politique de vérification

Définissez le cadre de risque et les considérations en matière d'audit qui s'y rapportent. Décrivez les exigences en matière d'évaluation des risques et d'audit portant sur les renseignements et les ressources de l'entreprise.

7.1.9 Politique de gestion des menaces et des vulnérabilités

Une évaluation ou une analyse des vulnérabilités permet d'identifier les faiblesses en matière de sécurité au sein de vos systèmes de réseau, de vos ordinateurs et, le cas échéant, de vos applications. Elle est réalisée à l'aide d'outils qui analysent automatiquement votre environnement informatique, vos applications et vos composants réseau à la recherche des vulnérabilités actuellement connues, dans le but d'exposer celles qui sont détectées. Ces analyses sont également effectuées à l'aide des informations d'identification administratives nécessaires pour effectuer les diagnostics sécurisés au sein des systèmes auxquels seul un administrateur peut accéder.

Le résultat fournit un niveau de gravité et propose une action corrective recommandée pour chaque problème détecté. Ces analyses doivent être effectuées sur une base régulière, au minimum chaque année, mais il est recommandé de le faire au moins deux fois par an, voire plus.

Un test d'intrusion est une méthode permettant de simuler une attaque réelle et d'évaluer ainsi la sécurité d'un système informatique et d'un environnement réseau. Il est réalisé sans accès administratif, comme pour imiter un utilisateur hostile non autorisé. Il se distingue d'une analyse de vulnérabilité par le fait qu'il tente de trouver une vulnérabilité réelle et d'exploiter cette vulnérabilité si celle-ci existe. Le test d'intrusion tente de reproduire les méthodes malveillantes de violation de ces systèmes afin de montrer comment la menace peut perturber, arrêter, surpasser ou voler ces systèmes, mais il le fera d'une manière qui prouve seulement qu'il peut effectuer ces actions sans réellement endommager les systèmes ciblés. Les systèmes internes accessibles depuis l'Internet doivent être évalués à partir d'un point d'accès externe (basé sur l'Internet), à partir d'un système émulant une entité hostile qui attaque à distance, depuis l'extérieur du réseau de l'entreprise, comme dans le cas d'une tentative de piratage lancée à partir d'un pays étranger. Les tests d'intrusion peuvent utiliser certains outils automatisés, mais ils sont orchestrés par un professionnel compétent qui sait utiliser ces outils et ces tactiques. Les attaques par fraude psychologique sont également incluses dans ce test afin de déterminer si les erreurs humaines peuvent exposer une faiblesse et fournir un vecteur d'attaque efficace, permettant d'accéder à des systèmes et à des données qui n'auraient pas dû être fournis ou exposés. De plus, il est toujours recommandé d'effectuer le test d'intrusion physique (attaque, évaluation) depuis l'intérieur du réseau, comme si la menace ou l'attaque avait été lancée depuis l'environnement de l'organisation (et comme si l'attaque avait réussi à contourner ou à déjouer le périmètre de protection).

De manière objective, l'analyse de la vulnérabilité et le test d'intrusion devraient tous deux être effectués régulièrement. Le cycle doit consister à effectuer une analyse des vulnérabilités afin de les identifier et d'y remédier. L'objectif est de déjouer idéalement l'action du test d'intrusion ultérieur qui tente de contourner la sécurité en exploitant les vulnérabilités qui peuvent exister ou persister.

Notez qu'une protection de grande qualité des points d'extrémité installée sur tous les ordinateurs de bureau, les portables, les serveurs et les tablettes constitue une meilleure pratique prescriptive pour réduire la vulnérabilité, fournir une protection contre les menaces et les prévenir, et surveiller en permanence les notifications. La meilleure solution et la plus efficace est une protection des points d'extrémité qui permet une communication instantanée avec un centre d'opérations de sécurité (SOC) pour un examen immédiat par des professionnels de la sécurité.

Pour obtenir divers modèles de politique de sécurité, veuillez consulter le site suivant (en anglais) : https://www.sans.org/information-security-policy.

7.2 Guide de gestion des identités et des accès

Couvrez entièrement la gestion des identités et des accès. Commencez par présenter les concepts de base, suivis des sous-sections suivantes : la gestion de l'identité, l'authentification, les autorisations et leur importance, les processus de gestion des accès, les utilisateurs finaux et les considérations physiques, et les niveaux de protection. Terminez par une introduction aux trois niveaux de maturité.

7.2.1 Introduction

Gartner Inc. définit la gestion des identités et des accès (IAM) comme une discipline de sécurité qui permet :

- de donner accès aux bonnes personnes,
- aux bonnes ressources,
- aux bons moments,
- et pour les bonnes raisons.

Même si la définition est assez simple, elle capture l'essence du concept et implique de nombreuses considérations dans différents domaines.

7.2.2 Concepts de base et définitions

Pour établir une base de référence, définissez les conditions essentielles liées à la gestion des identités et des accès.

- **Entité** : personne réelle ou système d'information.
- **Identité** : entité dans un contexte particulier (p. ex. au travail ou dans les médias sociaux).
- **Identifiant** : ensemble d'attributs permettant d'identifier l'identité (p. ex. numéro de sécurité sociale, adresse électronique, empreinte digitale).
- **Authentification** : processus de confirmation de l'identité revendiquée par une entité (p. ex. en fournissant un mot de passe).
- **Autorisations** : ensemble des autorisations attribuées à quelqu'un ou à quelque chose (p. ex. autorisation à consulter le dossier médical d'un patient).
- **Comptabilité et audit** : historique des événements.

Les points susmentionnés doivent être considérés à la fois sous leurs aspects physiques et logiques; les aspects physiques se rapportent à la limitation de l'accès aux bâtiments, aux locaux et aux autres biens informatiques physiques, et les aspects logiques renvoient à la limitation de l'accès au monde informatique virtuel, comme les connexions aux réseaux informatiques, aux systèmes d'information, aux fichiers ou aux données. Une fois ces éléments mis en œuvre, introduisez la pièce maîtresse de ce casse-tête.

- **Contrôle d'accès** : vérification de la conformité aux règles d'autorisation. On peut considérer qu'il s'agit de la mise en œuvre de l'authentification, de l'autorisation et de la comptabilité dans les dimensions physiques et logiques.

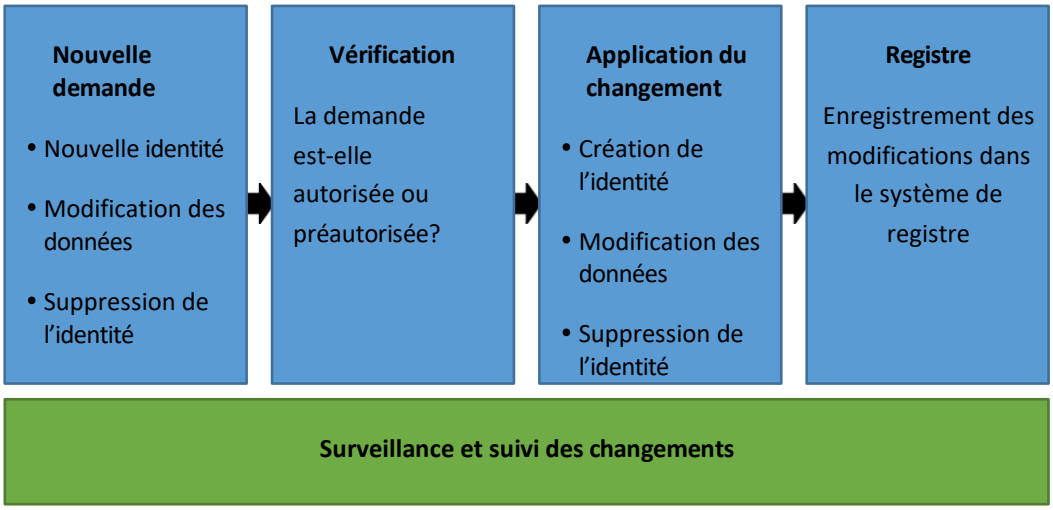
7.2.3 Gestion de l'identité

Les aspects suivants de la gestion de l'identité doivent être soigneusement examinés :

- Cycle de vie des identités;
- Gestion et stockage des identités;
- Gestion des mots de passe;
- Fédération des identités.

Cycle de vie des identités

Le cycle de vie doit être pris en compte du début de la relation jusqu'à la fin de celle-ci et doit être surveillé au fil du temps pour détecter les changements de contexte (p. ex. un membre du personnel qui change d'affectation). Le processus peut être illustré comme suit :



Mettez l'accent sur les principaux aspects suivants :

- Limitez le nombre d'identités liées à une entité spécifique et centralisez leur gestion (p. ex. essayez d'éviter les situations où il existe des comptes propres à une application);
- Essayez d'éviter les comptes de groupe. Si vous en avez absolument besoin, veillez à ce que chacun d'entre eux ait son propre gardien responsable;
- N'oubliez pas que les identités sont liées non seulement aux utilisateurs finaux, mais aussi aux services ou aux réseaux, et que ces types d'identités doivent également être gérés et maintenus avec soin. Veillez à ce que chaque identité non personnelle ait son propre gardien responsable;
- Veillez à ce que le stockage des identités soit protégé, en particulier lorsque des renseignements confidentiels y sont stockés. Les mots de passe sont généralement cités en exemple, mais il peut également s'agir d'informations sensibles sur l'utilisateur (p. ex. les coordonnées GPS des lieux visités).

Il est recommandé de suivre les normes communes du marché et les protocoles de sécurité, ainsi que les produits.

Gestion des mots de passe

Les mots de passe doivent être sécurisés à la fois lors de leur transmission et lorsqu'ils sont stockés. De plus, les procédures relatives aux mots de passe doivent être conçues avec soin. Le stockage des mots de passe peut être envisagé sous deux angles.

- **Du côté du serveur :** endroit où l'identité est gérée (p. ex. Active Directory, applications d'entreprise, etc.).
    - Principaux aspects :
        - Le mot de passe ne doit pas être stocké en texte clair et, s'il est chiffré de manière réversible, la clé de déchiffrement doit être protégée de manière appropriée;

- Tous les mots de passe par défaut fournis par le fournisseur doivent être modifiés avant la mise en service de tout système d'information.

- **Du côté du client :** endroit où un mot de passe est utilisé pour accéder aux ressources. S'il est nécessaire de stocker un mot de passe, il est fortement recommandé de le stocker sous une forme chiffrée (p. ex. dans une application KeyPass ou un fichier Excel chiffré). Ensuite, il est important de protéger le mot de passe principal de manière sécurisée. Il est particulièrement important de déconseiller aux membres du personnel de noter leurs mots de passe et de les laisser à la vue des autres (p. ex. sur un Post-it à proximité du lieu de travail).

    - Ne pas divulguer le mot de passe à quiconque, à moins que cela ne soit absolument nécessaire (p. ex. soutien technique), et de ne pas oublier de modifier le mot de passe après la divulgation.

  Tous les mots de passe doivent être rapidement modifiés si l'on soupçonne qu'ils ont été compromis ou divulgués à des fournisseurs pour la maintenance ou le soutien.

  Il est également important de s'assurer que toutes les copies de sauvegarde dans lesquelles les mots de passe sont stockés sont également sécurisées avec soin. Procédures courantes nécessitant d'être conçues de manière sécuritaire :

    - Envoi du mot de passe initial de manière sécuritaire;
    - Récupération du mot de passe en cas d'oubli;
    - Déverrouillage du mot de passe en cas de verrouillage;
    - Changement de mot de passe en libre-service;
    - Politiques relatives au cycle de vie des mots de passe (voir la section sur les politiques relatives aux mots de passe). Rappelez-vous que des politiques trop restrictives peuvent aussi avoir des conséquences négatives.

Fédération d'identité et authentification unique

Lorsqu'une entreprise est établie avec d'autres partenaires au niveau des systèmes informatiques, il convient d'examiner la politique de fédération d'identité. En bref, il s'agit de partager la même identité entre les entreprises sur la base d'un certain niveau de confiance. Il existe un ensemble de technologies éprouvées qui soutiennent cette approche. Voici les avantages immédiats :

- Authentification unique : l'utilisateur final doit s'authentifier une fois et peut accéder à un certain nombre d'applications (sans avoir besoin de s'authentifier à nouveau);
- Réduction des coûts liés à la gestion du cycle de vie de l'identité;
- Diminution des risques liés à la nécessité de conserver des identités distinctes pour l'utilisateur final.

Ultimement, il faut calculer si l'investissement dans la fédération d'identité est justifié dans un contexte précis.

7.2.4 Authentification

La preuve la plus courante en matière d'authentification est le mot de passe, mais un problème se pose : les mots de passe sont difficiles à retenir. C'est pourquoi il est de plus en plus courant d'utiliser des phrases de passe. Il faut se rappeler que la recommandation de phrases de passe nécessite des changements dans les politiques ainsi que dans les systèmes informatiques pour soutenir les nouvelles politiques.

Il existe d'autres options d'authentification que le mot de passe, comme la biométrie, les mots de passe à usage unique, les cartes à puce prises en charge par jeton RSA, les applications mobiles comme Google Authenticator ou Yubikey. Chaque méthode est généralement classée dans l'une des trois catégories suivantes :

- Ce que vous connaissez (mots de passe, motifs visuels);
- Ce que vous possédez (carte à puce, jeton RSA, téléphone intelligent);
- Ce que vous êtes (biométrie, comportement).

Il existe deux raisons d'appliquer des méthodes d'authentification différentes :

- Meilleure expérience utilisateur (p. ex. biométrie);
- Meilleure sécurité (carte à puce).

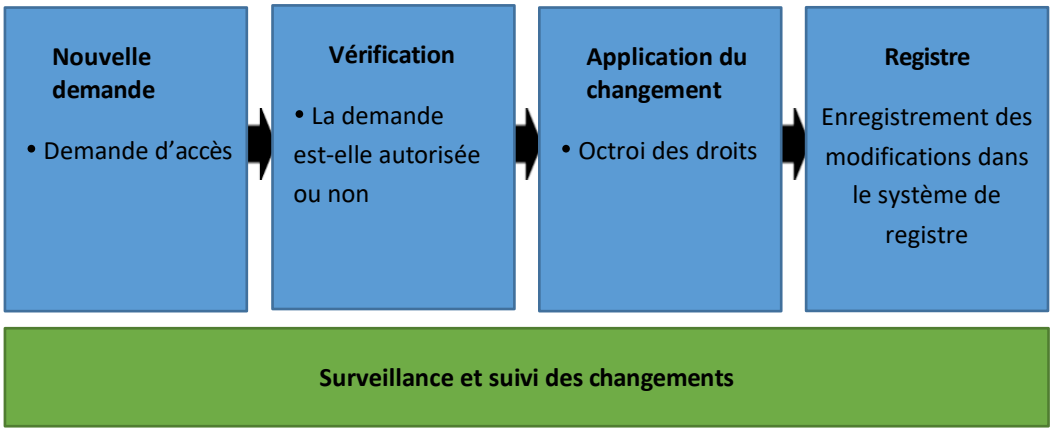
Lorsque deux méthodes ou plus appartenant à des catégories différentes sont combinées, on parle d'***authentification multifactorielle***, qui vise à accroître le niveau de sécurité.

7.2.5 Processus de gestion des autorisations et des accès

Les autorisations correctes (c.-à-d. la définition des permissions et leur représentation dans les systèmes informatiques) sont l'un des éléments les plus importants du paysage global de la sécurité informatique. Les aspects suivants doivent être correctement sécurisés :

- Définissez une structure de rôles et de niveaux d'accès;
- Définissez un ensemble de permissions pour un rôle donné;
- Veillez à ce que les autorisations soient documentées et facilement accessibles;
- Veillez à ce que les autorisations soient mises en œuvre dans les systèmes de contrôle d'accès;
- Veillez à ce que les demandes d'accès soient approuvées par les personnes qualifiées et que les responsables de l'approbation soient clairement identifiés;
- Surveillez et examinez (audits) les droits d'accès et les autorisations.

Par ailleurs, le ***processus de gestion des accès*** doit être établi et mis en œuvre pour faire en sorte que les autorisations définies soient appliquées partout et à tout moment. Le processus est semblable à celui de la gestion du cycle de vie des identités et peut être illustré comme suit :



Voici les éléments principaux à prendre en compte dans le cadre d'un tel processus :

- L'accès est révoqué ou modifié chaque fois qu'un membre du personnel quitte l'entreprise ou change de poste;
- L'accès doit être mis à jour en temps opportun, en fonction des besoins de l'entreprise;
- L'accès doit être revu périodiquement selon une fréquence documentée (trimestrielle, semestrielle, annuelle). Cette évaluation, qui n'est pas motivée par le départ ou la transition d'une personne, vise à déterminer si le niveau d'accès actuellement accordé correspond à la position de cette personne au sein de l'entreprise. Veuillez noter que la fréquence des examens peut varier en fonction de la criticité des actifs protégés;
- Le principe du « besoin de connaître », c'est-à-dire que l'accès aux ressources ne doit être accordé que s'il existe un besoin opérationnel, constitue également une bonne pratique.

Une fois encore, on ne saurait trop insister sur l'importance du contrôle et de l'audit des autorisations et des droits d'accès, en particulier pour s'assurer que le retrait des accès est correctement mis en œuvre. Malheureusement, il est fréquent que des droits d'accès soient accordés et qu'ils ne soient jamais retirés.

7.2.6 Utilisateurs finaux et considérations physiques

Il est de notoriété publique que la plupart des problèmes de sécurité sont souvent dus à un comportement incorrect de la part de certains utilisateurs (les problèmes de sécurité liés aux dimensions logiques, comme le fait de cliquer sur des courriels dangereux, sont abordés dans d'autres sections). Les éléments relatifs au contrôle d'accès physique sont présentés ci-dessous et doivent également constituer la base d'une stratégie de formation appropriée.

- Les salles de serveurs et d'équipement doivent être verrouillées. L'accès du personnel doit être limité aux membres qui ont un besoin opérationnel légitime. Il faut prévoir des mécanismes permettant de savoir si une personne accède au site et à quel moment.
- Exigez que les dossiers contenant des données et des informations sensibles soient conservés à tout moment dans des armoires fermées à clé, sauf lorsqu'une personne travaille sur ceux-ci. De plus, lorsqu'un membre du personnel travaille sur le dossier, veillez à ce que les personnes non autorisées ne puissent pas voir le dossier (p. ex. lors d'un voyage en avion).
- Rappelez au personnel de ne pas laisser de documents ou d'informations sensibles sur les bureaux lorsqu'une personne n'est pas à son poste de travail.
- Demandez aux membres du personnel de ranger leurs dossiers, de fermer leur ordinateur et de verrouiller les classeurs et les portes de leur bureau à la fin de la journée.
- Mettez en place des contrôles d'accès appropriés pour votre bâtiment. Indiquez au personnel ce qu'il doit faire et qui prévenir si une personne inconnue est aperçue dans les locaux de l'entreprise.
- Si des installations d'entreposage hors site sont maintenues, il faut limiter l'accès du personnel aux membres dont le besoin opérationnel est légitime. Il faut prévoir des mécanismes permettant de savoir si une personne accède au site et à quel moment.
- Si des appareils recueillant des informations sensibles sont utilisés, tels que des claviers d'identification personnelle, il convient de sécuriser l'équipement afin de réduire le risque d'altération. Ces équipements doivent également être sécurisés afin de réduire le risque qu'un attaquant ne remplace l'équipement par un dispositif fictif.

7.2.7 Niveaux de protection

Le contrôle d'accès (y compris la prise en compte de l'identité) doit être envisagé à différents niveaux.

- **Applications d'entreprise** : applications nécessaires à la gestion des commandes, à la planification du travail, à l'organisation des ressources humaines et des finances, etc. L'accent est mis sur la protection des informations et des fonctionnalités sensibles de l'entreprise. Les identités concernent généralement les utilisateurs finaux.
- **Systèmes d'exploitation** : fondement de l'exécution des applications sur les ordinateurs portables, les ordinateurs de bureau, les serveurs, les téléphones, les tablettes, etc. L'accent est mis sur la protection des fichiers et des données, sur la lutte contre les logiciels malveillants et sur les possibilités offertes par le contrôle d'accès. Les identités concernent généralement les utilisateurs finaux (ordinateurs portables, téléphones, etc.) et les services (serveurs).
- **Appareils d'infrastructure et services de soutien** : routeurs, commutateurs, points d'accès, services d'authentification, etc. L'accent est mis sur la protection d'un trafic adéquat sur le réseau, la sécurisation de la communication et le maintien à l'écart des intrus. Les identités concernent généralement les utilisateurs et les services techniques.
- **Appareils mobiles** : appareils tels que les téléphones, les tablettes et même les ordinateurs portables. L'accent est mis sur la protection des données stockées sur les appareils et sur un accès sécurisé, notamment en cas d'utilisation hors ligne ou de vol des appareils.
- **Lieux et emplacements physiques** : bâtiments, salles de serveurs, salles d'impression, bureaux, ateliers, salles d'exposition, etc. Il s'agit de s'assurer que les personnes peuvent entrer aux bons endroits et avoir accès aux bons équipements.

De plus, il est possible de faire correspondre les éléments ci-dessus aux différentes couches du réseau :

- Couche application (p. ex. HTTP)
- Couche transport (p. ex. TCP)
- Couche Internet (p. ex. IP)
- Couche réseau (p. ex. Ethernet)

Il est important de s'assurer que la gestion des identités et des accès est entièrement couverte par les différentes couches et les différents domaines, conformément aux exigences qui doivent être basées sur la criticité des informations.

- Mettez en œuvre une protection complète sur toutes les couches et pour tous les types d'applications et d'appareils, tant sur les aspects physiques que logiques.

7.3 Directives sur la maturité du niveau de sécurité des concessions

Les concessions ont souvent du mal à mettre en œuvre les recommandations en matière de sécurité. Cette situation est souvent attribuée au niveau de maturité de la concession en matière de complexité des technologies de l'information et de la sécurité. Utilisez le présent guide pour vous aider à identifier le niveau de maturité de votre concession et les prochaines étapes à suivre pour améliorer sa posture de sécurité.

7.3.1 Conseils aux concessionnaires sur les politiques de sécurité

Pour déterminer les prochaines étapes du développement des politiques de sécurité d'une concession, il faut d'abord identifier son niveau de maturité actuel. Déterminez ensuite les mesures qui peuvent être prises pour améliorer la position de la concession en matière de sécurité. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base :** les concessions ont identifié et documenté des politiques concernant l'utilisation acceptable, l'audit, la gestion des accès (y compris les mots de passe) et la prise en compte du réseau de base (y compris l'accès externe et les normes sans fil).
- **Niveau de maturité intermédiaire :** les concessions ont défini et documenté des politiques pour tous les domaines concernés. Par ailleurs, il faut mettre en place des processus pour fournir au personnel de la concession des politiques de sécurité documentées, pour le sensibiliser à ces politiques et pour l'aider à les mettre en œuvre.
- **Niveau de maturité avancé :** les concessions contrôlent, vérifient et peaufinent régulièrement les politiques et les procédures de sécurité.

7.3.2 Conseils aux concessionnaires sur la gestion des identités et des accès (IAM)

Pour déterminer les prochaines étapes du développement de la gestion des identités et des accès d'une concession, il faut d'abord identifier son niveau de maturité actuel. Déterminez ensuite les mesures qui peuvent être prises pour améliorer la position de la concession en matière de sécurité. Utilisez le guide ci-dessous pour vous aider.

Niveau de maturité de base

- Processus explicites de gestion du cycle de vie des identités et des droits d'accès;
- Audits et examens réguliers des autorisations pour les systèmes essentiels;
- Processus explicites de gestion des mots de passe;
- Formation de base pour le personnel (du moins pour les personnes nouvellement embauchées);
- Système de contrôle d'accès aux locaux physiques essentiels.

Niveau de maturité intermédiaire

- Processus explicites de gestion du cycle de vie des identités et des droits d'accès;
- Audits et examens réguliers des autorisations pour les systèmes essentiels;
- Processus explicites pour la gestion des mots de passe et recommandations sur le stockage des mots de passe du côté du client;
- Formation régulière du personnel;
- Système de contrôle d'accès pour tous les lieux physique;
- Niveau de protection (p. ex. authentification multifactorielle, défense en profondeur) lié à la criticité des informations et des fonctions de l'entreprise.

Niveau de maturité avancé

- Processus automatisés de gestion du cycle de vie des identités et des droits d'accès;
- Stockage et gestion centralisés des identités, y compris le niveau adéquat de fédération des identités;
- Processus centralisés pour la gestion des mots de passe et l'authentification;
- Fortes recommandations (ou politiques) sur le stockage des mots de passe du côté du client;
- Niveau de protection (p. ex. authentification multifactorielle, défense en profondeur) lié à la criticité des informations et des fonctions de l'entreprise.
- Système de contrôle d'accès centralisé pour tous les lieux physiques;
- Formation régulière du personnel;
- Audits et examens réguliers des autorisations et des identités;
- Protection complète sur toutes les couches et pour tous les types d'applications et d'appareils, tant sur les aspects physiques que logiques.

7.3.3 Conseils aux concessionnaires sur la gestion des correctifs

Niveau de maturité de base : les concessions ont réglé chaque système de manière à ce qu'il soit automatiquement mis à jour pour les correctifs critiques ou de sécurité.

Niveau de maturité intermédiaire : les concessions disposent d'un système de gestion des correctifs à l'échelle de l'entreprise.

Niveau de maturité avancé : les concessionnaires testent, déploient et valident les correctifs dès qu'ils sont disponibles et le plus rapidement possible.

7.3.4 Conseils aux concessions en matière de reprise après sinistre

Pour déterminer les prochaines étapes du développement de la reprise après sinistre d'une concession, il faut d'abord identifier son niveau de maturité actuel. Déterminez ensuite les mesures qui peuvent être prises pour améliorer la position de la concession en matière de sécurité. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base :** les concessions effectuent régulièrement des copies de sauvegarde de tous les systèmes.
- **Niveau de maturité intermédiaire :** les concessions effectuent des sauvegardes incrémentielles régulières et stockent les images de sauvegarde hors site.
- **Niveau de maturité avancé :** les concessions déploient un système de continuité des activités qui comprend des sauvegardes complètes du système hors site dans un environnement virtuel qui permettra à la concession de lancer immédiatement l'image de sauvegarde en cas de panne ou de défaillance.

7.3.5 Conseils aux concessionnaires sur la formation relative à la sensibilisation à la sécurité

Pour déterminer les prochaines étapes du développement du programme de sensibilisation à la sécurité d'une concession, il faut d'abord identifier son niveau de maturité actuel. Déterminez ensuite les mesures qui peuvent être prises pour améliorer la position de la concession en matière de sécurité. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base :** tous les membres du personnel suivent une formation annuelle en matière de sécurité. L'achèvement de la formation est documenté et les rapports sont rendus accessibles à des fins d'audit. Il arrive que les membres du personnel ne sachent pas très bien quel est leur rôle vis-à-vis de la protection de l'organisation. L'organisation peut ne pas être sécuritaire malgré sa conformité. Il n'existe pas de procédure établie permettant au personnel de signaler un comportement suspect ou une perte accidentelle de données, ou alors, le personnel ne se sent pas en mesure de le faire.
- **Niveau de maturité intermédiaire :** le programme de formation peut se dérouler plus d'une fois par année et un suivi est effectué pour s'assurer que tout le personnel participe au programme conformément aux conditions d'emploi. Les sujets abordés portent sur les risques les plus importants pour l'organisation. Des documents de sensibilisation sont affichés dans les espaces consacrés aux pauses du personnel. Le personnel connaît les politiques de sécurité de l'entreprise et sait comment reconnaître et signaler un incident de sécurité.
- **Niveau de maturité avancé :** le programme de formation destiné à l'ensemble du personnel et des contractants comprend des modules courts, mais fréquents sur des sujets d'actualité en lien avec leur rôle. Le personnel est testé sur sa capacité à se défendre contre diverses tactiques de fraude psychologique, comme l'hameçonnage, les arnaques par clé USB, la fraude, etc. Le personnel sait comment signaler un incident de sécurité et, lors d'un test, au moins la moitié des membres rapporte un événement suspect. Moins de 10 % des personnes testées cliquent sur les courriels d'hameçonnage. La concession adopte une culture de la sécurité : les membres du personnel comprennent leur rôle dans la protection de l'organisation, recherchent des processus sécurisés et encouragent leurs collègues à mener leurs activités d'une manière qui favorise la sécurité et la protection de l'organisation contre la fraude, le vol et la perte accidentelle de données ou d'argent.

7.3.6 Conseils aux concessionnaires sur la conformité aux lois fédérales

Pour déterminer les prochaines étapes du développement de la mise en conformité d'une concession aux lois sur la sécurité, il faut d'abord identifier son niveau de maturité actuel. Déterminez ensuite les mesures qui peuvent être prises pour améliorer la position de la concession en matière de sécurité. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base :** les concessions ont effectué des recherches sur les normes PCI et sur la GLB Act afin de déterminer si elles sont conformes aux lois fédérales. Les concessionnaires disposent de politiques et de processus documentés pour respecter la conformité.
- **Niveau de maturité intermédiaire :** les concessions examinent et révisent régulièrement leur conformité aux lois fédérales en matière de sécurité.
- **Niveau de maturité avancé :** les concessionnaires effectuent des audits réguliers des systèmes et suivent les résultats en fonction des exigences législatives.

7.3.7 Conseils aux concessionnaires sur la sécurité du réseau

Pour déterminer les prochaines étapes du développement de la sécurité du réseau d'une concession, il faut d'abord identifier son niveau de maturité actuel. Déterminez ensuite les mesures qui peuvent être prises pour améliorer la position de la concession en matière de sécurité. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base :** les concessions ont élaboré et documenté une politique d'utilisation de l'Internet. Les concessions disposent d'une protection au niveau de la passerelle du réseau. Elles ont aussi configuré et segmenté le réseau afin d'éviter tout accès indésirable aux ressources du réseau. Le réseau est surveillé en temps réel par des technologies de gestion des événements d'information en matière de sécurité afin de le protéger contre tout accès indésirable. L'accès à distance est surveillé et limité sur le réseau.
- **Niveau de maturité intermédiaire :** les concessions ont utilisé des politiques et des processus documentés pour mettre en place un réseau de concessions sécurisé et segmenté. Les concessions testent régulièrement le réseau en fonction des risques connus. Le réseau est surveillé en tout temps par des experts en sécurité qui utilisent des technologies de gestion des événements d'information en matière de sécurité. L'accès à distance est contrôlé et limité au personnel et aux fournisseurs connus.
- **Niveau de maturité avancé :** les concessions ont utilisé des politiques et des processus documentés pour mettre en place un réseau de concessions sécurisé et segmenté. Les concessions testent régulièrement le réseau en fonction des risques connus. Le réseau est surveillé en tout temps par un fournisseur de services certifié SOC 2. Le réseau est surveillé en tout temps par des experts en sécurité. L'accès à distance est contrôlé et limité au personnel et aux fournisseurs connus. L'accès au RPV par le personnel est assuré par une authentification à deux facteurs.

7.3.8 Conseils sur l'antivirus des concessions

Pour déterminer les prochaines étapes du développement de la sécurité de l'antivirus d'une concession, il faut d'abord identifier son niveau de maturité actuel. Déterminez ensuite les mesures qui peuvent être prises pour améliorer la position de la concession en matière de sécurité. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base :** les concessions ont identifié tous les systèmes et installé un logiciel antivirus sur chaque système du réseau.
- **Niveau de maturité intermédiaire :** les concessions ont mis en place un système antivirus d'entreprise. Cette solution comprend la gestion des licences à l'échelle de l'entreprise, un portail d'entreprise pour la création de rapports et les interventions, ainsi que l'audit et la création de rapports sur l'ensemble du réseau.

- **Niveau de maturité avancé :** les concessionnaires réagissent de manière proactive et immédiate aux alertes générées par la solution antivirus de l'entreprise.

7.3.9 Conseils aux concessionnaires sur la sécurité des courriels

Pour déterminer les prochaines étapes du développement de la sécurité des courriels d'une concession, il faut d'abord identifier son niveau de maturité actuel. Déterminez ensuite les mesures qui peuvent être prises pour améliorer la position de la concession en matière de sécurité. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base :** les concessions ont pris des mesures pour mettre en œuvre des technologies visant à protéger les systèmes de messagerie électronique des concessionnaires.
- **Niveau de maturité intermédiaire :** les concessionnaires effectuent une inspection active de la sécurité des courriels entrants et sortants et assurent leur protection. Les concessionnaires chiffrent les données sensibles transmises par courrier électronique.
- **Niveau de maturité avancé :** les concessionnaires disposent d'un système de surveillance et de réponse actives aux menaces par courriel.

7.3.10 Conseils sur la gestion unifiée des menaces (UTM), les pare-feu et les systèmes de détection d'intrusion (SDI)

Pour déterminer les prochaines étapes du développement de la gestion unifiée des menaces, des pare-feu et des systèmes de détection d'intrusion d'une concession, il faut d'abord identifier le niveau de maturité actuel de celle-ci. Déterminez ensuite les mesures qui peuvent être prises pour améliorer la position de la concession en matière de sécurité. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base :** les concessionnaires déploient un système de gestion unifiée des menaces entièrement géré et sous licence, qui comprend des licences pour l'antivirus, la gestion des pourriels et les systèmes de détection et de prévention des intrusions. Les signatures sont automatiquement mises à jour en temps réel.
- **Niveau de maturité intermédiaire :** les concessions répondent aux alertes et aux événements de la gestion unifiée des menaces de manière continue et en temps réel. Les concessions utilisent un système de gestion des informations et des événements de sécurité (GIES) pour signaler les événements survenant au niveau de la passerelle du réseau et répondre à ces événements (voir la section 3.5).
- **Niveau de maturité avancé :** les concessions se tournent vers les fournisseurs de services de sécurité gérés (FSSG) pour une gestion, une surveillance et une intervention proactives du système de gestion unifiée des menaces en tout temps.

7.3.11 Conseils sur la gestion des informations et des événements de sécurité (GIES)

Pour déterminer les prochaines étapes du développement de la gestion des informations et des événements de sécurité d'une concession, il faut d'abord identifier son niveau de maturité actuel. Déterminez ensuite les mesures qui peuvent être prises pour améliorer la position de la concession en matière de sécurité. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base :** les concessions installent et utilisent un logiciel GIES. Toutes les alertes sont traitées en temps quasi réel, et ce, en tout temps. Tous les journaux du système sont conservés conformément aux lois fédérales (voir la section 2.6 sur le respect des lois fédérales).
- **Niveau de maturité intermédiaire :** les concessions font appel à un fournisseur de services de sécurité gérés pour une surveillance et une intervention avancées. Les concessions intègrent les renseignements sur les cybermenaces pour une surveillance et des alertes avancées.
- **Niveau de maturité avancé :** les concessions se tournent vers les fournisseurs de services de sécurité gérés

(FSSG) certifiés SOC 2 pour une gestion, une surveillance et une intervention proactives du système de gestion unifiée des menaces en tout temps. Les concessions intègrent les renseignements sur les menaces dans la solution de GIES. Les billets, les alertes et les activités sont régulièrement examinés par la direction de la concession et le FSSG afin de peaufiner, de documenter et d'améliorer la posture de sécurité.

7.3.12 Conseils aux concessionnaires sur la sécurité des applications

Pour déterminer les prochaines étapes du développement de la sécurité des applications d'une concession, il faut d'abord identifier son niveau de maturité actuel. Déterminez ensuite les mesures qui peuvent être prises pour améliorer la position de la concession en matière de sécurité. Utilisez le guide ci-dessous pour vous aider.

Niveau de maturité de base

- Présentez un catalogue d'applications;
- Maintenez à jour la gestion de base des identités et des accès;
- Appliquez régulièrement les mises à jour et les correctifs des applications.

Niveau de maturité intermédiaire

- Tenez à jour le catalogue des applications en ayant une bonne compréhension de l'analyse des répercussions sur les activités et de la classification de l'information;
- Mettez en œuvre une stratégie mature de gestion des identités et des accès;
- Protégez les flux d'informations de bout en bout, à la fois en transit et en stockage;
- Instaurez des processus de traitement des incidents et des demandes d'accès;
- Appliquez la stratégie de défense en profondeur.

Niveau de maturité avancé

- Appliquez tous les éléments de la section précédente.

7.3.13 Conseils aux concessionnaires sur la mobilité

Pour déterminer les prochaines étapes du développement de la sécurité en matière de mobilité d'une concession, il faut d'abord identifier son niveau de maturité actuel. Déterminez ensuite les mesures qui peuvent être prises pour améliorer la position de la concession en matière de sécurité. Utilisez le guide ci-dessous pour vous aider.

Niveau de maturité de base

- Tenez à jour le logiciel antimaliciel;
- Définissez les informations qui peuvent être traitées et stockées sur les appareils mobiles; veillez à inclure les considérations relatives aux appareils gérés et non gérés;
- L'accès aux appareils doit être restreint, nécessitant l'authentification de l'utilisateur. La plupart des appareils peuvent être verrouillés au moyen d'un verrouillage d'écran, d'un mot de passe ou d'un numéro d'identification personnel (NIP).
- Mettez à jour le système d'exploitation mobile avec les correctifs de sécurité. De plus amples informations sur la gestion des correctifs sont disponibles à la section 2.6.3.

Niveau de maturité intermédiaire

- Tous les éléments du niveau de maturité de base;
- Appliquez le chiffrement des données à la fois sur les ordinateurs portables et sur les appareils mobiles en veillant particulièrement à la gestion des clés de déchiffrement;
- Passez en revue toutes les méthodes de connectivité, en accordant une attention particulière à la connectivité sans fil automatisée, car les mots de passe peuvent être exposés et des attaques par interception peuvent être exécutées;

- Créez des politiques et des procédures pour savoir qui peut accéder à distance à l'environnement de l'entreprise, quand et comment, et à quelles parties (réseau, serveurs, applications, etc.). Déployez une solution technique appropriée pour soutenir l'approche établie.

Niveau de maturité avancé

- Appliquez tous les éléments de la section précédente.

8. Glossaire

802.11 : 802.11 est un groupe de spécifications sans fil développées par l'IEEE pour les communications des réseaux locaux sans fil (WLAN). Il détaille une interface sans fil entre les appareils pour gérer le trafic de paquets afin d'éviter les collisions. Les spécifications les plus courantes sont les suivantes : 802.11a, 802.11b, 802.11g, 802.11n, etc. La norme 802.1X est conçue pour renforcer la sécurité des réseaux locaux câblés et sans fil qui respectent la norme IEEE.

Antenne : appareil permettant de transmettre et de recevoir des signaux de radiofréquence (RF). Les antennes sont souvent camouflées sur des bâtiments existants, des arbres, des tours d'eau ou d'autres structures élevées; leur taille et leur forme sont généralement déterminées par la fréquence du signal qu'elles prennent en charge.

Application (appli) : outils, ressources, jeux, réseaux sociaux ou presque tout ce qui ajoute une fonction ou une caractéristique à un appareil sans fil et qui est disponible gratuitement ou moyennant une redevance. Certaines applications peuvent également offrir aux utilisateurs la possibilité d'acheter du contenu ou des fonctions améliorées au sein de l'application. Les parents peuvent limiter la capacité de leur enfant à télécharger ou à effectuer ces achats intégrés en protégeant ces fonctions par un mot de passe sur un appareil sans fil. La Cellular Telecommnunications Industry Association (CTIA) a créé un système d'évaluation des applications afin d'informer les parents et de leur permettre de déterminer si l'application est adaptée à leurs enfants (en anglais) : **https://www.ctia.org/the-wireless-industry/industry- commitments/app-content-classification-ratings-guidelines**

Large bande : installation de transmission ayant une largeur de bande (capacité) suffisante pour transporter simultanément plusieurs canaux de voix, de vidéo ou de données. La large bande est généralement considérée comme un moyen de fournir des vitesses accrues et des capacités avancées, y compris l'accès à l'Internet et aux services connexes.

Câble de catégorie 5 : type de câble à paires torsadées conçu pour une intégrité accrue des signaux. La plupart de ces câbles ne sont pas blindés, mais certains le sont. La catégorie 5 a été remplacée par la spécification de catégorie 5e. Ce type de câble est souvent utilisé dans le câblage structuré des réseaux informatiques, tels que l'Ethernet, et sert également à transporter de nombreux autres signaux, comme les services vocaux de base, les anneaux à jeton et les guichets automatiques bancaires (jusqu'à 155 Mbits/s, sur de courtes distances).

Câble de catégorie 5e : la spécification de la catégorie 5e améliore les caractéristiques de la catégorie 5 en renforçant certaines dispositions relatives à la diaphonie et en introduisant de nouvelles dispositions relatives à la diaphonie qui n'étaient pas présentes dans les spécifications originales de la catégorie 5. La bande passante des catégories 5 et 5e est la même, soit 100 MHz.

Câble de catégorie 6 : norme de câble pour le protocole Gigabit Ethernet et d'autres protocoles de réseau rétrocompatible avec les normes de câble de catégorie 5 et 5e et de catégorie 3. La catégorie 6 présente des spécifications plus strictes en ce qui concerne la diaphonie et le bruit de réseau. La norme de câble offre une performance allant jusqu'à 250 MHz et convient aux normes 10Base-T, 100Base-TX et 1000Base-T (Gigabit Ethernet). On s'attend à ce qu'il convienne à la norme 10GBase-T (Ethernet 10 Gigabits), mais avec des limitations de longueur si un câble non blindé de catégorie 6 est utilisé. Ford Motor Company recommande un câblage de catégorie 6 lors de l'installation de nouveaux câbles ou du remplacement de nouveaux segments de réseau câblé.

Ligne d'abonné numérique (DSL) : ligne numérique reliant le terminal de l'abonné au bureau central de l'entreprise de service, offrant de multiples canaux de communication capables de transmettre simultanément des communications vocales et de données.

Chiffrement : brouillage numérique des informations afin qu'elles puissent être transmises de façon sécuritaire sur un réseau non sécurisé. À l'autre extrémité, le destinataire utilise généralement une « clé » numérique pour désembrouiller l'information, de sorte qu'elle retrouve sa forme initiale.

Ordinateurs portatifs ou tablettes : ces appareils sont des ordinateurs qui peuvent être transportés par un utilisateur. Ils sont

généralement beaucoup plus petits qu'un ordinateur portable classique et ne disposent pas de toutes les capacités d'un ordinateur de bureau, mais peuvent néanmoins effectuer la plupart des tâches nécessaires. Ils permettent également à l'utilisateur d'effectuer des travaux à différents endroits de la concession, ce qui peut accroître la productivité.

IEEE (Institute of Electrical and Electronics Engineers) : association professionnelle dont le siège social se trouve à New York et qui se consacre à la promotion de l'innovation et de l'excellence technologiques. Elle compte environ 425 000 membres dans quelque 160 pays, dont un peu moins de la moitié réside aux États-Unis (**http://www.ieee.org [en anglais]**).

Réseau local (LAN) : le réseau local (LAN) est un petit réseau de données couvrant une zone restreinte comme un bâtiment ou un groupe de bâtiments. La plupart des réseaux locaux connectent des stations de travail ou des ordinateurs personnels entre eux. Ainsi, de nombreux utilisateurs peuvent partager des appareils comme des imprimantes laser, ainsi que des données. Le réseau local permet également une communication facile, en favorisant l'envoi de courriels ou en soutenant les séances de clavardage.

Logiciel malveillant : les logiciels malveillants sont des programmes ou des fichiers nuisibles à une personne qui utilise un ordinateur. Les logiciels malveillants comprennent donc les virus informatiques, les vers informatiques et les chevaux de Troie, ainsi que les logiciels espions, c'est-à-dire les programmes qui recueillent sans autorisation des données sur une personne qui utilise un ordinateur.

Mégahertz : le mégahertz (MHz) est une unité de fréquence égale à un million de hertz ou de cycles par seconde. Aux États-Unis, les communications mobiles sans fil se font généralement dans les bandes de fréquences de 800 MHz, 900 MHz et 1900 MHz (Wi-Fi : 250, 400).

Authentification multifactorielle (AMF) : mesure de sécurité, processus ou technologie qui exige des utilisateurs qu'ils fournissent plus d'un justificatif d'identité pour accéder à l'information. Les utilisateurs doivent généralement fournir une combinaison d'éléments qu'ils connaissent (comme un mot de passe, des questions-réponses ou un NIP), des éléments qu'ils possèdent (comme un téléphone intelligent ou une clé USB) ou des éléments qui les constituent (comme une empreinte digitale ou la reconnaissance faciale).

Système d'exploitation : composante logicielle d'un système informatique responsable de la gestion et de la coordination des activités et du partage des ressources de l'ordinateur. Le système d'exploitation agit comme un hôte pour les programmes d'application qui sont exécutés sur l'ordinateur. En tant qu'hôte, l'un des objectifs d'un système d'exploitation est de gérer les détails du fonctionnement du matériel. Ford Motor Company recommande le système d'exploitation Windows 7 pour la compatibilité avec les applications Ford.

Gestion des correctifs : processus de mise à jour des serveurs ou des ordinateurs. Cette opération est souvent effectuée pour mettre à jour les ordinateurs avec les derniers correctifs de sécurité et ensembles de modifications provisoires (service pack). Les auteurs de virus, de logiciels espions et d'autres logiciels malveillants exploitent les failles existantes dans les logiciels installés sur un ordinateur pour se propager et causer des dommages. STAR recommande aux concessions d'appliquer dès que possible les correctifs critiques, comme ceux relatifs à la sécurité.

Point d'accès sans fil indésirable : point d'entrée sans fil dans le réseau de la concession qui n'est pas autorisé, sécurisé ou connu des services informatiques, de la direction et des propriétaires du concessionnaire. Tout réseau sans fil indésirable doit être détecté, localisé et supprimé immédiatement.

Routeur : appareil permettant à des ordinateurs de différents réseaux et sous-réseaux de communiquer. Dans les concessions, des routeurs peuvent être utilisés pour connecter à Internet un réseau local de fabricants d'équipement d'origine, un réseau local de système de gestion des concessions et un réseau local de système de gestion des données.

Spectre radio : fréquences radio désignées pour un usage précis, comme les services de communications personnelles et la sécurité publique.

Logiciel espion : toute technologie permettant de recueillir des informations sur une personne ou une organisation à son insu. Sur Internet, le logiciel espion (parfois appelé « spybot » ou « logiciel de suivi ») est un programme installé dans l'ordinateur d'une personne pour recueillir secrètement des informations sur celle-ci et les transmettre à des annonceurs ou à d'autres parties intéressées. Les concessionnaires doivent déployer des systèmes de détection et de suppression des logiciels espions afin de protéger les données des clients et l'intégrité de la sécurité du réseau.

Identifiant SSID (identifiant de l'ensemble de services) : dans le domaine des réseaux informatiques, un identifiant SSID est un ensemble composé de tous les appareils associés à un réseau local sans fil de la norme IEEE 802.11X. Les identifiants SSID doivent

être associés à un réseau local virtuel spécifique.

Protocole TCP/IP (Transmission Control Protocol/Internet Protocol) : protocole qui permet les communications sur les réseaux et entre eux; le protocole TCP/IP est à la base des communications sur Internet.

Cheval de Troie : le cheval de Troie est un programme d'apparence inoffensive dans lequel un code malveillant ou nuisible est contenu de manière à ce qu'il puisse prendre le contrôle d'un appareil et causer les dommages prévus, comme la destruction d'une certaine zone d'un disque dur.

Réseau privé virtuel (RPV) : un RPV permet à un utilisateur d'effectuer des transactions sécurisées sur un réseau public ou non sécurisé. Le chiffrement des messages envoyés entre les appareils permet de préserver l'intégrité et la confidentialité des données transmises.

Réseau local virtuel (VLAN) : dans les réseaux informatiques, un réseau de couche 2 unique (basé sur un commutateur) peut être partitionné pour créer plusieurs domaines de diffusion distincts, mutuellement isolés, de sorte que les paquets ne peuvent passer entre eux que par l'intermédiaire d'un ou plusieurs routeurs. On appelle ce domaine un réseau local virtuel (LAN virtuel) ou un VLAN. Ce type de réseau est généralement mis en place sur des commutateurs ou des routeurs.

Voix par protocole Internet (VoIP) : le protocole VoIP peut non seulement fournir de la voix par protocole Internet, mais il est également conçu pour permettre des vidéoconférences bidirectionnelles et le partage d'applications. Basé sur la technologie IP, le protocole VoIP est utilisé pour transférer une vaste gamme de types de trafic différents.

Réseau étendu (WAN) : terme général désignant un grand réseau couvrant un pays ou le monde entier. Internet est un réseau étendu. Un système de communication mobile public tel qu'un réseau cellulaire ou un réseau de service de communication personnelle (SCP) est un WAN. Les concessions peuvent mettre en réseau des sites et des bâtiments éloignés grâce à la technologie WAN. Dans la plupart des termes utilisés par les concessionnaires, le terme WAN fait référence au fournisseur d'accès Internet de la concession.

Ver informatique : un ver informatique est un virus autoreproducteur qui ne modifie pas les fichiers, mais qui se reproduit. Il est fréquent que les vers informatiques ne soient remarqués que lorsque leur réplication incontrôlée consomme les ressources du système, ralentissant ou interrompant d'autres tâches.

Wi-Fi : le Wi-Fi fournit une connectivité sans fil sur un spectre sans licence (en utilisant les normes IEEE 802.11a ou 802.11b), généralement dans les bandes radio de 2,4 et 5 GHz. Le Wi-Fi offre une connectivité locale aux ordinateurs compatibles avec le Wi-Fi.

Norme WPA (Wi-Fi Protected Access) : protocoles de sécurité et programmes de certification de sécurité développés par la Wi-Fi Alliance pour sécuriser les réseaux informatiques sans fil. La Wi-Fi Alliance l'a conçu comme une mesure intermédiaire en prévision de la disponibilité de la norme WPA2, plus sécuritaire et plus complexe. La norme WPA n'est pas sûre et ne doit pas être utilisée par les concessionnaires.

Norme WPA-2 (Wi-Fi Protected Access II) : la norme WPA2 a remplacé la norme WPA. La norme WPA2, qui doit être testée et certifiée par la Wi-Fi Alliance, met en œuvre les éléments obligatoires de la norme IEEE 802.11i.

Réseau local sans fil (WLAN) : grâce à la technologie des radiofréquences, les réseaux locaux sans fil transmettent et reçoivent des données sans fil dans une zone donnée. Les utilisateurs d'une petite zone peuvent ainsi transmettre des données et partager des ressources, telles que des imprimantes, sans être physiquement connectés à l'appareil.