Directives relatives à l'infrastructure des concessionnaires STAR

2020

LES MEILLEURES PRATIQUES ET RECOMMANDATIONS DE L'INDUSTRIE EN MATIÈRE DE TECHNOLOGIES DE L'INFORMATION POUR LA VENTE AU DÉTAIL DE VÉHICULES AUTOMOBILES

1. Directives relatives à l'infrastructure des concessionnaires STAR

1.1 Vue d'ensemble

Ce document complet - Directives pour l'infrastructure des concessionnaires STAR (DIG) - décrit les meilleures pratiques du secteur et doit être consulté par les concessionnaires pour vérifier les besoins en matière de réseau et d'infrastructure. Les concessionnaires, petits et grands, doivent disposer d'administrateurs de réseau internes - ou de responsables informatiques - chargés d'examiner ces lignes directrices, listes de contrôle et conseils ainsi que le guide de référence rapide pour s'assurer que leur concession a mis en place une solution sûre, sécurisée et robuste qui répond à la fois aux besoins du client et à ceux des équipes de la concession.

1.2 Le groupe de travail de DIG (WG)

Les directives relatives à l'infrastructure des concessionnaires (DIG) sont soutenues par l'un des nombreux groupes de travail (WG) au sein de l'organisation STAR. Contrairement à la plupart des groupes de travail qui se concentrent sur les structures et les transports de données, DIG a été créé pour aider les concessionnaires, les vendeurs et les équipementiers à élaborer un guide commun pour l'infrastructure informatique nécessaire à la sécurité, l'efficacité et la solidité des concessions automobiles.

1.3 Avantages de DIG - Concessionnaires, vendeurs et fabricants d'équipement d'origine (OEM)

Comme les autres concessionnaires, la concession automobile doit disposer de la technologie appropriée pour soutenir des processus robustes visant à vendre et à entretenir les véhicules. Avec l'avènement d'Internet, de nombreux systèmes différents sont mis à profit au sein d'une concession pour répondre aux demandes toujours croissantes des clients. Ces systèmes pour concessionnaires sont fournis et soutenus par les fournisseurs de systèmes pour concessionnaires (DSP) et comprennent tout, du système de gestion de la concession (DMS) de base aux nombreuses solutions de soutien telles que le marketing de la relation client (CRM), la gestion des prospects, l'extraction d'actions, la gestion de la réputation, les sites web, le marketing numérique, la gestion des stocks en ligne, les outils de voie de service, et bien d'autres. Avec le besoin toujours croissant de DSP, il est également nécessaire que les données soient partagées de manière efficace et sécurisée entre ces systèmes de concessionnaires et les OEM. Ce DIG est conçu comme un guide pour soutenir l'intégration efficace des données, la protection des données, la fiabilité du système et l'efficacité des processus commerciaux.

1.4 Décharge de responsabilité

Tout nom de société, application, lien de site web ou référence technologique mentionné dans ce document ne doit pas être considéré comme une approbation par les OEM ou par STAR, sauf si cette approbation est expressément mentionnée.

Ce document fournit une spécification de base ou une ligne directrice aux concessionnaires pour établir une communication sur Internet. Il est important de noter que l'infrastructure du réseau, les données des concessionnaires et la sécurité du système sont de la responsabilité du concessionnaire. Des entreprises tierces, telles que des prestataires de services et des partenaires, peuvent fournir des conseils et des recommandations. Certaines entreprises peuvent fournir des logiciels, du matériel ou des éléments de réseau propriétaires pour aider à rationaliser les opérations du réseau. Toutefois, ces applications, recommandations ou outils ne remplacent pas la gestion du réseau.

2. Infrastructure du réseau de concessionnaires

2.1 Vue d'ensemble

L'infrastructure de réseau d'un concessionnaire se compose des ressources matérielles et logicielles utilisées pour permettre la connectivité du réseau, 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, l'OEM et les clients finaux. La sélection et la mise en œuvre appropriées de l'infrastructure réseau sont essentielles pour assurer l'efficacité du réseau et sa compatibilité avec les applications et les données des OEM, des fournisseurs de services de traitement numérique des données et des concessionnaires.

2.2 Matériel

Le matériel des concessionnaires est un dispositif physique qui sert à saisir les données des concessionnaires (par exemple, les PC, les ordinateurs portables, les appareils de poche), à acheminer ces données (par exemple, les routeurs, les commutateurs, les pare-feu) et à fournir ces données sur demande (par exemple, les serveurs, les moniteurs et les périphériques).

La sélection du matériel réseau est un élément essentiel de la gestion du réseau d'un concessionnaire. Alors que le nouveau matériel peut représenter une dépense d'investissement très coûteuse, le vieux matériel peut entraver les opérations commerciales en raison de problèmes de vitesse ou de compatibilité, par exemple.

La section suivante détaille quand acheter du nouveau matériel, les directives d'achat et les recommandations pour l'achat d'ordinateurs de bureau, d'ordinateurs portables et d'équipements de réseau.

2.2.a Quand acheter du nouveau matériel ?

Un matériel informatique bien entretenu peut durer de trois à cinq ans, voire plus, dans certains cas. Toutefois, à un moment donné, un revendeur devra évaluer les possibilités de mettre à niveau - ou de remplacer - le matériel actuel.

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

- Lorsque le matériel actuel ne répond pas aux spécifications minimales nécessaires au fonctionnement d'une technologie spécifique.
- Le matériel actuel ne répond pas aux normes minimales fixées par un OEM, un DSP ou d'autres partenaires technologiques du concessionnaire.
- Le matériel actuel ne possède pas le matériel, les accessoires ou le support nécessaire aux périphériques pour une fonction spécifique.
- Le fonctionnement de l'appareil est si lent qu'il affecte les opérations commerciales. *Veuillez noter que cela n'est pas nécessairement dû à un problème de matériel. La lenteur peut être due à une erreur de configuration, de stockage, de sécurité ou d'utilisation.*
- Les nouveaux logiciels (tels que les systèmes d'exploitation, les navigateurs ou les applications des revendeurs) ne sont pas compatibles avec le matériel actuel.
- Un nouveau matériel pourrait permettre de réaliser des économies suffisantes grâce à des gains de temps, à des fonctionnalités supplémentaires ou à la facilité d'utilisation.
- Les coûts de mise à niveau sont égaux ou proches du coût d'un remplacement, ou le produit est en fin de vie et/ou n'est plus pris en charge.
- Le matériel n'est plus pris en charge par le fabricant. Cela signifie que les correctifs, les mises à jour de sécurité et les améliorations logicielles ne sont pas effectués sur le matériel. Lorsque le matériel n'est plus pris en charge, le concessionnaire est exposé à des risques de sécurité et de fiabilité.

2.2.b Quoi acheter : Matériel grand public ou matériel d'entreprise

La plupart des fabricants d'ordinateurs proposent deux catégories d'ordinateurs : du matériel grand public destiné à un usage domestique et personnel, et du matériel d'entreprise destiné aux entreprises. Si le prix du matériel grand public peut sembler intéressant pour les concessionnaires, le coût total de possession est souvent plus élevé en raison des fonctionnalités limitées, des taux d'échec plus élevés et de la complexité de l'assistance.

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

- Les systèmes grand public sont généralement fabriqués avec des pièces plus génériques ou des pièces moins coûteuses à fournir en gros. En outre, les fabricants sont connus pour changer de pièces, de fournisseurs et de composants sans changer de modèle. En raison de ces facteurs, ces pièces peuvent avoir un taux de défaillance plus élevé. Cela peut entraîner des temps d'arrêt plus longs, un temps de support plus long et un taux de remplacement des systèmes plus lent.
- Les systèmes d'entreprise sont généralement fabriqués avec des pièces normalisées de marque, ce qui facilite la normalisation du réseau et l'assistance pour de nombreuses entreprises.
- Les PC grand public sont souvent équipés de systèmes d'exploitation destinés à un usage domestique. Cela peut entraîner des difficultés de mise en réseau des entreprises, comme la connexion à des serveurs ou à d'autres PC.
- Le matériel réseau grand public est souvent conçu pour un petit nombre de connexions seulement. Le matériel de qualité professionnelle est conçu pour accueillir le grand nombre de connexions que les réseaux de concessionnaires exigent.
- Le matériel de qualité grand public peut être assorti de garanties limitées. Certaines garanties grand public ne s'étendent pas aux entreprises.
- Les économies initiales pourraient être compensées par un remplacement plus coûteux et une assistance technique ainsi que par des délais d'exécution plus longs pour obtenir un remplacement.

2.2.c Recommandations relatives au matériel

Ordinateur de bureau	
Composant	**Spécifications**
Processeur	Intel Core i5 et au-dessus, ou équivalent AMD
Mémoire (RAM)	4 GB ou plus
Disque dur	500 GB ou plus
Lecteur CD/DVD	Lecteur CD/DVD, ou un lecteur externe
Port en série	1 (facultatif adaptateur USB)
Ports USB	2 ou plus
Adaptateur Audio	16 bit
Haut-parleur	Facultatif
Affichage	1280x768 résolution minimum
Adaptateur réseau	Câblé: Gigabit (u supérieur) Ethernet Sans fil: 802.11 n ou ac

Garantie	3 ans sur site
Système d'exploitation	Les systèmes d'exploitation Windows sont compatibles avec la plupart des applications des concessionnaires. Veuillez consulter vos partenaires OEM et technologiques lors du choix d'un système d'exploitation.

Ordinateurs portables	
Composant	**Spécifications**
Processeur	Intel Core i5 ou au-dessus, ou équivalent AMD
Mémoire (RAM)	4 GB ou plus
Disque dur	320 GB ou plus
Lecteur CD/ DVD	Lecteur CD/DVD, ou lecteur externe
Ports USB	2
Haut-parleur	Facultatif
Affichage	1280x768 résolution minimum
Adaptateur réseau	Câblé: Gigabit (ou supérieur) Ethernet Sans fil: 802.11 n ou ac
Garantie	3 ans sur site
Système d'exploitation	Les systèmes d'exploitation Windows sont compatibles avec la plupart des applications des concessionnaires. Veuillez consulter vos partenaires OEM et technologiques lors du choix d'un système d'exploitation.

Routeurs & Commutateurs	
Composant	**Spécifications**
Spécification de la norme Ethernet	IEEE 802.3 100baseT ou 1000baseT
Redondance	La connexion de plusieurs commutateurs ensemble doit utiliser des liens redondants de la plus haute vitesse disponible, en utilisant STP ou rSTP pour assurer une topologie sans boucle.
Alimentation électrique	Des alimentations redondantes sont recommandées pour réduire les temps d'arrêt.
Vitesse	100 ou 1000 Mbps
VLAN	Les commutateurs avec VLAN et la technologie trunk 802.1Q 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 industrielles de gestion à distance telles que le protocole SNMP (Simple Network Management Protocol) et le RMON (Remote Network Monitoring).
Commutateurs sans fil	Les appareils sans fil doivent être à double bande et compatibles avec la norme IEEE 802.11b/g/n.

2.2.d Tablettes et appareils mobiles

Les tablettes sont des appareils portables conçus pour la mobilité et l'accessibilité. Les tablettes n'ont pas les mêmes fonctionnalités qu'un ordinateur de bureau ou un ordinateur portable. Pour cette raison, il est fortement recommandé aux concessionnaires de ne pas remplacer les ordinateurs de bureau ou les ordinateurs portables par des tablettes, mais plutôt de les

compléter par des tablettes lorsque les applications et les fonctions exigent une mobilité et une accessibilité plus grandes.

Certaines applications sont spécifiquement développées pour fonctionner sur certains appareils à tablettes tels que les iPads. Lorsque ces applications sont déployées, l'OEM ou le DSP communiquent avec les appareils 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 et/ou des versions de systèmes d'exploitation de dispositifs mobiles spécifiques.

2.2.e Déclassement et recyclage du matériel

Il incombe au propriétaire de l'appareil d'origine de veiller à ce que tous les appareils électroniques usagés soient éliminés de manière appropriée. Il existe des milliers de recycleurs d'appareils électroniques aux États-Unis, mais il est important de choisir le bon. Vous trouverez ci-dessous quelques suggestions à suivre pour choisir un recycleur.

Renseignez-vous sur les politiques / pratiques du recycleur en matière de destruction des données personnelles sur 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 l'effacement des données doit être effectuée plus d'une fois (multi-pass).
- Les supports de stockage peuvent être détruits par broyage, découpage, incinération, perforations multiples ou écrasement.
- Un recycleur doit être en mesure de fournir une certification écrite attestant que les données ont été effacées - ou les supports de stockage détruits - ainsi qu'un enregistrement de la ou des méthodes utilisées.

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

- Le recycleur doit être certifié. Si on nous dit qu'il n'est pas certifié, qu'il s'agit d'un "secret commercial" ou que sa méthode est "confidentielle", évitez de faire appel à lui.
- Les principales certifications de la branche sont :
    - E-Stewards – www.e-stewards.org
    - Basel Action Network – www.ban.org
    - R2 – www.sustainableectronics.org
- Les recycleurs et les groupeurs doivent pouvoir prouver qu'ils disposent des installations, de la formation et de l'équipement appropriés pour effectuer les opérations déclarées en présentant un système de gestion/exploitation vérifié, accompagné des preuves des 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'Association internationale des recycleurs d'appareils électroniques (IAER) ou l'Institut des industries de recyclage de la ferraille (ISRI).
- Pour ceux qui ne sont pas certifiés, la prudence est de mise. Le concessionnaire, en tant que propriétaire de l'appareil d'origine, a la responsabilité d'assurer un recyclage adéquat.

Renseignez-vous pour savoir si le recycleur a commis des infractions à l'environnement ou à la sécurité (procès-verbaux, amendes, avis d'infraction, ordonnances de consentement, etc.) ou

s'il a déposé une demande d'indemnisation auprès de l'assurance contre les dommages causés à l'environnement au cours des cinq dernières années.

- Les entreprises qui ont de bons antécédents en matière de respect des exigences environnementales et de sécurité sont privilégiées.
- Une entreprise qui est en activité depuis plusieurs années et qui n'a commis que quelques infractions mineures rapidement résolues peut-être tout aussi responsable qu'une entreprise qui n'a commis aucune infraction pendant un an ou deux.
- Vérifiez les violations majeures telles que les rejets de déchets en grande quantité ou les plaintes importantes du voisinage.

Vérifiez si le recycleur envoie des équipements usagés ou des déchets à d'autres partenaires commerciaux ou fournisseurs de services ; ceux-ci sont appelés "partenaires en aval".

- La bonne tenue des dossiers est une pratique de gestion exemplaire dans l'industrie. Recherchez les 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 recycleurs " tous services " aux États-Unis, il est probable que le recycleur ne s'occupe pas du traitement complet de l'appareil.
- L'entreprise de recyclage doit disposer de registres écrits indiquant ce qui est traité sur place (tri et/ou broyage, par exemple) et qui reçoit les matériaux ou les produits après le traitement initial.
- Demandez si les partenaires commerciaux du recycleur (partenaires en aval) sont contractuellement tenus de respecter les mêmes normes ou les meilleures pratiques de gestion que le recycleur choisi. Une liste complète de tous les partenaires en aval devrait être disponible auprès du recycleur choisi.
- Méfiez-vous des recycleurs qui déclarent que leurs procédés et leurs partenaires commerciaux sont "confidentiels", "exclusifs" ou qu'"ils ne connaissent pas".
- Toute exportation doit être effectuée dans le respect des lois applicables aux pays exportateurs et importateurs.

Un recycleur doit disposer d'une assurance responsabilité générale et d'une assurance responsabilité environnementale.

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

2.3 Logiciel

Le logiciel est le programme ou les informations d'exploitation utilisés par le matériel du concessionnaire pour saisir, stocker, manipuler et afficher des données sur le matériel du réseau. Les concessionnaires utilisent des logiciels pour capturer les données des clients, automatiser les processus commerciaux pour la vente et l'entretien des véhicules et communiquer avec d'autres systèmes ou réseaux.

Pour les concessionnaires, ces programmes ou processus résident souvent sur le système d'exploitation d'un PC ou sur un navigateur internet. Les logiciels sont souvent conçus pour des systèmes d'exploitation ou des navigateurs internet spécifiques. Les logiciels étant essentiels pour les communications et les processus commerciaux des concessionnaires, il est important que ces derniers utilisent des systèmes d'exploitation et des navigateurs compatibles avec les logiciels de la concession.

La section suivante détaille les systèmes d'exploitation et les navigateurs les plus courants. L'objectif de cette section est de fournir des conseils pour comprendre et sélectionner les systèmes d'exploitation et

les applications de navigation. Il est fortement recommandé aux concessionnaires de vérifier auprès de leurs OEM et de leurs fournisseurs de services pour s'assurer de la compatibilité des logiciels avec les applications des concessionnaires.

2.3.a Systèmes d'exploitation

Vous trouverez ci-dessous une liste des systèmes d'exploitation les plus courants sur le marché actuel. Certaines applications ne sont pas compatibles avec des systèmes d'exploitation spécifiques. Il est recommandé aux distributeurs de vérifier auprès de leurs OEM, DSP et autres vendeurs pour déterminer les systèmes d'exploitation à utiliser. Veuillez noter que Microsoft a cessé de prendre en charge les systèmes d'exploitation XP, Vista et Windows 7. Cela inclut les mises à jour de sécurité critiques. STAR recommande aux concessionnaires de ne pas utiliser Windows XP, Vista, ni Windows 7.

Systèmes d'exploitation clients communs actuels	Dernière mise à jour ou service pack*	Fin du soutien général	Fin du soutien prolongé
Windows XP	Service Pack 3	14-Apr-09	8-Apr-14
Windows Vista	Service Pack 2	10-Apr-12	11-Apr-17
Windows 7	Service Pack 1	13-Jan-15	14-Jan-20
Windows 8	Windows 8.1	9-Jan-18	10-Jan-23
Windows 10, disponible en juillet 2015	N/A	13-Oct-20	14-Oct-25
MAC OS X	10.9 (ou supérieur pris en charge) 10.11	Les versions 10.8 (Mountain Lion) et inférieures ne sont plus prises en charge.	Les versions 10.8 (Mountain Lion) et inférieures ne sont plus prises en charge.
IOS (pour iPad et iPhone)	9.1		
Android	5		

**** Dernières mises à jour / Service Pack à partir de novembre 2015***

2.3.b Navigateurs Internet

Vous trouverez ci-dessous une liste des navigateurs internet les plus courants sur le marché actuel. Certaines applications ne sont pas compatibles avec des navigateurs spécifiques. D'autres applications nécessitent des paramètres de navigateur spécifiques, tels que le mode de compatibilité. Il est recommandé aux revendeurs de vérifier auprès de leurs OEM, DSP et autres vendeurs pour déterminer les systèmes d'exploitation à utiliser.

Navigateur	Dernière mise à jour ou service pack*	Remarques
Google Chrome	77	
Mozilla Firefox	69	
Internet Explorer	11	
Apple Safari	13	Utilisation non recommandée sur les systèmes d'exploitation Microsoft
Opera	63	
Edge	44	

**** Dernières mises à jour / pack de services à partir de janvier 2020***

2.3.c Licences de logiciels

La conformité des licences de logiciels est une chose sur laquelle la plupart des concessionnaires ne se concentrent pas. Cependant, elle peut coûter des milliers de dollars à un concessionnaire si elle est ignorée. Voici les erreurs les plus courantes en matière de licences de logiciels pour un concessionnaire.

- Partager une licence commune au lieu d'en avoir une par appareil
- Partage de logins pour les logiciels en Cloud
- Avoir installé des copies sous licence légale de logiciels mais ne pas les utiliser

- Acheter des versions " familiales " de logiciels au lieu d'acheter des versions professionnelles ou d'entreprise
- Utilisation de logiciels piratés, téléchargés gratuitement

Pour résoudre ce problème, les entreprises doivent créer un programme de gestion des actifs logiciels (SAM). Le SAM est la pratique consistant à gérer et à optimiser l'achat, le déploiement, la maintenance et le cycle de vie des actifs logiciels au sein d'une organisation. Les deux principaux avantages d'un programme SAM sont le contrôle des coûts et la réduction des risques.

2.4 Réseau local (LAN)

Un réseau local (LAN) est un groupe d'ordinateurs et de dispositifs associés connectés ensemble en utilisant des communications communes partagées telles qu'une ligne de câble ou une liaison sans fil. Les concessionnaires doivent gérer un réseau afin que les appareils de la concession puissent communiquer et partager des ressources de manière efficace mais sûre.

La gestion d'un réseau peut être une tâche difficile pour les concessionnaires automobiles. Les concessionnaires doivent mettre le réseau à disposition pour partager des données ainsi que limiter l'accès à des fins de sécurité. Outre les employés du concessionnaire, il arrive souvent qu'un prestataire de services, un OEM et même des clients doivent également partager les ressources du réseau. Fournir un accès sûr et sécurisé au réseau de concessionnaires peut s'avérer difficile.

La section qui suit fournit des recommandations pour la configuration et la gestion du réseau local. Elle fournit également des conseils sur les réseaux sans fil, la mobilité des concessionnaires et l'accès des clients.

2.4.a Configuration et gestion du réseau

Recommandation	Spécification
Réseau local	Gigabit Ethernet
Câblage de données	Le câblage des réseaux de données existants devrait être - au minimum - conforme aux normes TIA-568-A Catégorie 5e. La catégorie 6a doit être utilisée pour le nouveau câblage. Aucun câble horizontal ne doit dépasser 90 mètres (295 pieds). Il est fortement recommandé d'utiliser des câbles à fibres optiques au lieu de câbles de données lorsque la longueur dépasse 295 pieds.
Emplacement des équipements	L'équipement LAN doit être logé dans un placard de câblage ou une salle de communication. Tout l'équipement doit être monté ou fixé sur un rack ou une étagère.
Adresse IP	Le fournisseur d'accès Internet du concessionnaire doit fournir une adresse IP routable. Pour le réseau local du concessionnaire, l'adressage dynamique (DHCP) devrait être utilisé pour faciliter le support.
Adaptateur réseau	Gigabit Ethernet
Commutation Ethernet	Commutateur géré de Gigabit. Étiqueter chaque interface et chaque câble. Cela permettra de gagner du temps lors du suivi des câbles réseau pour le support ou une nouvelle installation.
Routeurs	Routeur de niveau professionnel. Les routeurs doivent prendre en charge la technologie NAT/PAT (Network Address Translation/Process Analytical Technology). Les routeurs doivent également prendre en charge le routage dynamique en utilisant RIPv2, OSPF et BGP. - Changez le mot de passe de l'appareil au moment de l'installation et de façon continue et régulière. - Conserver une configuration de sauvegarde dans un fichier en cas de panne de logiciel ou de remplacement de matériel.
Firewall	Un dispositif de sécurité entièrement géré qui surveille en permanence les menaces par le biais du système de détection des intrusions "IDS" et du système de prévention des intrusions "IPS" et d'autres mécanismes tels que le filtrage des paquets, l'antivirus et l'inspection des paquets par état. - Les firewalls doivent prendre en charge la technologie NAT/PAT (Network Address Translation/Process Analytical Technology). Les firewalls doivent également prendre en charge le routage dynamique en utilisant RIPv2, OSPF et BGP. - Changez le mot de passe de l'appareil au moment de l'installation et de façon continue et régulière. - Conserver une configuration de sauvegarde dans un fichier en cas de panne de logiciel ou de remplacement de matériel. - Pour plus d'informations sur les firewalls et la sécurité des réseaux, voir la section 2.6.
Services de noms de domaine (DNS)	Utilisez le DNS public, sauf si vous utilisez Windows Active Directory. (Dans ce cas, il est nécessaire de disposer d'un serveur DNS interne).

2.4.b Réseaux sans fil

Les réseaux locaux sans fil permettent la communication en réseau sans les contraintes physiques du réseau câblé. La technologie sans fil peut être particulièrement pratique dans la mesure où elle peut offrir une certaine mobilité aux employés, permettre aux clients d'apporter et d'utiliser leur propre appareil et étendre le réseau de concessionnaires au-delà des murs physiques de la concession. Les concessionnaires doivent également comprendre que l'omniprésence des réseaux sans fil pose des problèmes de conception, d'assistance et de sécurité.

Utilisez les instructions suivantes lors de la conception, du support et de la sécurisation d'un réseau sans fil de concessionnaires.

Conception de réseaux sans fil	
Recommandation	**Spécification**
Matériel sans fil	Seuls les points d'accès de niveau entreprise doivent être utilisés. Les points d'accès d'entreprise sont conçus pour fournir l'itinérance et d'autres fonctionnalités de classe affaires (telles que les VLAN et/ou les SSID multiples) nécessaires à la prise en charge des appareils sans fil pour les applications. Les points d'accès sans fil de niveau professionnel sont également conçus pour accueillir un plus grand nombre de connexions que le matériel de niveau consommateur.
Segmentation du réseau	Les concessionnaires doivent veiller à ce que le trafic des visiteurs soit segmenté à partir du réseau de la concession par des VLAN ou une connexion internet séparée.
SSIDs	Il est recommandé aux concessionnaires d'utiliser des SSID distincts pour les différentes fonctions commerciales (c'est-à-dire la vente, le service et l'administration). Toutefois, les concessionnaires ne doivent pas confondre les SSID avec la segmentation du réseau. Les SSID ne séparent généralement pas le trafic du réseau, mais fournissent seulement une manière différente de rejoindre le réseau.
Couverture	Déployer des points d'accès sans fil pour assurer une couverture adéquate. Les outils sans fil peuvent fournir une puissance de signal autour du bâtiment. Soyez attentif aux structures ou aux objets qui peuvent interférer avec la couverture sans fil (interférences électriques, interférences de radiofréquence ou matériaux physiques tels que les métaux ou le béton).
Authentification et cryptage	WPA2 avec authentification RADIUS et cryptage AES
Norme de réseau	802.11n ou 802.11ac
Détection des réseaux sans fil malveillants	Scanner, identifier et supprimer tout point d'accès sans fil malveillant qui pourrait se trouver sur le réseau du concessionnaire. - Un point d'accès sans fil malveillant 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 informatique et le propriétaire. - Tous les réseaux sans fil malveillants 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 à la recherche de menaces sans fil.

Mobilité des concessionnaires	
Recommandations	**Spécification**
Mobilité au sein de la concession	Utiliser un réseau maillé sans fil pour s'assurer que les utilisateurs finaux peuvent naviguer dans le lieu sans perdre la connexion ou 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 les points d'accès légers sur le réseau de la concession. Cela permettra d'assurer une couverture adéquate, la fiabilité et l'efficacité du réseau.

Accès client	
Recommandations	**Spécification**
Hiérarchisation des priorités en matière de trafic	Les concessionnaires devraient utiliser un firewall ou un autre mécanisme pour limiter la consommation de bande passante des clients. Cela empêchera l'accès des visiteurs d'interférer avec les opérations commerciales en consommant trop de bande passante.
Authentification des invités/ Conditions de service	STAR recommande aux concessionnaires d'utiliser un portail captif exigeant des invités qu'ils acceptent les conditions d'utilisation de la concession. Ces conditions peuvent inclure des restrictions de contenu, des limitations de bande passante et des accords d'utilisation.
Bande passante Internet	Pour s'assurer que la concession dispose d'une bande passante suffisante, le concessionnaire doit choisir la technologie et la vitesse appropriées. (Voir les sections 2.5a et 2.5b dans le STAR DIG pour plus d'informations sur les technologies et la bande passante internet). - STAR recommande également à chaque concessionnaire de disposer d'une connexion de secours à un fournisseur d'accès Internet (FAI) d'un autre fournisseur, utilisant une technologie différente. - Voir la section 2.5c pour les recommandations sur les connexions de sauvegarde sur internet.

2.5 Bande passante Internet

La largeur de bande Internet est la quantité de données qui peut être envoyée vers et depuis le concessionnaire, généralement mesurée en bits par seconde. La plupart des logiciels des concessionnaires reposent sur 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 via l'internet. En outre, de nombreux employés et clients dépendent de l'accès à l'internet de la concession pour des raisons personnelles, par exemple pour consulter leur courrier électronique ou surfer sur le web. Étant donné que de nombreux utilisateurs dépendent d'Internet pour obtenir des informations, il est essentiel que le concessionnaire se procure une bande passante suffisante pour que chaque ressource dispose d'une largeur de bande suffisante pour accéder rapidement aux données. Pour s'assurer que la concession dispose d'une largeur de bande suffisante, le concessionnaire doit choisir la technologie et la vitesse appropriées.

La section suivante détaille les technologies disponibles pour l'accès à l'internet et la manière de prévoir une largeur de bande suffisante pour chaque ressource sur le réseau local (LAN).

2.5.a Technologies Internet

Technologie	Description	Vitesse	Support physique	Commentaires
Câble	Un modem câble spécial et une ligne de câble sont nécessaires.	Les vitesses peuvent varier, mais se situent généralement entre 10 Mbps et 100 Mbps	Câble coaxial	Le service Internet par câble utilise une infrastructure partagée et peut se dégrader en cas d'utilisation intensive. Les concessionnaires doivent vérifier quels fournisseurs de câble offrent déjà un service dans la région. Le coût de la mise en place du service dans une zone et de l'excavation des câbles peut être prohibitif. Ford recommande aux concessionnaires d'acheter du câble de qualité professionnelle et de demander au fournisseur un accord écrit sur le niveau de service (SLA) ou un objectif de niveau de service (SLO).
DSL	La technologie utilise la partie numérique inutilisée d'une ligne téléphonique ordinaire en cuivre pour transmettre et recevoir des informations. L'ADSL est asymétrique, ce qui signifie que la vitesse de téléchargement en amont du service est plus lente que la vitesse de téléchargement en aval. La SDSL est symétrique, c'est-à-dire qu'elle se compose des mêmes vitesses de téléchargement en amont et en aval. Le VDSL est une autre technologie asymétrique qui peut offrir des vitesses allant jusqu'à 52 Mbps.	128 Kbps à 52 Mbps	Paire torsadée (utilisée comme support numérique à large bande)	Ford recommande aux concessionnaires d'acheter des lignes DSL de qualité professionnelle avec une vitesse de téléchargement en amont et en aval suffisante pour pouvoir utiliser les applications des concessionnaires Ford. Le VDSL est le seul service DSL recommandé, car c'est peut-être le seul à disposer d'une bande passante suffisante pour répondre aux exigences de bande passante recommandées.
T1	Des lignes et des équipements spéciaux (DSU/CSU et routeur) sont nécessaires.	1.544 Mbps	Paire torsadée, câble coaxial ou fibre optique	Plusieurs lignes T1 peuvent être reliées entre elles pour obtenir des vitesses plus élevées.
Satellite		6 Mbps ou plus	Ondes radio Peut utiliser l'accès par ligne commutée pour le trafic en amont	La bande passante n'est pas partagée. De plus, la latence est généralement élevée. Cette latence élevée interfère souvent avec les applications des distributeurs. Le satellite n'est pas une technologie recommandée pour les revendeurs.
Fibre	Les types de connectivité Internet par service de fibre optique fonctionnent sur un réseau optique.	Jusqu'à 300Mbps	Réseau optique	La fibre optique offre des vitesses élevées, des coûts réduits et de bons accords de niveau de service. Toutefois, la disponibilité 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 nombreux concessionnaires ignorent la technologie, la vitesse et l'utilisation actuelles de l'internet. La compréhension de la technologie peut aider à identifier les limites et les économies potentielles. Utilisez le tableau ci-dessus pour mieux comprendre les différentes

technologies disponibles sur le marché. Renseignez-vous sur les vitesses de téléchargement en amont et en aval de la bande passante du service actuel (généralement identifiées en Mbps ou Kbps) en vous renseignant auprès du fournisseur d'accès Internet du concessionnaire. Enfin, connectez-vous au dispositif de passerelle du concessionnaire, demandez au fournisseur d'accès Internet du concessionnaire ou trouvez des tests en ligne pour comprendre l'utilisation actuelle de la bande passante.

Prévoir les pics d'utilisation

L'utilisation de la bande passante n'est pas toujours cohérente. Les concessionnaires constatent des pics d'utilisation en fonction des processus commerciaux (tels que les "périodes de pointe"), des processus technologiques (tels que l'exécution de sauvegardes ou le téléchargement de mises à jour) et de l'utilisation des clients (tels que la diffusion de vidéos en continu depuis la salle d'attente des clients). Il est recommandé que les concessionnaires enregistrent une moyenne d'utilisation d'environ 60 % pour tenir compte des pics potentiels.

Prévoir les progrès technologiques

La plupart des OEM, des DSP et des concessionnaires développent des solutions qui permettent d'exploiter davantage les communications Internet. Les concessionnaires doivent comprendre que leurs besoins en bande passante ne sont pas statiques, mais qu'ils continueront de croître à mesure que les concessionnaires, les vendeurs et les partenaires mettront en œuvre de nouvelles technologies.

Plan de croissance

L'IEEE (Institut des ingénieurs en électricité et en électronique) affirme que les réseaux devront pouvoir supporter des taux de croissance annuels composés 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 à la demande et les médias sociaux.

Rester vigilant

L'utilisation de la bande passante n'étant pas statique, la planification doit être une activité permanente. En obtenant une visibilité sur les habitudes d'utilisation de la concession, un administrateur informatique peut mieux anticiper les éventuelles limitations de la bande passante avant qu'elles n'aient un impact sur les performances de la concession. Il est recommandé aux concessionnaires de mettre en place des alertes pour les pics d'utilisation, l'utilisation moyenne de la consommation ou les périodes d'indisponibilité de la bande passante. Cela permettra d'atténuer les risques, de limiter les temps d'arrêt et de permettre au concessionnaire de se mettre à niveau avant que cela n'ait un impact significatif sur l'activité de l'entreprise.

2.5.c Connexion de secours

La disponibilité du service Internet est essentielle pour les entreprises de concessionnaires. Comme les concessionnaires dépendent d'Internet pour vendre et entretenir les véhicules, une connexion de secours est recommandée.

Lorsque vous choisissez une connexion de secours, suivez les recommandations suivantes :

- Utilisez un autre fournisseur et une autre technologie Internet pour la connexion de secours.
- Disposez au minimum d'un service de secours/ de basculement à large bande 3G/4G. Testez le signal sans fil à l'avance pour vous assurer que la puissance du signal est suffisante. Les fournisseurs d'accès à Internet, l'emplacement physique et la conception du bâtiment sont autant de variables qui déterminent la puissance du signal dans une concession donnée.
- STAR recommande un circuit dédié pour une haute disponibilité.

- STAR recommande aux concessionnaires d'utiliser un appareil de passerelle qui prend en charge le basculement automatique pour garantir un temps d'arrêt minimal.
- Le service de secours ne doit pas nécessairement être aussi rapide que la connexion principale, mais doit néanmoins disposer d'une bande passante suffisante pour prendre en charge les fonctions commerciales critiques de la concession.

2.6 Sécurité

L'objectif de l'infrastructure de réseau d'un concessionnaire est de partager des données et des ressources avec les employés, les clients et les fournisseurs ou partenaires tiers. Les concessionnaires doivent également prendre des mesures pour garantir que ces données sont partagées en toute sécurité. Les concessionnaires doivent surveiller les connexions connues et inconnues pour détecter tout signe de perte de données. Un concessionnaire doit prendre des mesures pour protéger les données au niveau de la passerelle et de chaque point d'extrémité du réseau. Les technologies, les processus et les procédures 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, du bureau, de la gestion des événements de sécurité des informations et de la sécurité des données, ainsi que du point de vue du client, du gouvernement, des risques et de la conformité. De plus, des informations sur les processus et les procédures de sécurité se trouvent dans 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 du concessionnaire doit être complet, cohérent et approuvé par l'organe de gestion du concessionnaire. Il est important de s'assurer que toutes les parties prenantes s'engagent à respecter les 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 - et la compréhension des exigences de sécurité est ici le facteur clé. L'accent doit être mis sur la confidentialité, l'intégrité et la disponibilité des données et des ressources sensibles, y compris l'environnement physique, l'infrastructure de réseau, les applications et les données (physiques et numériques). Toutefois, cette liste n'est pas exhaustive, car il existe de nombreuses autres considérations. Par exemple, la non-répudiation, la traçabilité ou l'authenticité doivent souvent être prises en compte.

En outre, 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 dans les airs 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 devraient refléter ces considérations.

Il existe de nombreuses politiques ou directives cadres de sécurité prêtes à l'emploi parmi lesquelles choisir et appliquer dans une entreprise. Toutefois, même si ce type de cadre peut fournir une base de référence générale, une entreprise devra ajuster et développer les politiques pour les appliquer dans son contexte commercial.

2.6.b Gestion des identités et des accès Gestion des correctifs

Couvrir la gestion des identités et des accès de manière exhaustive. Commencez par une introduction et des concepts de base suivis de sous-sections : gestion des identités, authentification, autorisations, pourquoi elles sont si importantes, processus de gestion des accès, utilisateurs finaux et considérations physiques, et niveaux de protection. Terminez par une introduction aux trois niveaux de maturité.

2.6.c Gestion des correctifs

Les systèmes d'exploitation des serveurs/ordinateurs locaux nécessitent de temps en temps des mises à jour, dont beaucoup sont dues à des risques de sécurité. Les correctifs envoyés 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 garantir une application fiable et sûre. En outre, les concessionnaires doivent accorder une attention particulière aux points suivants :

- Systèmes en fin de vie (EOL)
  - Se tenir au courant des systèmes d'exploitation en fin de vie (EOL) permettra de s'assurer que l'établissement 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'assurer l'assistance.
  - En général, les fournisseurs fournissent un avis de fin de vie et cela peut toujours être vérifié sur leurs sites web respectifs.
- Appareils mobiles
  - Les appareils mobiles quittent souvent la protection d'un réseau de concessionnaires pour se connecter à un autre réseau, souvent moins sécurisé. De ce fait, ces appareils peuvent être considérés comme plus vulnérables. Il est important que les appareils mobiles soient rapidement réparés afin de limiter les risques et l'exposition aux menaces et aux vulnérabilités.

2.6.d Formation de 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 cliquer sur un courriel de phishing, par exemple. Tout comme les techniciens sont formés aux derniers développements en matière de véhicules et les vendeurs aux nouvelles caractéristiques des véhicules et aux techniques de vente, tous vos employés doivent être formés à la protection de votre entreprise contre le vol, les violations de données et autres problèmes de sécurité.

L'objectif du programme de formation n'est pas seulement d'éduquer vos employés, mais aussi d'influencer leur comportement. Ils doivent devenir un pare-feu humain pour l'entreprise.

La sécurité ne doit pas être fastidieuse - si les gens ne font pas attention, le message ne passera pas - alors n'ayez pas peur de faire preuve de créativité avec le programme de formation et de sensibilisation. L'humour, les exemples concrets, les concours et les jeux sont autant de moyens de maintenir l'intérêt et d'obtenir l'engagement des employés.

Pour maintenir l'engagement des employés, envisagez d'utiliser plus fréquemment des modules de formation à la sécurité en ligne, plus courts, plutôt qu'une fois par an, dans le cadre de longues sessions de formation. Cela permettra également de tenir la formation à jour sur les dernières évolutions en matière de logiciels malveillants et d'attaques.

- La formation devrait être annuelle, au minimum, et porter sur des sujets tels que :
  - Sensibilisation à l'ingénierie sociale : phishing, Business Email Compromise (BEC), phishing, logiciels de rançon, navigation sécurisée sur le web
  - Mots de passe
  - Données sensibles - PII, PCI, PHI, etc. - et traitement des données
  - Partage des données et politiques d'utilisation acceptable
  - Protection et destruction des données
  - Sécurité des appareils mobiles
  - Un réseau social sûr

    - La violence sur le lieu de travail
    - Politiques d'entreprise liées à la sécurité
- Une formation complémentaire peut être nécessaire en fonction du rôle de l'employé dans l'entreprise. Par exemple, les employés qui gèrent les finances de l'entreprise peuvent avoir intérêt à comprendre la manière unique dont ils sont ciblés par les cybercriminels pour l'accès qu'ils ont aux comptes bancaires. Envisagez une formation basée sur les rôles pour aider les employés à comprendre le rôle qu'ils jouent dans la protection de l'entreprise dans leurs activités quotidiennes.
- Utilisez des supports de sensibilisation à la sécurité dans les salles de pause et autres espaces réservés aux employés, tels que des affiches ou des dépliants rappelant aux employés la nécessité de traiter en toute sécurité les données des clients, la sensibilisation à l'ingénierie sociale, les rappels de formation, etc.
- Utilisez les bulletins d'information de l'entreprise, les courriels, les sessions de formation en direct et d'autres fonctions de l'entreprise pour renforcer continuellement le message de sécurité.
- Revoir régulièrement les programmes de formation et s'adapter aux nouvelles technologies, aux changements dans l'activité des concessionnaires et aux commentaires des employés.
- Ressources. Elles peuvent être gratuites ou payantes, mais certains de vos partenaires commerciaux peuvent proposer à vos employés des formations en ligne sur la sécurité.
    - Fournisseur DMS
    - Prestataire d'assurance
    - Cabinet d'expertise comptable
    - Cabinet juridique
- Autres ressources :
    - https://staysafeonline.org/business-safe-online/train-your-employees
    - SANS Ouch – un bulletin d'information mensuel gratuit sur la sécurité destiné aux employés https://securingthehuman.sans.org/resources/newsletters/ouch/2016

2.6.e **Respect des législations fédérales**

Veiller à ce que le concessionnaire respecte toutes les réglementations fédérales, étatiques, locales et sectorielles applicables aux institutions financières et de détail, telles que la loi Gramm-Leach-Bliley, la règle de sauvegarde, le PCI DDS, etc.

- Loi Gramm-Leach-Bliley (GLB) et règle de sauvegarde
    - La loi de modernisation financière de 1999, également connue sous le nom de "Gramm-Leach-Bliley Act" ou GLB Act, comprend des dispositions visant à protéger les informations financières personnelles des consommateurs détenues par les institutions financières. La loi Gramm-Leach-Bliley (GLB) exige des entreprises définies comme "institutions financières" qu'elles assurent la sécurité et la confidentialité des informations sensibles. Étant donné que les concessionnaires louent et prêtent (même par l'intermédiaire d'un tiers), ils doivent respecter la loi GLBA.
    - La règle de sauvegarde a été publiée par la Commission fédérale du commerce (FTC), dans le cadre de la loi GLB. La règle de sauvegarde exige des institutions financières qu'elles mettent en place des mesures pour assurer la sécurité des informations sur les clients.
    - Pour plus d'informations sur ces législations et les exigences, veuillez consulter le site :http://www.ftc.gov/privacy/privacyinitiatives/glbact.html https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

- Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)

- PCI DSS est une norme mondiale de sécurité de l'information assemblée par le Conseil des normes de sécurité de l'industrie des cartes de paiement (PCI SSC). La norme a été créée pour aider les organisations qui traitent les paiements par carte à prévenir la fraude par carte de crédit grâce à des contrôles accrus des données et de leur exposition aux compromis.
- Tous les commerçants qui stockent, acceptent, traitent et/ou transmettent des données sur les titulaires de cartes doivent se conformer aux exigences techniques et opérationnelles définies par le PCI DSS. Tous les concessionnaires doivent adhérer à la norme PCI DSS. Toutefois, les exigences en matière de rapports et d'audit diffèrent d'un concessionnaire à l'autre, en fonction du niveau du commerçant. Le niveau du commerçant est déterminé par le nombre de transactions par carte de crédit effectuées chez le concessionnaire. Pour plus d'informations sur la norme PCI DSS et ces exigences, veuillez consulter le site : https://www.pcisecuritystandards.org

- Ressources supplémentaires
  - Les organisations suivantes disposent d'informations pour aider à mettre en œuvre des garanties appropriées pour les données :
    - Le Centre de ressources sur la sécurité informatique - Institut national des normes et de la technologie (NIST) - http://csrc.nist.gov
    - Stratégie nationale de sécurisation du cyberespace, ministère de la sécurité intérieure- http://www.dhs.gov/files/publications/editorial_0329.shtm
    - The SysAdmin, Audit, Network, Security (SANS) Institut des vingt vulnérabilités de sécurité Internet les plus critiques - www.sans.org/top20
    - Équipe de préparation aux urgences informatiques des États-Unis (US CERT) - www.us-cert.gov/resources.html
    - Institut de génie logiciel Carnegie Mellon Centre de coordination du CERT- www.cert.org

2.6.f Sécurité des réseaux

Les concessionnaires doivent se concentrer sur la sécurité et l'intégrité des données du réseau local (LAN) de la concession. Cela commence par des politiques sur l'utilisation du réseau pour les employés et les invités. Ces politiques doivent inclure les données auxquelles chaque utilisateur a accès, les ressources du réseau auxquelles chaque utilisateur peut accéder et l'endroit où les données sont stockées sur le réseau. Les politiques doivent également indiquer délibérément sur quels appareils les données de l'entreprise sont stockées. Voir la section 2.6.a pour plus de conseils sur les politiques et pratiques de sécurité.

Au-delà des politiques, le réseau doit être configuré et segmenté de la manière la plus sûre possible pour éviter tout accès indésirable. Utilisez les recommandations suivantes lors de la configuration et de la sécurisation du réseau de concessionnaires.

Recommandation	Spécification
Firewall/ UTM	Un dispositif de sécurité entièrement géré qui surveille en permanence les menaces par le biais du système de détection des intrusions "IDS", du système de prévention des intrusions "IPS" et d'autres mécanismes. Le dispositif doit également présenter les caractéristiques suivantes : • Mécanismes tels que le filtrage de paquets, l'antivirus et l'inspection des paquets par état • Filtrer les paquets et les protocoles (par exemple, IP, ICMP) • Analyse antivirus • Effectuer une inspection officielle des connexions • Effectuer des opérations par proxy sur des demandes sélectionnées • Signaler régulièrement (c'est-à-dire tous les mois) le trafic autorisé et refusé par le dispositif de sécurité En raison de l'importance du firewall, et du fait qu'il se trouve souvent dans le chemin de données de la plupart du trafic des concessionnaires, STAR recommande un dispositif de sauvegarde en cas de panne. Pour limiter les temps d'arrêt, les concessionnaires devraient envisager une solution de basculement automatique vers le dispositif de sauvegarde en cas de défaillance matérielle.
Segmentation des réseaux	Les informations relatives aux cartes de paiement, les informations sur les clients, le trafic de la concession et le trafic des clients doivent être segmentés via une segmentation du réseau (comme le VLAN) ou 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 être due au fait que des employés naviguent sur le web pour des activités non professionnelles. STAR recommande aux concessionnaires de filtrer les contenus sur le réseau pour éliminer tout trafic potentiellement dangereux, inapproprié ou autre trafic non lié à l'activité professionnelle.
Gestion des événements liés à la sécurité (SIEM)	Une solution SIEM offre une visibilité au-delà de la protection AV ou du firewall. Le but ultime d'une solution SIEM est de collecter et d'inspecter le trafic de sécurité du réseau pour trouver des indications de compromission. Cette indication doit être envoyée, sous forme d'alerte, à une ressource qualifiée pour mener immédiatement une enquête et des mesures correctives éventuelles. Il est important de noter que l'adoption d'un logiciel SIEM ne suffit pas à elle seule à protéger le réseau de distributeurs. Les concessionnaires doivent avoir des processus et des ressources en place pour répondre aux informations générées par la technologie SIEM. Voici les orientations générales pour la gestion des informations de sécurité des concessionnaires. Les concessionnaires doivent avoir : • Une surveillance proactive des événements en temps réel qui utilise un service SIEM. • La SIEM doit pouvoir collecter des données avec la possibilité d'agréger et de corréler en temps réel les différentes données de sécurité du réseau. • Le fournisseur de services SIEM doit être en mesure d'informer l'administrateur du réseau en cas d'événement de sécurité et de fournir la documentation appropriée à des fins de conformité. • Le but ultime d'un service SIEM est d'aider à identifier ou à prévenir une intrusion dans votre réseau. Une réponse immédiate à une violation peut réduire ou prévenir considérablement la perte de données. **Remarque** : il ne faut pas confondre un logiciel de gestion réactif (c'est-à-dire un firewall ou un antivirus de bureau) avec un service SIEM proactif.
Test de pénétration et analyse de vulnérabilité	Il est fortement recommandé de procéder à un test de pénétration interne et externe annuel du réseau de concessionnaires. Un test de pénétration ("pen test") est une méthode d'évaluation de la sécurité d'un système ou d'un réseau informatique en

	simulant une attaque provenant d'une source malveillante. Un test d'intrusion doit être effectué sur tout système informatique devant être déployé dans un environnement en réseau, en particulier sur ceux dont le système est connecté à Internet ou exposé. Le test de pénétration peut être effectué en externe (simulation d'une attaque depuis l'extérieur de votre réseau et exactement comme une tentative de piratage lancée depuis un pays étranger), ou il peut être effectué en interne (depuis l'intérieur de votre réseau pour voir quels accès et quelles vulnérabilités existent).
Partenaires d'intégration certifiés	Assurez-vous que les intégrateurs de données des concessionnaires sont certifiés pour les applications DMS et OEM. Les points d'intégration non autorisés ou hostiles sont souvent moins sûrs et exigent parfois que le concessionnaire partage les informations relatives aux utilisateurs et aux mots de passe.
Système de détection sans fil	Scannez, identifiez et supprimez tout point d'accès sans fil malveillant qui pourrait se trouver sur le réseau du détaillant. Un point d'accès sans fil malveillant est défini comme un point d'entrée sans fil dans le réseau du concessionnaire qui n'est pas autorisé, sécurisé ou connu des services informatiques, de la direction et des propriétaires du concessionnaire. Tous les réseaux sans fil malveillants 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 à la recherche de menaces sans fil.

2.6.g Sécurité des ordinateurs de bureau

Recommandation	Spécification
Surveillance des virus informatiques	Des produits antivirus de qualité professionnelle doivent être installés sur tous les PC et configurés pour effectuer automatiquement les opérations suivantes : • Télécharger et installer les mises à jour les plus récentes des signatures de virus • Surveiller activement les virus • Mettre en quarantaine et éradiquer les fichiers infectés • La solution antivirus doit comprendre un antivirus, un antispyware, la prévention des intrusions, le contrôle des applications, le contrôle du spam et la détection des rootkits
Gestion des patchs	STAR recommande que la gestion des patchs soit effectuée sur chaque PC afin de s'assurer que chaque poste de travail dispose des patchs Microsoft actuels. La gestion des postes de travail doit inclure la surveillance à distance des défaillances matérielles/logicielles, des serveurs en panne, du manque d'espace disque, de l'utilisation excessive des processeurs et de la mémoire.
Protection par mot de passe	Les mots de passe doivent expirer tous les 60 jours ou moins. Les concessionnaires devraient utiliser des "mots de passe forts" contenant un minimum de 8 caractères et comprenant 3 des 4 exigences suivantes 1) Majuscules 2) Minuscules 3) Caractères numériques 4) Caractères spéciaux
Plateforme de détection et de réponse aux points terminaux	• Une plateforme unique de protection des points d'extrémité (EPP) et une solution de détection et de réponse des points d'extrémité (EDR) devraient être déployées sur les dispositifs d'extrémité afin de prévenir les attaques de logiciels malveillants basées sur des fichiers, de détecter les activités malveillantes et de fournir les capacités d'investigation et de correction nécessaires pour répondre aux incidents de sécurité et aux alertes dynamiques. Il convient de répondre immédiatement aux alertes de ce service afin d'atténuer les risques et les pertes potentielles de données. L'offre de service devrait fournir une visibilité multiplateforme des activités des points finaux/serveurs ainsi que : Détection des menaces par des moteurs d'IA statiques et comportementaux et des HIDS dans le dispositif du point terminal. • Confinement de la menace et orientation en matière d'assainissement • Rapports d'activité et chasse aux menaces • Visibilité multiplateforme sur l'exécution des processus, les communications réseau, l'accès aux fichiers, les applications, les demandes DNS et le trafic web crypté

2.6.h Sécurité du courrier électronique

Vue d'ensemble : La sécurité du courrier électronique est un risque critique pour bon nombre des plus grandes organisations du monde. Aujourd'hui, 91 % de toutes les attaques réussies sur les réseaux d'entreprise impliquent l'utilisation du courrier électronique. Une solution de sécurité du courrier électronique permettra d'inspecter le contenu entrant et sortant, de le crypter et de donner des alertes de sécurité pour atténuer bon nombre de ces risques.

Sécurité du courrier électronique sortant : Identifier et répondre aux logiciels malveillants, aux courriels inappropriés, aux contenus non autorisés et aux informations privées de l'entreprise avant qu'ils ne quittent le réseau.

Sécurité du courrier électronique entrant : Appliquer des filtres pour arrêter les logiciels malveillants, le phishing ou les courriels malveillants avant d'entrer sur le réseau.

Cryptage : Le cryptage du courrier électronique TLS est recommandé pour rendre plus difficile la lecture des courriers électroniques en transit par des tiers.

2.6.i Sécurité des applications

Ci-dessous, supposons que toutes les applications soient acquises auprès de fournisseurs externes et déployées soit sans aucune modification, soit en appliquant seulement une petite personnalisation. En outre, par application, on entend les applications commerciales et la sécurité de l'application consiste à s'assurer que toutes les données traitées - et toutes les fonctions commerciales offertes par l'application - sont protégées de manière appropriée.

- Domaines et activités principales
  - Effectuer un inventaire des applications. Documentez les applications qui se trouvent sur le réseau de concessionnaires, leur objectif, les personnes responsables et la manière d'obtenir de l'aide. Effectuer une analyse de l'impact sur les entreprises (BIA), y compris la classification des informations, pour comprendre la criticité des entreprises et appliquer un ordre de priorité correct. Ce catalogue aidera également à trouver et à éliminer les applications malveillantes qui peuvent devenir une menace pour le réseau de concessionnaires et la sécurité des données.
  - Protéger les informations traitées en transit et en 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. Examiner les intégrations d'application à application ainsi que les applications de communication interne, en particulier les connexions à la base de données, qui sont très souvent oubliées. Si nécessaire, assurez-vous que la protection en stockage est assurée par une cryptographie correcte. Enfin, assurez-vous que les flux d'informations sont protégés de bout en bout.
  - Envisager des exigences supplémentaires pour les entreprises, telles que l'authenticité, la non-répudiation ou la traçabilité, souvent requises pour respecter les réglementations relatives à la protection de la vie privée (par exemple, GDPR).
  - Appliquer le principe de la défense en profondeur en introduisant une configuration précise des zones de sécurité et le placement des composants d'application, des services d'infrastructure supplémentaires comme les reverse proxies ou les firewalls d'application web, et des couches de contrôle d'accès comme l'authentification multifactorielle, etc.
  - Introduire la stratégie appropriée de gestion des identités et des accès (voir plus dans la section IAM). Appliquer les principes du moindre privilège et du besoin de savoir.
  - Attendez d'un fournisseur le résultat d'une analyse de vulnérabilité des applications effectuée par une société tierce indépendante. Veillez à ce que tous les risques élevés et moyens 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 avec le niveau de qualité attendu. Ainsi, on peut s'attendre à ce qu'une entreprise fournisse des résultats de tests ou des rapports d'audit.
  - Introduire des processus de traitement des incidents, des demandes d'accès, etc. Envisagez d'introduire une surveillance des applications commerciales afin de retracer ou même de prévenir les événements indésirables. Cela fait

généralement partie de la mise en œuvre d'une gestion des services informatiques.
    - Effectuer régulièrement des activités de modélisation des menaces pour s'assurer que les risques liés au paysage applicatif sont documentés, atténués et maîtrisés.
    - Appliquer les mises à jour et les correctifs de l'application dès que possible afin de limiter l'exposition à d'éventuels exploits.

2.6.j Mobilité

Ce domaine est fortement lié à d'autres domaines comme la sécurité des applications ou la sécurité du courrier électronique. Cependant, il est considéré séparément en raison des risques supplémentaires qu'il introduit par un contrôle beaucoup moins strict des types de dispositifs définis. Les appareils mobiles sont définis ici comme les smartphones, les tablettes, les ordinateurs portables et tout autre appareil spécialisé qui traite ou stocke des données d'entreprise.

- Domaines et activités principales
    - Créer des politiques et des procédures pour savoir qui, quand et comment accéder à distance à l'environnement de l'entreprise et à quelles parties (réseau, serveurs, applications, etc.). Par exemple, une politique peut permettre aux smartphones et aux tablettes d'accéder à un réseau externe de l'entreprise et restreindre l'accès au réseau interne de l'entreprise ; et permettre l'accès au réseau interne de l'entreprise pour les ordinateurs portables gérés via un réseau privé virtuel (VPN). Déployer une solution technique appropriée pour soutenir l'approche établie.
    - Définissez les informations qui peuvent être traitées et stockées sur les appareils mobiles ; assurez-vous d'inclure les considérations liées aux appareils gérés et non gérés.
    - Introduire des politiques, des procédures et des capacités techniques pour définir quels logiciels peuvent être installés et exécutés sur tous les types d'appareils mobiles. Dans le cas des appareils non gérés, introduire des conditions dans lesquelles les données de l'entreprise ne sont pas exposées à des risques inacceptables (par exemple, en installant des solutions comme MobileIron ou Microsoft iTunes pour les smartphones).
    - L'accès aux dispositifs devrait être restreint, ce qui nécessite une authentification de l'utilisateur. La plupart des appareils peuvent être verrouillés à l'aide d'un verrou d'écran, d'un mot de passe ou d'un code PIN.
    - Appliquer la stratégie appropriée de gestion des identités et des accès.
    - Assurez-vous de la bonne configuration et du bon renforcement du dispositif et du système d'exploitation (par exemple, mot de passe du BIOS, cryptage au niveau du dispositif, disponibilité des ports USB et SD). Assurez-vous (en particulier dans le cas des appareils Android et iOS) que l'appareil n'est pas "rooté" et jailbreaké.
    - Gardez un logiciel anti-programmes malveillants à jour et, de préférence, géré de manière centralisée sur les ordinateurs portables et les smartphones.
    - Mettez à jour le système d'exploitation mobile avec des correctifs de sécurité. Pour plus d'informations sur la gestion des correctifs, voir la section 2.6.c.
    - Appliquer un cryptage approprié des données à la fois sur les ordinateurs portables et les appareils mobiles en accordant une attention particulière à la gestion des clés pour le décryptage.
    - Examinez toutes les méthodes de connectivité, en faisant attention à la connectivité sans fil automatisée, car les mots de passe peuvent être exposés et des attaques de type "man-in-the-middle" peuvent être exécutées.
    - Activez l'option d'effacement des données à distance si elle est disponible.
    - Sauvegardez régulièrement l'appareil mobile.

2.7 Fournisseurs de services gérés

Les concessionnaires se tournent souvent vers des vendeurs ou des partenaires pour les aider à gérer, entretenir et sécuriser l'infrastructure de la concession. Un prestataire 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 de concessionnaires. Les concessionnaires n'ont souvent pas le temps, les ressources ou l'expertise nécessaires pour gérer seuls un réseau d'entreprise. Par conséquent, le recours à un prestataire de services pourrait être un choix logique.

Un accord de niveau de service (SLA) est très important lors de la sélection d'un tiers pour l'assistance à l'infrastructure du réseau. Le fournisseur s'engagera sur le niveau de service à attendre, l'étendue du ou des services, et tout remboursement ou frais compensatoires pour les engagements manqués.

La section suivante fournit quelques conseils pour la sélection et la compréhension des accords sur le niveau de service.

2.7.a Accords sur les niveaux de service (SLA)

Les concessionnaires qui reçoivent des services informatiques accordent une grande confiance à l'accord de niveau de service (SLA) qu'ils sélectionnent. Le SLA détaillera la qualité de service (QoS) que le fournisseur offre avec son service - en d'autres termes, sa garantie que le service sera livré comme promis.

Les SLA sont utilisés dans une grande variété de services informatiques de concessionnaires qui comprennent (mais ne sont pas limités à) :

- Service Internet
- Services d'intégration de réseaux
- Services d'assistance pour le matériel et les logiciels
- Assistance sur place
- Service d'assistance et centre d'appel

Lorsque vous choisissez un fournisseur de services, assurez-vous de poser les questions suivantes concernant les accords de niveau de service.

- Existe-t-il un SLA écrit ?
- Quels sont les revers, remboursements ou autres conséquences si le fournisseur ne respecte pas son SLA ?
- Existe-t-il des rapports sur le SLA ?
- Le service peut-il être annulé si le SLA n'est pas respecté ?

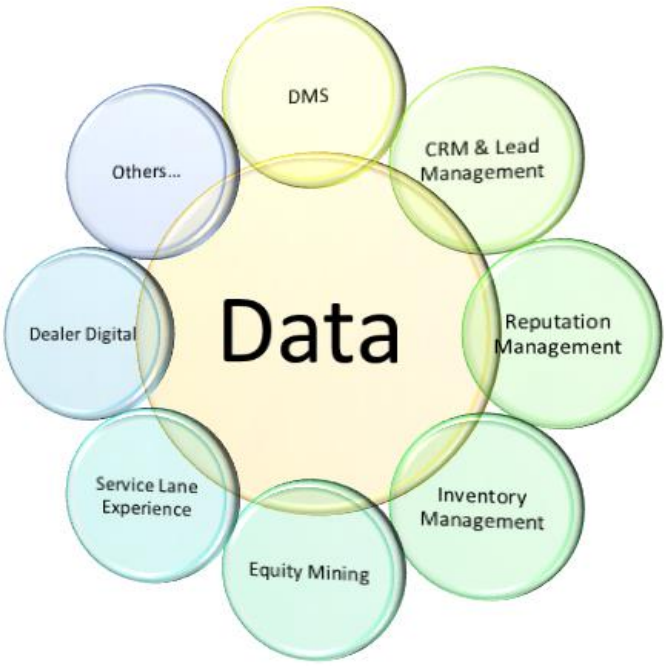
Les SLA courants comprennent (mais ne sont pas limités à) :

- Disponibilité du réseau
- Vitesse du réseau
- Latence du réseau
- Délai de remplacement du matériel
- Heures d'assistance disponibles
- Engagements de service sur site
- Accords de maintenance du matériel ou des logiciels

3. Fournisseurs de systèmes de concessionnaires

3.1 Vue d'ensemble

La complexité d'une concession et de la technologie qui lui est associée a beaucoup évolué depuis la création de STAR. Cette technologie en constante évolution a continué à renforcer la valeur commerciale globale de STAR et les normes d'intégration utilisées pour aligner les données entre les systèmes et les processus.



Si le système de gestion des concessionnaires (DMS) 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 que les clients, les véhicules et les pièces peuvent être gérés efficacement tout au long du trajet en ligne et hors ligne. L'écosystème du fournisseur de services aux concessionnaires (DSP) est en constante évolution et il est absolument essentiel de veiller à ce que des processus soient mis en œuvre pour une intégration des données sûre et efficace.

Les choix du DSP évoluent de jour en jour et il est essentiel que les concessionnaires comprennent l'importance d'une intégration de données sûre et efficace. Il existe des solutions DSP qui se concentrent sur l'amont de la concession et d'autres qui se concentrent sur l'aval. D'autres solutions visent à gérer les clients de l'Internet au hors ligne et certaines cherchent spécifiquement à aider les concessionnaires dans le marchandisage des stocks de véhicules neufs/usagés, la gestion et la distribution de contenu, ou à maintenir une image positive dans les médias sociaux et le monde en ligne.

Que l'on travaille avec un vendeur qui propose de nombreux produits ou qui se spécialise dans une capacité spécifique, il est important de s'assurer de comprendre comment les données seront intégrées et gérées dans l'ensemble de l'écosystème.

Il n'existe pas d'approche unique pour la mise en œuvre d'une solution DSP pour une concession, mais il est essentiel d'aligner les technologies avec les professionnels de l'entreprise et de mettre en œuvre des processus de gouvernance des données qui soutiennent l'expérience client souhaitée. Les clients s'attendent de plus en plus à une expérience en ligne et hors ligne transparente, qui ne peut être obtenue que par l'intégration des données.

Le concessionnaire dispose d'un grand nombre de choix pour décider quels DSP seront utilisés dans le cadre de son réseau. Les DSP servent souvent de "plaque tournante" pour les données, les communications et les opérations commerciales des concessionnaires. Lors de l'examen des différentes offres de DSP, la section Infrastructure du réseau de concessionnaires de STAR DIG peut fournir des conseils sur les différentes fonctions qu'un fournisseur de services système peut offrir aux concessionnaires.

3.2 Intégration des données et normes : L'avantage STAR

La société STAR et les normes d'intégration qu'elle contient ont été créées pour optimiser les activités d'intégration des données des concessionnaires entre l'OEM et le DSP (principalement le DMS au début) en utilisant l'Internet comme principal moyen.

Comme toute technologie, Internet a continué à évoluer et l'infrastructure utilisée pour faire fonctionner les entreprises qui l'utilisent a fait l'objet d'un grand nombre d'innovations. Ces améliorations ont abouti à une méthode extrêmement fiable pour intégrer les processus d'entreprise et les systèmes associés.

Au cœur de tous ces systèmes se trouvent les données nécessaires pour soutenir le processus commercial souhaité. Les données relatives aux véhicules, aux pièces détachées, aux clients, au service après-vente, aux finances et de nombreux autres groupes de données doivent passer d'un système à l'autre - et entre le concessionnaire (avec le DSP) et l'OEM - de manière transparente et sécurisée. Les normes d'intégration de données STAR sont des normes ouvertes qui permettent aux fournisseurs et aux OEM 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 (BOD - Business Object Documents).

Au fil du temps, ces BOD peuvent être enrichis de définitions/règles commerciales et alignés sur diverses méthodologies de transport de données afin de fournir des intégrations de données efficaces et reproductibles. Lorsque STAR a commencé ce voyage important, l'écosystème était beaucoup plus simple. Le paysage technologique des distributeurs se compliquant d'année en année, les normes commenceront vraiment à montrer les avantages de STAR !

3.3 Paysage technologique des concessionnaires (Choix DSP)

Il semble que le paysage technologique des concessionnaires sera en constante évolution dans un avenir prévisible. Passer du temps à essayer de définir ce paysage ne ferait qu'aboutir à un document qui deviendrait obsolète peu après sa publication.

Ces dernières années, plusieurs catégories de produits DSP nouvelles et importantes ont rejoint le DMS traditionnel et se sont imposées de façon permanente dans l'écosystème de la vente au détail de produits automobiles. Il est donc utile de fournir quelques informations sur leur contexte. Comme pour tous les choix de DSP, il faut prendre le temps de comparer les capacités et de s'assurer que la solution est conforme aux lignes directrices de l'infrastructure STAR.

En plus de comparer les capacités et de comprendre l'intégration globale, il est extrêmement important de comprendre la gestion des données et les éléments d'acceptation et de refus associés à la solution. Une gouvernance complète des données et une transparence de l'utilisation sont cruciales pour toute solution DSP/OEM.

3.3.a DMS

Le système de gestion des concessionnaires (DMS) est un système d'information de gestion groupé créé spécifiquement pour les concessionnaires automobiles de l'industrie automobile. Il a été adapté (généralement sous la forme d'un produit DMS spécialisé) pour les concessionnaires d'équipements lourds, de bateaux, de motos, de véhicules de loisirs et d'équipements de sports motorisés. Le DMS contient des fonctionnalités permettant de prendre en charge les finances, les ventes, les stocks, les pièces détachées, le service et la comptabilité/le bureau d'affaires pour le fonctionnement de la concession.

Certaines solutions DMS sont proposées avec des serveurs centraux sur site, et d'autres tirent parti du "cloud" en utilisant un modèle de logiciel-service (SaaS) ; une solution sur site ou basée sur le SaaS pourrait convenir, selon les besoins de la concession. Une considération importante est la maintenance du matériel utilisé pour répondre aux besoins des applications. Les services SaaS sont générés dans le nuage et ne nécessitent pas beaucoup de maintenance, tandis que les solutions sur site nécessitent souvent la gestion des correctifs, des mises à jour et la maintenance générale du serveur.

Bien que les fonctionnalités générales des deux solutions soient similaires d'un DMS à l'autre, les capacités spécifiques peuvent varier. Dans tous les cas, il est essentiel de s'assurer que la solution prendra en charge les réglementations de l'État, de la localité, du marché ou de la région, ainsi que les marques OEM pour le groupe spécifique de concessionnaires.

3.3.b CRM et gestion des prospects

Les systèmes de gestion des relations avec la clientèle (CRM) et de gestion des prospects sont utilisés pour saisir, suivre et gérer efficacement la correspondance en ligne et hors ligne avec les prospects et les clients.

Les solutions de CRM et de gestion des prospects nécessitent une intégration avec les données du DMS (clients) et toutes les sources de prospects.

Le système CRM offre des fonctionnalités qui aident le personnel de la concession à gérer la relation client tout au long du cycle de vie du client. Les dates clés des clients et des véhicules, les rendez-vous de service et de nombreux autres aspects peuvent tous être gérés.

Le système de gestion des prospects offre une fonctionnalité permettant d'attribuer des prospects au personnel de vente et de service (ou par l'intermédiaire d'un centre de développement commercial défini) pour le suivi. Ces activités de suivi des prospects ont toutes pour but d'augmenter les ventes et les revenus.

Les prospects (enquêtes) sont recueillis et stockés à partir de nombreuses sources différentes, notamment mais pas exclusivement :

- Les visites à pied ou en voiture
- Acheter des prospects en ligne
- Prospects fournis par les OEM
- Les prospects par téléphone
- Prospects dans des événements

Les solutions de CRM et de gestion des prospects sont également mises à profit pour générer de nouvelles affaires. En alignant les solutions des concessionnaires sur les manifestes des équipementiers, les autres solutions DSP (par exemple, Equity Mining) et les besoins en matière de voitures d'occasion, il est possible d'atteindre efficacement les clients existants et de créer de nouvelles activités.

Les concessionnaires ont besoin de l'infrastructure en place pour soutenir les clients potentiels des entreprises de niveau 3. Une solution efficace de gestion des pistes 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 pour vous aider à surveiller, comprendre, identifier et traiter ce que les gens écrivent en ligne sur votre concession.

Une solution de gestion de la réputation nécessite une intégration avec les DMS et les sources de données des OEM.

La réputation en ligne d'une concession est définie par les commentaires que l'on trouve sur les sites d'évaluation des clients, les blogs, les sites web et les sites de médias sociaux. L'internet permet de trouver facilement des informations sur une concession sans trop d'efforts. En quelques clics, un client a un aperçu de ce qu'est une concession, de son emplacement et de ce que les clients pensent de la concession dans son ensemble. Dans la plupart des cas, les

résultats de la recherche comprennent des étoiles et des commentaires. Ces évaluations et avis influencent la décision d'un client d'acheter un véhicule chez un concessionnaire.

3.3.d Gestion de stocks en ligne

Une solution de gestion de stocks pour les concessionnaires offre des fonctionnalités permettant le marchandisage, la gestion du contenu et la distribution des stocks de véhicules. Cela comprend la distribution par le concessionnaire des stocks de véhicules neufs ou d'occasion sur le web et/ou dans des publications imprimées, ainsi que des photos de véhicules, des visites vidéo, des prix, des incitations, etc.

Une solution de gestion des stocks des concessionnaires nécessite des intégrations avec le DMS, des outils de tarification tiers, des fournisseurs de services de lot, des fournisseurs de services de description des véhicules (validation du VIN et données de construction) et des OEM.

3.3.e Equity Mining

Une solution Equity Mining offre une fonctionnalité permettant d'identifier les consommateurs qui ont des capitaux propres dans leur véhicule et de les proposer ensuite comme clients potentiels via un centre de développement commercial (BDC), un gestionnaire Internet, une équipe de vente ou d'autres représentants de concessionnaires appropriés.

Une solution d'Equity Mining nécessite une intégration avec les données DMS (clients), CRM/LM (prospects), les sources de reprise, les données bancaires (financement et crédit-bail) et les mesures d'incitation.

3.3.f Outils pour les voies de service

Les outils de voie de service sont une solution basée sur des processus ou des flux de travail qui englobe des fonctionnalités que l'on retrouve traditionnellement dans des solutions distinctes liées aux services (c'est-à-dire DMS, la programmation des services en ligne, les menus de service, les contrôles de santé des véhicules, etc.). Elle permet une expérience client cohérente et sans faille à travers les étapes suivantes : 1) prise de rendez-vous, 2) rédaction du contrat de service, 3) véhicule en service et 4) nouvelle prestation de service.

L'outil de voie de service nécessite une intégration avec les sources de données des DMS et des OEM.

3.3.g Concessionnaire numérique

Un paquet de marketing numérique pour les concessionnaires est une suite de services de marketing de détail qui permet aux concessionnaires de fournir des messages cohérents et synchronisés aux consommateurs en utilisant les canaux numériques et émergents. Il fournit une plate-forme de marketing de réseau intelligente avec un alignement du marketing de la marque et du concessionnaire. Il fournit également des analyses permettant d'optimiser les dépenses de marketing à plusieurs niveaux et d'améliorer les performances du réseau de concessionnaires dans les processus de marketing et de vente.

Les solutions numériques des concessionnaires nécessitent une intégration avec les sources de données de DMS, de CRM et des OEM.

Les composants principaux d'une solution concessionnaire numérique peuvent inclure :

- Site web du concessionnaire (Web et mobile)
- Optimisation des moteurs de recherche (SEO)
- Gestion de l'audience
- Perspectives et analyses
- Gestion des actifs (images, vidéos, etc.)

- Chat
- Nominations

4. Reprise après sinistre et continuité des activités

4.1 Vue d'ensemble

La reprise après sinistre et la continuité des activités est la capacité d'une organisation à se remettre d'un sinistre et à reprendre le fonctionnement normal du réseau. Les concessionnaires doivent disposer d'un plan détaillant la technologie, les processus et les procédures à suivre en cas de panne. La clé d'une reprise après sinistre réussie est de disposer d'un plan bien avant que la panne ne se produise.

La reprise après sinistre et la planification de la continuité des activités sont des processus qui aident les entreprises à se préparer à des événements perturbateurs - qu'il s'agisse d'une tornade dévastatrice ou simplement d'une ligne Internet rompue par des gelées et dégels répétés.

Pour comprendre ce qui pourrait se passer en cas de panne de réseau, il est recommandé aux concessionnaires de comprendre d'abord quelles données sont en danger. Combien de temps ces données peuvent-elles être indisponibles ? Que se passe-t-il lorsqu'elles sont indisponibles ? Quelles mesures peuvent être prises pour s'assurer que le risque est atténué ? Cette section fournit des réponses de base à ces questions ainsi que des recommandations pour la planification avant la panne et la restauration des opérations du réseau.

4.2 Analyse et atténuation des risques

Le principal objectif de l'analyse des risques est d'aider le concessionnaire à identifier tous les domaines pour lesquels il peut y avoir un risque de perte. Il peut s'agir de matériel, de logiciels, de bâtiments, de personnel, etc. Après avoir identifié les différents éléments, le concessionnaire peut classer le niveau de chaque risque et déterminer comment ce risque affecte le concessionnaire.

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

- Personnel clé
- Bâtiment
- Défaillance du système de clés
- Défaillance totale du système
- Pert de données

Une entreprise peut atténuer les risques de diverses manières. Ces plans ou solutions peuvent être mis en œuvre sur place ou hors site. Voici quelques exemples de chacune d'entre elles.

Options d'atténuation des risques sur site	Options d'atténuation des risques hors site
Matériel redondant	Logiciel de sauvegarde à distance
Logiciels et serveurs de sauvegarde des données sur site	Stockage dans le Cloud
Alimentation sans interruption (UPS)	Contrats de service pour le matériel RMA
Générateurs	

5. Informatique en Cloud et virtualisation

5.1 Vue d'ensemble

Les tendances émergentes importantes dans le domaine des technologies de l'information peuvent être résumées comme un paradigme basé sur les services et la virtualisation. Avec un "paradigme basé sur les services", nous condensons différents acronymes tels que l'architecture orientée services (SOA) et le concept populaire d'informatique en Cloud (qui a des implications commerciales pertinentes). *"La principale technologie habilitante pour l'informatique en Cloud est la virtualisation. La virtualisation fournit l'agilité nécessaire pour accélérer les opérations informatiques et réduit les coûts en augmentant l'utilisation de l'infrastructure"*. (Wikipédia)

5.2 Virtualisation client/serveur

La virtualisation, en informatique, signifie créer une version virtuelle d'un dispositif ou d'une ressource comme un serveur, un dispositif de stockage, un réseau, etc. où le "cadre" divise la ressource en un ou plusieurs environnements d'exécution. Les applications et les utilisateurs humains sont en mesure d'interagir avec la ressource virtuelle comme s'il s'agissait d'une ressource physique réelle et unique. Dans un environnement de revendeur, les domaines les plus pertinents pour la virtualisation sont la virtualisation de serveur et la virtualisation de client ; les deux sont intéressants et assurent des économies constantes.

5.3 Informatique en Cloud

"Informatique en Cloud est un modèle qui permet un accès réseau omniprésent, pratique et à la demande à un ensemble partagé de ressources informatiques configurables (par exemple, réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement approvisionnées et libérées avec un minimum d'effort de gestion ou d'interaction avec le fournisseur de services". (Définition du NIST - Institut national des normes et de la technologie)

Informatique en Cloud repose sur le partage des ressources pour réaliser des économies d'échelle, comme dans le cas d'un service public (comme le réseau électrique), sur un réseau. À la base due l'Informatique en Cloud se trouve le concept plus large de services partagés et standardisés, exploités avec un modèle de consommation.

Selon le NIST, le modèle de l'Informatique en Cloud est composé de trois modèles de services de base.

- Logiciel-comme-Service (SaaS) : la possibilité offerte au consommateur d'utiliser les applications du fournisseur fonctionnant sur une infrastructure en Cloud.
- Plateforme-comme-Service (PaaS) : la capacité fournie au consommateur de déployer sur l'infrastructure en Cloud des applications créées par le consommateur ou acquises en utilisant des langages de programmation, des bibliothèques, des services et des outils pris en charge par le fournisseur.
- Infrastructure-comme-Service (IaaS) : la capacité fournie au consommateur de fournir le traitement, le stockage, les réseaux et d'autres ressources informatiques fondamentales où le consommateur est capable de déployer et d'exécuter des logiciels arbitraires, qui peuvent inclure des systèmes d'exploitation et des applications.

Le courrier électronique et la gestion des relations avec la clientèle sont déjà utilisés par de nombreux distributeurs avec un modèle SaaS. De nombreux fournisseurs de DMS proposent déjà quelque chose de similaire à un modèle SaaS pour leur DMS. Les deux autres modèles sont rarement adoptés par les revendeurs - à quelques exceptions près (par exemple, l'IaaS pour la reprise après sinistre est une option intéressante).

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

De nombreux experts affirmeront que la plupart des violations de données sont dues à des erreurs humaines. Au cours des années précédentes, des études menées par Nuspire Networks, IBM, Verizon et le 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 employés sont souvent la cause de pannes de réseau, de défaillances d'appareils et de ralentissement des opérations commerciales. La plupart du temps, la cause fondamentale n'est pas un mauvais employé, mais plutôt une formation et une documentation déficientes. Souvent, les employés signalent un incident de sécurité, ne savent pas comment utiliser les systèmes et/ou provoquent une panne de réseau parce qu'ils n'ont pas été formés sur ce qu'il faut faire ou ne pas faire. Ce manque de formation des employés peut souvent conduire 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 concessionnaires sont encouragés à adopter des politiques et des procédures de formation. Ces politiques doivent être bien documentées et utilisées avec la formation des employés. La documentation, le processus et la procédure peuvent à eux seuls avoir un impact positif sur les opérations du réseau et la sécurité des données des concessionnaires.

6.1 Formation des employés

Recommandation	Spécification
Formation à la sécurité	Disposer d'un programme de formation officiel et écrit sur la sécurité pour chaque employé. La formation doit couvrir des aspects tels que la sensibilisation à l'ingénierie sociale, la gestion des mots de passe, les politiques de partage des données et les procédures de traitement des données sensibles. Revoir régulièrement les programmes de formation et les adapter en fonction des nouvelles technologies, de l'évolution de l'activité des concessionnaires et des commentaires des employés.
Conception de la responsabilité en matière de sécurité	Désigner un employé comme coordinateur de programme pour votre programme de sécurité de l'information.
Formation aux systèmes informatiques des concessionnaires	Offrir une formation formelle pour les applications critiques, le matériel et les autres systèmes informatiques des concessionnaires. Un employé bien informé peut augmenter la productivité, réduire les coûts de support et améliorer la satisfaction des clients.

6.2 Processus

Recommandation	Spécification
Accès des nouveaux employés	Disposer d'une procédure écrite et formelle pour accorder aux nouveaux employés l'accès au système. Cette procédure doit comprendre des noms d'utilisateur et des mots de passe uniques.
Accès des employés licenciés	Disposer d'une procédure écrite et formelle pour retirer les employés du réseau informatique du concessionnaire, récupérer le matériel du concessionnaire et désactiver tous les comptes des employés avant leur départ.
Formation aux systèmes informatiques	Disposer d'un programme formel de formation aux technologies, aux applications et au matériel informatique de la concession. Un employé bien informé peut accroître la productivité, réduire les coûts d'assistance et améliorer la satisfaction des clients.
Évaluation des risques	Identifier les risques internes et externes raisonnablement prévisibles pour la sécurité, la confidentialité et l'intégrité des informations sur les clients. Concevoir et

	mettre en œuvre des mesures de protection des clients pour contrôler les risques identifiés par l'évaluation des risques.
Contrôles de sécurité effectués par des tiers (vendeurs)	La sélection de fournisseurs de services de confiance est très importante. Sélectionnez des fournisseurs de services qui ont l'expérience de la protection des informations sur les clients d'un concessionnaire.
Traitement et réponse aux incidents de sécurité	Disposer d'un processus formel pour répondre aux incidents de sécurité sur le réseau. Couvrir les aspects relatifs à l'identification des failles de sécurité, à la réponse, à la communication et à la documentation.

6.3 Documentation

Recommandation	Spécification
Documentation sur la sécurité	Créer une politique de sécurité écrite qui aborde les normes techniques, de processus et administratives pour traiter la sécurité des données des clients. Cette documentation devrait comprendre : • La formation des employés • Réponse et gestion des incidents/infractions • Accords d'utilisation de l'internet par les employés • Politiques et procédures de surveillance et de gestion des réseaux
Documentation pour les nouveaux employés	Disposer d'un programme écrit pour les nouvelles embauches. Ce programme doit comprendre une formation à la sécurité, une formation au système et un processus documenté pour demander une assistance technique en matière d'informatique.
Documentation sur les systèmes	Mettre à disposition une formation pour les applications critiques, le matériel et les autres systèmes informatiques des concessionnaires. Un employé bien informé peut augmenter la productivité, réduire les coûts de support et améliorer la satisfaction des clients.

7. Annexes

7.1 Guide de la politique de sécurité des concessionnaires

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

Les politiques doivent refléter la stratégie de sécurisation des informations - et non l'inverse - et la compréhension des exigences de sécurité est ici le facteur clé. L'accent doit être mis sur la confidentialité, l'intégrité et la disponibilité des données et des ressources sensibles, y compris l'environnement physique, l'infrastructure de réseau, les applications et les données (physiques et numériques). Toutefois, cette liste n'est pas exhaustive, car il existe de nombreuses autres considérations. Par exemple, la non-répudiation, la traçabilité ou l'authenticité doivent souvent être prises en compte.

De plus, chaque industrie a ses propres zones sensibles. Par exemple, nous nous soucions beaucoup plus de l'intégrité - plutôt que de la confidentialité - d'un avion dans les airs 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 devraient refléter ces considérations.

Il existe de nombreuses politiques ou directives cadres de sécurité prêtes à l'emploi parmi lesquelles choisir et appliquer dans une entreprise. Toutefois, même si ce type de cadre peut fournir une base de référence générale, une entreprise devra ajuster et développer les politiques pour les appliquer dans son contexte commercial.

Directives générales

- Assurez-vous qu'il existe une compréhension commune avec la direction quant à ce qui doit être protégé ainsi qu'au niveau d'ambition concernant la protection des données. D'une part, il est important que les politiques garantissent un niveau de protection attendu. D'autre part, il est également très important que les politiques ne soient pas restrictives au point d'empêcher l'entreprise de faire les affaires dont elle a besoin.
- Veillez à ce que les politiques soient alignées sur les lois et les règlements (par exemple, dans le domaine de la protection de la vie privée ou les règlements spécifiques au secteur).
- Élaborez des politiques qui reflètent les pratiques de sécurité réelles et réalisables. Il est préférable d'avoir un petit ensemble de règles plutôt qu'un document complet impossible à suivre. Juste au cas où l'état actuel serait loin d'être ambitieux, élaborer un plan de transition accepté par toutes les parties prenantes clés pour faire passer une organisation du niveau actuel au niveau attendu. Il est très important d'élaborer un bon plan de communication dans le cadre du programme de sécurité global.
- Les politiques ne doivent pas être modifiées trop souvent (y compris la manière et la langue dans lesquelles elles sont exprimées). Toutefois, si nécessaire, des changements appropriés devraient être apportés, car ils devraient toujours refléter les exigences de sécurité et les stratégies de sécurité de l'information actuelles.
- Les politiques doivent être exprimées de manière à ce qu'il n'y ait pas de place pour les exceptions. Cela concerne à la fois l'engagement de toutes les parties prenantes à suivre les politiques et le langage. Sinon, surtout lorsque de nombreuses exceptions sont autorisées, la question peut se poser de savoir si la direction est réellement engagée dans la politique et/ou si la politique reflète réellement la stratégie de l'entreprise en matière de protection de l'information.

- Les politiques doivent être exprimées de manière à ce qu'il n'y ait pas de place pour l'interprétation. En outre, les politiques doivent être soutenues par des lignes directrices, des processus, des procédures, des rôles avec des responsabilités et des interprétations afin que l'on sache clairement ce qu'il faut faire dans des cas spécifiques. Il faut également savoir à qui s'adresser en cas de besoin d'une interprétation ou d'une décision. C'est également une bonne pratique de maintenir les articles de la base de connaissances.
- Veillez à ce que des solutions et des technologies appropriées soient disponibles pour répondre aux attentes politiques. Par exemple, lorsqu'une politique exige une authentification à deux facteurs dans des circonstances spécifiques, il est important que l'environnement informatique existant permette une mise en œuvre de ce niveau de protection supplémentaire.
- Introduisez un tableau de bord pour suivre le niveau de mise en œuvre des politiques, permettant une gestion fiable des risques ainsi qu'une hiérarchisation des efforts.

Voici des lignes directrices avec des exemples de politiques jugées particulièrement valables du point de vue des concessionnaires.

7.1.1 Politique d'utilisation acceptable

Décrit l'utilisation acceptable des ressources physiques et numériques d'une entreprise. Couvre également la propriété et le contrôle. Souligne des exemples d'activités interdites.

7.1.2 Politique de gestion des actifs

Les actifs représentent tout ce qui a de la valeur pour une entreprise. Les actifs de l'entreprise sont considérés comme des dimensions à la fois physiques et logiques.

Physique. Serveurs, disques durs, routeurs, téléphones portables, 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 élimination et à leur réutilisation.

Logique. Il est important qu'une entreprise élabore des normes régissant la collecte, la conservation et l'utilisation appropriées des données. Ces normes doivent prendre en compte les informations collectées, la durée de conservation, le mode de stockage, les personnes qui peuvent y accéder et la manière dont l'accès est obtenu. Ceci est très lié au rôle accru de la réglementation sur la protection de la vie privée dans les différents pays.

En outre, une politique de classification des informations avec des exigences claires en matière de propriété et de protection des informations à différents niveaux devrait être développée. Elle est tellement importante qu'elle est parfois considérée dans une politique distincte et identifiable.

7.1.3 Politique relative aux applications commerciales

Introduire une politique de classification des demandes d'entreprises. Décrire les exigences de protection au niveau des applications pour différents niveaux de criticité (par exemple, placement des zones de sécurité, méthodes de connectivité, contrôle d'identité et d'accès, application de la défense en profondeur, échec en toute sécurité, moindre privilège et autres principes similaires). Inclure les attentes concernant l'architecture des applications, la communication avec d'autres systèmes et la séparation des données entre les clients. Définir les attentes à l'égard des solutions basées sur le cloud (qui sont de plus en plus populaires).

D'autres aspects à préciser sont la manière dont une application est achetée par l'entreprise, les étapes obligatoires, les exigences communes envers les fournisseurs, qu'elles soient fonctionnelles ou non (par exemple, SLA, sécurité, gestion de l'identité, intégrations). Définir les audits attendus de l'application

acquise (par exemple, rapports de Pentest ou d'analyse de vulnérabilité). Soutenir les politiques à l'aide de modèles et de lignes directrices à partager avec les fournisseurs.

7.1.4 Politique de communication électronique

À l'ère technologique actuelle, les entreprises disposent de nombreuses possibilités de communication et d'échange d'informations. Toutefois, ces options comportent des risques. Par exemple, on peut utiliser un service de cloud computing pour communiquer, mais il s'agit aussi de collecter des données dans une intention malveillante. Il est important de réglementer les communications électroniques telles que les courriers électroniques et la messagerie instantanée, en utilisant des cartes comme Trello, l'échange de fichiers sur Dropbox, et des solutions et plateformes similaires.

7.1.5 Politique de gestion des identités et des accès

Un des domaines les plus critiques. Vous trouverez plus de détails dans la section correspondante de cette ligne directrice. La politique relative aux mots de passe doit être incluse dans cette section.

7.1.6 Politique de gestion des incidents de sécurité

Il n'existe pas d'environnement informatique qui puisse être sécurisé à 100 %. Une entreprise doit être prête à faire face à tout incident de sécurité. La politique de gestion des incidents de sécurité doit faire partie - ou contribuer - à la gestion globale des incidents. Elle définit un incident de sécurité, introduit des processus et des procédures (c'est-à-dire un plan d'intervention) pour savoir quoi faire en cas d'incident de sécurité (en fonction de la catégorie d'incident, par exemple piratage informatique, mauvais comportement, panne d'équipement) et de la criticité. Définir les procédures exactes de réponse 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 son identité.
- Envisagez une enquête d'expert plus approfondie.
- Envisagez des solutions d'urgence pour soutenir les plans de service et de continuité des activités.
- Envisagez de savoir qui notifier en cas d'incident, tant à l'intérieur qu'à l'extérieur de l'organisation. Les parties suivantes peuvent avoir besoin d'être informées : les consommateurs, les forces de l'ordre, les clients, les bureaux de crédit et les autres entreprises qui peuvent être touchées par la violation.
- Très souvent, il existe également des lois et des règlements qui exigent un comportement spécifique en cas de violation de données et qui dépendent du pays, de l'État et du secteur d'activité.

La politique peut également s'attendre à introduire des solutions techniques appropriées pour soutenir la mise en œuvre de la politique.

Des informations plus spécifiques sur la réponse aux incidents sont disponibles à l'adresse suivante : 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 : https://www.sans.org/score/incident-forms.

7.1.7 Politique du réseau

La politique des réseaux est un autre aspect très important de la sécurité globale. Lors de l'élaboration d'une politique de réseau, il est recommandé de prendre en considération les aspects suivants :

- Définir les classes de zones de réseau avec l'organisation de soutien (propriétaire de la zone, opérateur de la zone, etc.), attribuer un niveau de confiance à chaque classe, définir les connexions autorisées entre les différents niveaux de confiance. Introduire des segments de réseau plus restreints pour les applications et les données plus sensibles.

- Une liste des dispositifs de réseau et des configurations associées ainsi que ce qui doit être autorisé à se connecter et à quel endroit.
- Connexions réseau externes, VPN (à la fois pour les employés et les partenaires externes)
- DNS, y compris la structure de nommage ainsi que l'infrastructure de soutien et le champ d'application
- Pare-feu, reverse proxy et configurations de proxy (par exemple, tout le trafic sortant doit passer par un proxy, tout le trafic entrant sensible doit passer par le reverse proxy)
- Les classes et les normes sans fil sur l'authentification et la protection en transit. Segments séparés, spécifiques et très limités pour les clients.
- Télémaintenance
- VoIP, téléphonie et conférences

7.1.8 Politique de gestion des risques et d'audit

Définir le cadre des risques et les considérations d'audit correspondantes. Décrire les exigences en matière d'évaluation des risques et d'audit des informations et des ressources de l'entreprise.

7.1.9 Politique de gestion des menaces et des vulnérabilités

Définir les exigences en matière de protection contre les logiciels malveillants, d'enregistrement des événements de sécurité et de solution SIEM appropriée, de détection des intrusions et d'analyse des vulnérabilités. Définir le niveau d'ambition approprié pour les calendriers d'analyse ainsi que les autres systèmes de soutien ; tous doivent être liés à la gestion des risques.

Outre les exemples énumérés ci-dessus, il existe d'autres politiques et procédures de sécurité qu'une entreprise devrait envisager de mettre en œuvre pour protéger les données. Vous trouverez de plus amples informations sur ces politiques tout au long de ce document. En outre, l'Institut SANS est une ressource précieuse pour l'élaboration et la mise en œuvre de telles politiques.

Pour obtenir des exemples de modèles de politiques de sécurité, veuillez consulter le site : https://www.sans.org/securityresources/policies.

Vous y trouverez également un excellent article sur l'introduction de politiques de sécurité dans une entreprise : https://www.csoonline.com/article/2124114/it-strategy/strategic-planning-erm-how-to-write-an-information-security-policy.html.

7.1.10 Directives des concessionnaires sur les politiques de sécurité

[aucun contenu]

7.2 Guide de gestion des identités et des accès

Couvrir la gestion des identités et des accès de manière exhaustive. Commencez par une introduction et des concepts de base suivis de sous-sections : gestion des identités, authentification, autorisations et pourquoi elles sont si importantes, processus de gestion des accès, utilisateurs finaux et considérations physiques, et 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 :

- aux personnes qui ont le droit d'accéder
- les bonnes ressources à
- les bons moments pour
- les bonnes raisons.

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

7.2.2 Concepts et définitions de base

Pour établir une base de référence, définissez les termes de base relatifs à la gestion des identités et des accès.

- **Entité** : une personne réelle ou un système d'information
- **Identité** : entité dans un contexte spécifique (par exemple, au travail ou dans les médias sociaux)
- **Identificateur** : ensemble d'attributs permettant d'identifier une identité (par exemple, SSN, courrier électronique, empreinte digitale)
- **Authentification** : un processus de confirmation de l'identité revendiquée par une entité (par exemple, en fournissant un mot de passe)
- **Autorisations** : ensemble d'autorisations attribuées à quelqu'un ou quelque chose (par exemple, "vous êtes autorisé à voir le dossier médical du patient XYZ")
- **Comptabilité/Audit :** l'histoire de ce qui s'est passé

Ce qui précède doit être considéré dans ses dimensions physiques et logiques, où physique signifie limiter l'accès aux bâtiments, pièces et autres biens informatiques physiques, et logique signifie limiter l'accès au monde informatique virtuel, comme les connexions aux réseaux informatiques, aux systèmes d'information, aux fichiers ou aux données. Une fois que ce qui précède est mis en œuvre, introduisez l'élément clé de ce puzzle.

- **Contrôle d'accès :** il s'agit de s'assurer que les règles d'autorisation sont exécutées. On peut considérer qu'il s'agit de la mise en œuvre de l'authentification, de l'autorisation et de la comptabilité (AAA) dans les dimensions physique et logique.

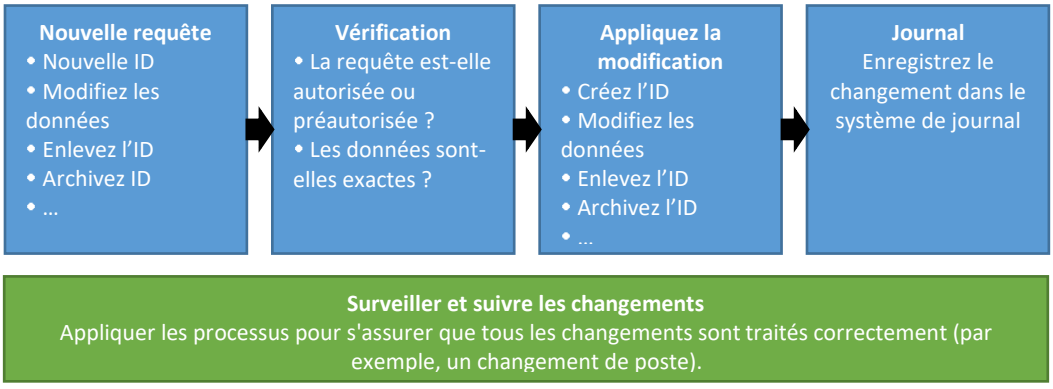
7.2.3 Gestion des identités

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 de l'identité

Cycle de vie des identités

Le cycle de vie doit être pris en compte depuis le début d'une relation jusqu'à sa fin et être suivi dans le temps pour détecter les changements de contexte (par exemple, l'employé change d'affectation). Le processus peut être illustré comme suit :



- Limiter le nombre d'identités liées à une entité spécifique et centraliser leur gestion (par exemple, essayer d'éviter les situations où il existe des comptes spécifiques à une application).
- Essayez d'éviter les comptes de groupe. Au cas où cela serait vraiment nécessaire, veillez à nouveau à ce que chacun ait son propre dépositaire responsable.
- N'oubliez pas que les identités sont liées non seulement aux utilisateurs finaux, mais aussi aux services ou aux réseaux et que ce type d'identités doit également être géré et entretenu avec soin. Veillez à ce que chaque identité non personnelle ait son propre gardien qui en soit responsable.
- Veillez à ce que le stockage des identités soit protégé, en particulier lorsque des informations confidentielles sont stockées. En général, les mots de passe sont cités à titre d'exemple, mais ils peuvent également faire référence à des informations sensibles sur les utilisateurs (par exemple, les coordonnées GPS des lieux visités).

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

Gestion des mots de passe
Les mots de passe doivent être sécurisés à la fois lors du transit et du stockage. En outre, 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** - où l'identité est gérée (par exemple, Active Directory, application métier, etc.).
    - Aspects principaux
        - Le mot de passe ne doit pas être stocké en texte clair et - dans le cas où il est crypté de manière réversible, la clé de décryptage doit être protégée de manière correcte.
        - Tous les mots de passe par défaut fournis par le vendeur doivent être modifiés avant la mise en service de tout système d'information.
- **Du côté du client** - 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 cryptée (par exemple, dans une application KeyPass, un fichier Excel crypté). Ensuite, il est important de protéger le mot de passe principal de manière sécurisée. Il est très important de décourager les employés de...
    - écrire les mots de passe et les conserver dans un endroit visible pour les autres (par exemple, sur un post-it à proximité du lieu de travail)
    - en divulguant les mots de passe à quiconque, sauf en cas d'absolue nécessité (par exemple, à l'assistance du service d'assistance) ; et en se rappelant de changer le mot de passe après l'avoir divulgué

Tous les mots de passe doivent être changés rapidement si l'on soupçonne qu'ils sont composés ou divulgués à des vendeurs pour la maintenance/le soutien.

Il est également important de s'assurer que toutes les sauvegardes où les mots de passe sont stockés sont également sécurisées avec soin.

Des procédures communes qui doivent être conçues de manière sûre :

- Envoi du mot de passe initial de manière sécurisée
- Récupération du mot de passe en cas d'oubli
- Déverrouillage en cas de verrouillage

- Libre-service pour le changement de mot de passe
- Politiques relatives au cycle de vie des mots de passe (voir la section sur les politiques relatives aux mots de passe) ;

Mais n'oubliez pas que des politiques trop restrictives peuvent également avoir des conséquences négatives.

Fédération d'identités et authentification unique
Au cas où une entreprise serait créée avec d'autres partenaires au niveau des systèmes informatiques, il est utile de se pencher sur la politique de la 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 matures qui soutiennent cette approche. Ce sont les avantages immédiats :

- Signature unique : l'utilisateur final doit s'authentifier une fois et a accès à un certain nombre d'applications (sans avoir besoin de se ré-authentifier)
- Moins de coûts liés à la gestion du cycle de vie de l'identité
- Moins de risques liés à la nécessité pour un utilisateur final de conserver des identités distinctes

En fin de compte, un calcul doit être effectué pour déterminer si l'investissement dans la fédération d'identité vaut la peine dans un contexte spécifique.

7.2.4 Authentification
La preuve la plus courante en matière d'authentification est le mot de passe, mais il y a aussi un problème : les mots de passe sont difficiles à retenir. C'est pourquoi il est de plus en plus courant d'utiliser des phrases de passe à la place. 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, telles que la biométrie, les mots de passe à usage unique, ou les cartes à puce prises en charge par les tokens RSA, les applications mobiles comme Google Authenticator ou Yubikey. Chaque méthode est généralement classée dans l'une des trois catégories suivantes

- Quelque chose que vous connaissez (mots de passe, motifs visuels)
- Quelque chose que vous avez (carte à puce, jeton RSA, smartphone)
- Quelque chose que vous êtes (biométrie, comportement)

Il y a deux raisons pour appliquer des méthodes d'authentification différentes :

- Une meilleure expérience utilisateur (par exemple, la biométrie)
- Une meilleure sécurité (carte à puce)

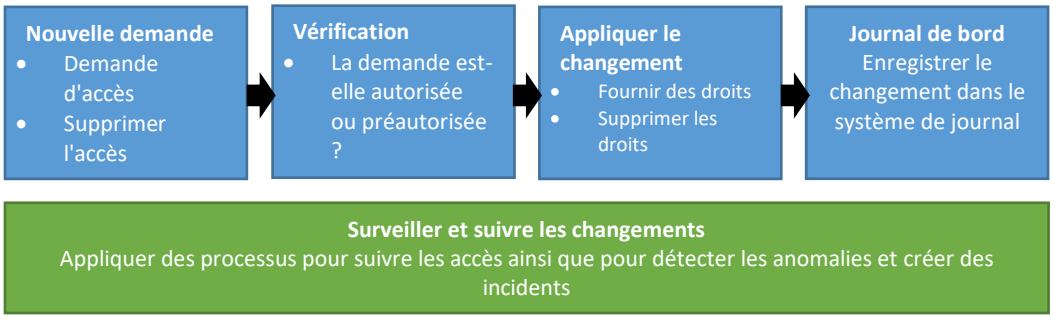
Lorsque deux ou plusieurs méthodes de différentes catégories sont combinées, on parle **d'authentification multifactorielle**, qui vise à augmenter le niveau de sécurité.

7.2.5 Processus de gestion des autorisations et de l'accès
Les autorisations correctes - c'est-à-dire la définition des permissions et leur représentation dans les systèmes informatiques - sont l'une des plus importantes du paysage global de la sécurité informatique. Les aspects suivants doivent être correctement sécurisés :

- Définir une structure de rôles et de niveaux d'accès

- Définir un ensemble d'autorisations pour un rôle donné
- Veiller à ce que les autorisations soient documentées et facilement accessibles
- Veiller à ce que les autorisations soient mises en œuvre dans les systèmes de contrôle d'accès
- Les demandes d'accès sont approuvées par les personnes compétentes et il est clairement défini qui sont les approbateurs
- Contrôle et révision (audits) des droits d'accès et des autorisations

En outre, le **processus de gestion des accès** doit être établi et mis en œuvre pour s'assurer que les autorisations définies sont appliquées en tout lieu et à tout moment. Le processus est similaire au processus de gestion du cycle de vie des identités et peut être illustré comme suit :



Les éléments clés d'un tel processus qui devraient être pris en compte :

- L'accès est révoqué ou modifié chaque fois qu'un employé quitte l'entreprise ou change de poste.
- L'accès doit être mis à jour en temps utile en fonction des besoins de l'entreprise.
- L'accès doit être revu périodiquement selon une cadence documentée (trimestriellement, semestriellement, annuellement). Cette évaluation, qui n'est pas motivée par le départ ou la transition de l'employé, vise à déterminer si le niveau d'accès actuellement accordé correspond au poste de la personne dans l'entreprise. Veuillez noter que la fréquence des examens peut varier en fonction de la criticité des biens qui sont protégés.
- Une bonne pratique consiste également à appliquer le principe du "besoin de savoir", c'est-à-dire que l'accès aux ressources ne devrait être accordé que s'il existe un besoin de l'entreprise.

Une fois encore, on ne saurait trop insister sur l'importance du contrôle et de l'audit des autorisations et des droits d'accès, notamment pour s'assurer que la suppression de l'accès est correctement mise en œuvre. Malheureusement, il est très courant que les droits d'accès soient accordés puis ne soient jamais supprimés.

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 des utilisateurs. (Ceux liés aux dimensions logiques (comme le fait de cliquer sur des e-mails dangereux) sont traités dans d'autres sections). Les éléments liés au contrôle d'accès physique suivent et devraient également servir de base à une stratégie d'éducation appropriée.

- Les salles de serveur/équipements doivent être verrouillées. L'accès des employés devrait être limité aux seules personnes qui ont un besoin professionnel légitime. Des mécanismes devraient être mis en place pour savoir si et quand quelqu'un accède au site.
- Exiger que les dossiers contenant des données et des informations sensibles soient conservés dans des classeurs verrouillés à tout moment, sauf lorsqu'un employé travaille sur le dossier. De plus, lorsqu'un employé travaille sur le dossier, assurez-vous que les personnes non autorisées ne puissent pas voir le dossier (par exemple, lorsqu'elles prennent l'avion).
- Rappelez aux employés de ne pas laisser de documents/informations sensibles sur les bureaux lorsqu'ils ne sont pas à leur poste de travail.
- Demandez aux employés de ranger les dossiers, de fermer les ordinateurs et de verrouiller les classeurs et les portes des bureaux à la fin de la journée.
- Mettez en place des contrôles d'accès appropriés pour votre bâtiment. Indiquez aux employés ce qu'ils doivent faire et qui doit être averti si une personne inconnue est vue sur les lieux.
- Si des installations de stockage hors site sont maintenues, limitez l'accès des employés à ceux qui ont un besoin professionnel légitime. Des mécanismes doivent être mis en place pour savoir si et quand quelqu'un accède au site.
- Si des dispositifs qui recueillent des informations sensibles sont utilisés, tels que des claviers NIP, sécurisez l'équipement afin de réduire le risque de falsification. Ces équipements doivent également être sécurisés afin de réduire le risque qu'un attaquant change d'équipement avec un dispositif factice.

7.2.7 Niveaux de protection

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

- **Applications commerciales** : applications nécessaires pour gérer les commandes, planifier le travail, organiser les ressources humaines et les finances, etc. L'accent est mis sur la protection des informations et des fonctionnalités commerciales sensibles. 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** : base permettant d'exécuter des applications sur des ordinateurs portables, des ordinateurs de bureau, des serveurs, des téléphones, des tablettes, etc. L'accent est mis sur la protection des fichiers et des données, contre les logiciels malveillants, et sur ce que le contrôle d'accès peut prendre en charge. Les identités concernent généralement les utilisateurs finaux (ordinateurs portables, téléphones, etc.) et les services (serveurs).
- **Dispositifs 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 réseau correct, la sécurisation des communications et la protection contre les 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 la garantie d'un accès sécurisé, y compris dans des situations telles que l'utilisation hors ligne ou le vol d'un appareil.
- **Locaux/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 biens.

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

- Couche application (par exemple, HTTP)
- Couche de transport (par exemple, TCP)
- Couche Internet (par exemple, IP)
- Couche réseau (par exemple, Ethernet)

Il est important de s'assurer que la couverture de l'IAM est complète dans les différentes couches et zones selon les exigences qui doivent être basées sur la criticité de l'information.

- Mettre en œuvre une protection complète sur toutes les couches et pour tous les types d'applications et de dispositifs, tant sur le plan physique que logique.

7.3 Orientations relatives à l'échéance du niveau de sécurité des concessionnaires

Les concessionnaires ont souvent du mal à appliquer les recommandations en matière de sécurité. Cela est souvent attribué au niveau de maturité de la concession en termes d'informatique et de sophistication de la sécurité. Utilisez ce guide pour vous aider à identifier le niveau de maturité de votre concession et les prochaines étapes à suivre pour améliorer la sécurité de votre concession.

7.3.1 Orientations des distributeurs sur les politiques de sécurité

Pour déterminer les prochaines étapes de la maturation des politiques de sécurité d'une concession, il faut d'abord identifier le niveau de maturité actuel de la concession. Ensuite, déterminez les mesures qui peuvent être prises pour améliorer la sécurité de la concession. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base :** Les concessionnaires ont identifié et documenté les politiques concernant l'utilisation acceptable, l'audit, la gestion de l'accès (y compris le mot de passe) et les considérations de base relatives au réseau (y compris l'accès externe et les normes sans fil).
- **Niveau de maturité intermédiaire** : les concessionnaires ont défini et documenté des politiques concernant l'utilisation, l'audit, la gestion de l'accès (y compris les mots de passe) et les considérations de base relatives au réseau (y compris l'accès externe et les normes sans fil) : Les concessionnaires ont identifié et documenté des politiques pour tous les domaines attendus. De plus, elles ont mis en place des processus pour fournir, former et soutenir le personnel de la concession avec des politiques de sécurité documentées.
- **Niveau de maturité avancé** : Les concessionnaires testent, vérifient et affinent régulièrement les politiques et procédures de sécurité.

7.3.2 Guide du concessionnaire sur la gestion de l'identité et de l'accès (IAM)

Lorsque vous déterminez les prochaines étapes pour faire mûrir l'AMI d'une concession, identifiez d'abord le niveau de maturité actuel de la concession. Ensuite, déterminez les mesures qui peuvent être prises pour améliorer la sécurité de la concession. Utilisez le guide ci-dessous pour vous aider.

Niveau de maturité de base

- Des processus explicites pour gérer le cycle de vie des identités et les droits d'accès
- Audits et révisions régulières des autorisations pour les systèmes critiques
- Procédures explicites pour la gestion des mots de passe
- Formation de base des employés (au moins pour les nouveaux employés)
- Système de contrôle d'accès aux locaux critiques

Niveau de maturité intermédiaire

- Des processus explicites pour gérer le cycle de vie des identités et les droits d'accès
- Audits et révisions régulières des autorisations pour les systèmes critiques
- Procédures explicites pour la gestion des mots de passe et recommandations sur le stockage des mots de passe du côté client
- Formation régulière des employés
- Système de contrôle d'accès pour tous les locaux physiques

- Niveau de protection (par exemple, authentification multifactorielle, défense en profondeur) lié à la criticité des informations et des fonctions commerciales

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 approprié de fédération des identités
- Processus centralisés pour la gestion et l'authentification des mots de passe
- Recommandations (ou politiques) fermes sur le stockage des mots de passe du côté client
- Niveau de protection (par exemple, authentification multifactorielle, défense en profondeur) lié à la criticité des informations et des fonctions commerciales
- Système de contrôle d'accès centralisé pour tous les locaux physiques
- Formation régulière des employés
- Audits et examens réguliers des autorisations et des identités
- Protection complète sur toutes les couches et pour tous les types d'applications et de dispositifs, tant sur le plan physique que logique

7.3.3 Guide du concessionnaire sur la gestion des patchs

Niveau de maturité de base : Les concessionnaires ont réglé chaque système pour qu'il se mette automatiquement à jour pour les correctifs critiques ou de sécurité.

Niveau de maturité intermédiaire : Les concessionnaires ont mis en place 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.

7.3.4 Conseils aux concessionnaires concernant la reprise après sinistre

Lorsque vous déterminez les prochaines étapes à suivre pour assurer la continuité des activités et la reprise après sinistre d'une concession, identifiez d'abord le niveau de maturité actuel de la concession. Ensuite, déterminez les mesures qui peuvent être prises pour améliorer la sécurité de la concession. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base** : Les concessionnaires effectuent régulièrement des sauvegardes de tous les systèmes.
- **Niveau de maturité intermédiaire** : Les concessionnaires effectuent régulièrement des sauvegardes incrémentielles et stockent les images de sauvegarde hors site.
- **Niveau de maturité avancé** : Les concessionnaires déploient un système de continuité des activités qui inclut des sauvegardes complètes du système hors site dans un environnement virtuel qui permettra au concessionnaire de faire tourner l'image de sauvegarde immédiatement en cas de panne ou de défaillance.

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

Lorsque vous déterminez les prochaines étapes pour faire mûrir le programme de sensibilisation à la sécurité d'une concession, identifiez d'abord le niveau de maturité actuel de la concession. Ensuite, déterminez les mesures qui peuvent être prises pour améliorer la sécurité de la concession. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base** : Tous les employés suivent une formation annuelle sur la sécurité. L'achèvement de la formation est documenté et les rapports sont disponibles pour vérification. Les employés peuvent être incertains de leur rôle dans la protection de l'organisation. L'organisation peut être conforme, mais pas sûre. Il n'y a pas de processus établi pour et/ou les

employés ne se sentent pas habilités à signaler un comportement suspect ou une perte accidentelle de données.

- **Niveau de maturité intermédiaire** : Le programme de formation peut être plus fréquent qu'une fois par an et un suivi est effectué pour s'assurer que tous les employés y participent comme condition d'emploi. Les sujets couverts se concentrent sur les risques les plus importants pour l'organisation. Des documents de sensibilisation sont affichés dans les zones de pause des employés. Les employés connaissent les politiques de sécurité de l'entreprise et savent comment reconnaître et signaler un incident de sécurité.
- **Niveau de maturité avancé** : Le programme de formation destiné à tous les employés et entrepreneurs comprend des modules courts mais fréquents sur des sujets d'actualité en rapport avec leur rôle. Les employés sont testés sur leur capacité à se défendre contre diverses tactiques d'ingénierie sociale telles que le phishing, les USB drops, la fraude, etc. Les employés savent comment signaler un incident de sécurité et, lorsqu'ils sont testés, au moins 50 % des employés signalent quelque chose de suspect. Lorsqu'ils sont testés, moins de 10 % d'entre eux cliquent sur des e-mails de test de phishing. Les concessionnaires ont une culture de la sécurité : les employés comprennent leur rôle dans la protection de l'organisation, recherchent des processus sécurisés et encouragent leurs collègues à mener leurs activités en respectant la sécurité et en protégeant l'organisation contre la fraude, le vol et la perte accidentelle de données ou d'argent.

7.3.6 Conseils aux concessionnaires sur le respect des législations fédérales

Lorsque vous déterminez les prochaines étapes à franchir pour qu'un concessionnaire se conforme aux législations en matière de sécurité, identifiez d'abord le niveau de maturité actuel du concessionnaire. Ensuite, déterminez les mesures qui peuvent être prises pour améliorer la sécurité de la concession. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base** : Les concessionnaires ont effectué des recherches sur le PCI et le GLBA pour déterminer la conformité avec la législation fédérale. Les concessionnaires disposent de politiques et de processus documentés pour respecter la conformité.
- **Niveau de maturité intermédiaire** : Les concessionnaires examinent et révisent régulièrement la conformité à la législation fédérale en matière de sécurité
- **Niveau de maturité avancé** : Les concessionnaires effectuent des audits réguliers des systèmes et suivent les résultats en fonction des exigences de la législation.

7.3.7 Conseils aux concessionnaires sur la sécurité des réseaux

Lorsque vous déterminez les prochaines étapes pour faire évoluer la sécurité du réseau d'un concessionnaire, identifiez d'abord le niveau de maturité actuel du concessionnaire. Ensuite, déterminez les mesures qui peuvent être prises pour améliorer la sécurité du réseau de la concession. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base** : Les concessionnaires ont élaboré et documenté une politique d'utilisation d'Internet. Les concessionnaires disposent d'une protection au niveau de la passerelle du réseau et ont configuré et segmenté le réseau pour éviter tout accès indésirable aux ressources du réseau. Le réseau est surveillé en temps réel par des technologies de gestion des événements de sécurité afin de se protéger contre tout accès indésirable au réseau. L'accès à distance est surveillé et limité sur le réseau.
- **Niveau de maturité intermédiaire** : Les concessionnaires ont utilisé des politiques et des processus documentés pour mettre en place un réseau de concessionnaires segmenté et sécurisé. Les concessionnaires testent régulièrement le réseau par rapport aux risques connus. Le réseau est surveillé 24 heures sur 24, 7 jours sur 7 et 365 jours par an par des experts en sécurité qui utilisent des technologies de gestion des événements liés à la sécurité. L'accès à distance est surveillé et limité aux vendeurs et employés connus.

- **Niveau de maturité avancé** : Les concessionnaires ont utilisé des politiques et des processus documentés pour mettre en place un réseau de concessionnaires segmenté et sécurisé. Les concessionnaires testent régulièrement le réseau par rapport aux risques connus. Le réseau est surveillé 24 heures sur 24, 7 jours sur 7 et 365 jours par an par un fournisseur de services certifié SOC 2. Le réseau est surveillé 24 heures sur 24, 7 jours sur 7, 365 jours par an par des experts en sécurité. L'accès à distance est surveillé et limité aux vendeurs et employés connus. L'accès au VPN des employés est réalisé par une authentification à deux facteurs.

7.3.8 Conseils concernant l'antivirus du concessionnaire

Lorsque vous déterminez les prochaines étapes de la maturation du titre AV d'un concessionnaire, identifiez d'abord le niveau de maturité actuel du concessionnaire. Ensuite, déterminez 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 ont identifié tous les systèmes et ont appliqué un logiciel antivirus à chaque système du réseau.
- **Niveau de maturité intermédiaire** : Les concessionnaires ont mis en place un système antivirus d'entreprise. Celui-ci comprend la gestion des licences à l'échelle de l'entreprise, un portail d'entreprise pour la production de rapports et de réponses, ainsi qu'un audit et des rapports sur l'ensemble du réseau.
- **Niveau de maturité avancé** : Les concessionnaires effectuent une réponse proactive et immédiate aux alertes générées par la solution AV de l'entreprise.

7.3.9 Conseils aux revendeurs sur la sécurité du courrier électronique

Lorsque vous déterminez les prochaines étapes pour faire évoluer la sécurité du courrier électronique d'un concessionnaire, identifiez d'abord le niveau de maturité actuel du concessionnaire. Ensuite, déterminez les mesures qui peuvent être prises pour améliorer la sécurité de la concession. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base** : Les concessionnaires 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 et une protection actives de la sécurité des courriels entrants et sortants. Les concessionnaires cryptent les données sensibles par courrier électronique.
- **Niveau de maturité avancé :** Les concessionnaires surveillent activement le courrier électronique et réagissent aux menaces qu'il représente.

7.3.10 Orientation avec UTM/Pare-feu/IDS

Lorsque vous déterminez les prochaines étapes pour faire mûrir le système unifié de gestion des menaces, de pare-feu et de détection des intrusions d'une concession, identifiez d'abord le niveau de maturité actuel de la concession. Ensuite, déterminez les mesures qui peuvent être prises pour améliorer la sécurité de la concession. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base :** Les concessionnaires déploient un UTM entièrement géré et sous licence, qui comprend l'octroi de licences pour l'AV, le SPAM et l'IDS/IPS. Les signatures sont automatiquement mises à jour en temps réel.
- **Niveau de maturité intermédiaire** : Les concessionnaires répondent aux alertes et aux événements de l'UTM 24x7x365 en temps réel. Les concessionnaires utilisent un SIEM (voir section 3.5) pour alerter et répondre aux événements au niveau de la passerelle du réseau.
- **Niveau de maturité avancé** : Les concessionnaires se tournent vers un fournisseur de services de sécurité gérés (MSSP) pour la gestion, la surveillance et la réponse proactive, 24 heures sur 24, 7

jours sur 7, 365 jours par an, de l'UTM.

7.3.11 Orientation avec le SIEM

Pour déterminer les prochaines étapes de la maturation de la gestion des événements de sécurité d'une concession, il faut d'abord identifier le niveau de maturité actuel de la concession. Ensuite, déterminez les mesures qui peuvent être prises pour faire progresser la posture de sécurité de la concession. Utilisez le guide ci-dessous pour vous aider.

- **Niveau de maturité de base** : Les concessionnaires installent et utilisent le logiciel SIEM. Toutes les alertes sont traitées en temps quasi réel 24x7x365. Tous les journaux du système sont stockés conformément à la législation fédérale (voir section 2.6 sur le respect des législations fédérales).
- **Niveau de maturité intermédiaire** : Les concessionnaires font appel à un fournisseur de services de sécurité gérés pour la surveillance et l'intervention avancées. Les concessionnaires intègrent le renseignement sur les menaces pour une surveillance et une alerte avancée.
- **Niveau de maturité avancé** : Les concessionnaires font appel à un fournisseur de services de sécurité gérés (MSSP) certifié SOC 2 pour la gestion, la surveillance et l'intervention proactives, 24h/24, 7j/7 et 365 jours par an. Les concessionnaires intègrent le renseignement sur les menaces dans la solution SIEM. Les tickets, les alertes et les activités sont régulièrement examinés par la direction de la concession et le MSSP pour affiner, documenter et améliorer la posture de sécurité.

7.3.12 Guide du concessionnaire sur la sécurité des demandes

Lorsque vous déterminez les prochaines étapes pour faire mûrir la sécurité d'application d'un concessionnaire, identifiez d'abord le niveau de maturité actuel du concessionnaire. Ensuite, déterminez les mesures qui peuvent être prises pour améliorer la sécurité de la concession. Utilisez le guide ci-dessous pour vous aider.

Niveau de maturité de base

- Introduire un catalogue des candidatures.
- Maintenir une gestion de base des identités et des accès.
- Appliquer régulièrement les mises à jour et les correctifs des applications.

Niveau de maturité intermédiaire

- Tenir à jour le catalogue des demandes en comprenant l'analyse de l'impact sur les entreprises et la classification des informations.
- Mise en œuvre d'une stratégie mature de gestion des identités et des accès.
- Protection des flux d'informations de bout en bout, tant au niveau du transit que du stockage.
- Mise en place de processus de traitement des incidents et des demandes d'accès.
- Appliquer une stratégie de défense en profondeur.

Niveau de maturité avancé

- Appliquer tous les éléments de la section précédente.

7.3.13 Guide du concessionnaire sur la mobilité

Lorsque vous déterminez les prochaines étapes pour faire mûrir la sécurité d'une concession en matière de mobilité, identifiez d'abord le niveau de maturité actuel de la concession. Ensuite, déterminez les mesures qui peuvent être prises pour améliorer la sécurité de la concession. Utilisez le guide ci-dessous pour vous aider.

Niveau de maturité de base

- Maintenez à jour les logiciels anti-malware.
- Définir quelles informations peuvent être traitées et stockées sur les appareils mobiles ; inclure des considérations relatives aux appareils gérés et non gérés.

- L'accès aux appareils doit être restreint, ce qui nécessite une authentification de l'utilisateur. La plupart des appareils peuvent être verrouillés à l'aide d'un verrou d'écran, d'un mot de passe ou d'un code PIN.
- Mettre à jour le système d'exploitation mobile avec des correctifs de sécurité. Pour plus d'informations sur la gestion des correctifs, voir la section 2.6.3.

Niveau de maturité intermédiaire

- Tous les articles du niveau de maturité de base.
- Appliquer un cryptage approprié des données à la fois sur les ordinateurs portables et les appareils mobiles avec une attention particulière à la gestion des clés pour le décryptage.
- Examinez toutes les méthodes de connectivité, soyez prudent avec la connectivité sans fil automatisée car les mots de passe peuvent être exposés ainsi qu'une attaque de type "man-in-the-middle" peut être exécutée.
- Créez des politiques et des procédures sur qui, quand et comment accéder à distance à l'environnement de l'entreprise (réseau, serveurs, applications, etc.) et quelles parties de celui-ci. Déployer une solution technique appropriée pour soutenir l'approche établie.
- Sauvegarder régulièrement l'appareil mobile.

Niveau de maturité avancé

- Appliquer tous les éléments des sections précédentes.

7.4 Glossaire

802.11 : 802.11 est un groupe de spécifications sans fil développé par l'IEEE pour les communications sur les 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. Voici quelques spécifications communes : 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 suivent la norme IEEE.

Antenne : Dispositif permettant de transmettre et de recevoir des signaux de radiofréquence (RF). Souvent camouflées sur des bâtiments existants, des arbres, des châteaux d'eau ou d'autres structures hautes, la taille et la forme des antennes sont généralement déterminées par la fréquence du signal qu'elles gèrent.

App (Application): Outils, ressources, jeux, réseaux sociaux ou presque tout ce qui ajoute une fonction ou une caractéristique à un appareil sans fil, téléchargeables gratuitement ou contre rémunération. 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 dans l'application en protégeant par un mot de passe ces fonctions sur un appareil sans fil. La CTIA a créé un système d'évaluation des applications pour aider à informer les parents sur une application afin qu'ils puissent déterminer si elle est appropriée pour leurs enfants :**http://bit.ly/JtPvve**.

Haut débit : Une 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 assimilée à la fourniture de vitesses accrues et de capacités avancées, y compris l'accès à l'internet et aux services connexes

Cat5 : Un type de câble à paires torsadées conçu pour une grande intégrité du signal. Beaucoup de ces câbles ne sont pas blindés, mais certains sont blindés. La catégorie 5 a été remplacée par la spécification de la catégorie 5e. Ce type de câble est souvent utilisé dans le câblage structuré pour les réseaux informatiques tels qu'Ethernet et sert également à transporter de nombreux autres signaux tels que les services vocaux de base, l'anneau à jetons et l'ATM (jusqu'à 155 Mbit/s, sur de courtes distances).

Cat5e: La spécification de la catégorie 5e améliore les spécifications de la catégorie 5 en resserrant certaines spécifications de diaphonie et en introduisant de nouvelles spécifications de diaphonie qui n'étaient pas présentes dans les spécifications originales de la catégorie 5. La largeur de bande des catégories 5 et 5e est la même - 100 MHz.

Cat6 : norme de câble pour l'Ethernet gigabit et d'autres protocoles de réseau qui est rétrocompatible avec les normes de câble de catégorie 5/5e et de catégorie 3. La catégorie 6 comporte des spécifications plus strictes pour la diaphonie et le bruit du système. La norme de câble offre des performances allant jusqu'à 250 MHz et convient aux protocoles 10BASE-T / 100BASE-TX et 1000BASE-T (gigabit Ethernet). Il devrait convenir à la norme 10GBASE-T (10gigabit Ethernet), bien qu'avec

des limitations de longueur s'il n'est pas blindé, le câble Cat 6 est utilisé. La Ford Motor Company recommande l'utilisation d'un câble Cat6 lors de l'utilisation d'un nouveau câble ou du remplacement de nouveaux segments de réseau câblé.

DSL (Digital Subscriber Line) : Une ligne numérique reliant le terminal de l'abonné au bureau central de la société de desserte, offrant plusieurs canaux de communication capables de transporter simultanément des communications vocales et des données.

Le cryptage : Embrouillage numérique des informations afin qu'elles puissent être transmises sur un réseau non sécurisé. À l'autre extrémité, le destinataire utilise généralement une "clé" numérique pour décrypter les informations afin de les restituer sous leur forme originale.

PC de poche/tablettes : Ces appareils sont des ordinateurs qui peuvent être portés par un utilisateur. Ils sont généralement beaucoup plus petits qu'un ordinateur portable typique et n'ont pas toutes les capacités d'un ordinateur de bureau, mais peuvent néanmoins effectuer la plupart des tâches nécessaires. Ils permettent également à un utilisateur de travailler dans différents endroits d'une concession, ce qui peut augmenter la productivité.

IEEE (Institut des ingénieurs en électricité et en électronique) : Association professionnelle dont le siège est à New York et qui se consacre à la promotion de l'innovation technologique et de l'excellence. 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).

LAN (Local Area Network) : Le réseau local (LAN) est un petit réseau de données couvrant une zone limitée comme un bâtiment ou un groupe de bâtiments. La plupart des réseaux locaux connectent des postes de travail ou des ordinateurs personnels. Cela permet à de nombreux utilisateurs de partager des appareils tels que des imprimantes laser, ainsi que des données. Le LAN permet également de communiquer facilement, en facilitant le courrier électronique ou en prenant en charge les sessions de chat.

Malware: Les logiciels malveillants : Un malware (pour "logiciel malveillant") est tout programme ou fichier qui est nuisible à l'utilisateur d'un ordinateur. Ainsi, les logiciels malveillants comprennent les virus informatiques, les vers et les chevaux de Troie, ainsi que les logiciels espions, c'est-à-dire les programmes qui recueillent des informations sur un utilisateur d'ordinateur sans autorisation.

Megahertz : 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 800 MHz, 900 MHz et 1900 MHz (Wi-Fi = 250, 400).

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 (OS) agit comme un hôte pour les programmes d'application qui sont exécutés sur la machine. En tant qu'hôte, l'un des objectifs d'un système d'exploitation est de gérer les détails du fonctionnement du matériel. La Ford Motor Company recommande le système d'exploitation Windows 7 pour la compatibilité avec les applications Ford.

Gestion des patchs : Le processus de mise à jour des serveurs ou des PC. Cela est souvent fait pour mettre à jour les machines avec les derniers correctifs de sécurité et les Service Packs. Les auteurs de virus, de logiciels espions et d'autres logiciels malveillants exploitent les failles existantes dans les logiciels chargés sur un PC pour se propager et causer des dommages. STAR recommande aux concessionnaires d'appliquer dès que possible les correctifs critiques, tels que les correctifs de sécurité.

Point d'accès sans fil malveillant : 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 de la concession. Tout réseau sans fil malveillant doit être détecté, trouvé et supprimé immédiatement.

Routeurs : Permettent aux ordinateurs de différents réseaux et sous-réseaux de communiquer. Dans les concessions, les routeurs peuvent être utilisés pour connecter un réseau local OEM, un réseau local de concession et un réseau local DMS à l'internet.

Spectre : Les fréquences radioélectriques qui sont désignées pour un usage spécifique tel que les services de communications personnelles et la sécurité publique.

Spyware : Toute technologie qui aide à recueillir des informations sur une personne ou une organisation à son insu. Sur l'internet (où il est parfois appelé "spybot" ou "logiciel de suivi"), un logiciel espion est un programme qui est placé dans l'ordinateur d'une personne pour recueillir secrètement des informations sur l'utilisateur et les transmettre à des

annonceurs ou à d'autres parties intéressées. Les commerçants doivent déployer des systèmes pour détecter et supprimer les logiciels espions afin de protéger les données des clients et l'intégrité de la sécurité du réseau.

SSID (Service Set identification) : Dans les réseaux informatiques, un SSID est un ensemble composé de tous les dispositifs associés à un réseau local sans fil IEEE 802.11x. Les SSID doivent être associés à un VLAN spécifique.

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

Trojan (cheval de Troie) : Un cheval de Troie est un programme dans lequel un code malveillant ou nuisible est contenu dans des données ou des programmes apparemment inoffensifs de telle sorte qu'il peut prendre le contrôle et causer la forme de dommage qu'il a choisie, comme par exemple détruire une zone déterminée de votre disque dur.

VPN (réseaux privés virtuels) : Un VPN permet à un utilisateur d'effectuer des transactions sécurisées sur un réseau public ou non sécurisé. En cryptant les messages envoyés entre les appareils, l'intégrité et la confidentialité des données transmises sont maintenues privées.

VLAN (Virtual Local Area Network) : Dans les réseaux informatiques, un réseau de couche 2 unique (basé sur un commutateur) peut être partitionné pour créer plusieurs domaines de diffusion distincts, qui sont mutuellement isolés de sorte que les paquets ne peuvent passer entre eux que par un ou plusieurs routeurs ; un tel domaine est appelé réseau local virtuel, LAN virtuel ou VLAN. Il est généralement réalisé sur des dispositifs de commutation ou de routage.

VoIP (Voice over Internet Protocol) : Le VoIP n'est pas seulement capable de fournir de la voix sur IP, mais il est également conçu pour permettre la vidéoconférence bidirectionnelle et le partage d'applications. Basé sur la technologie IP, le VoIP est utilisé pour transférer un large éventail de trafic de différents types.

WAN (Wide Area Network) : Terme général désignant un grand réseau couvrant un pays ou le monde entier. L'internet est un WAN. Un système de communication mobile public tel qu'un réseau cellulaire ou PCS est un WAN. Les concessionnaires peuvent mettre en réseau des sites et des bâtiments éloignés grâce à la technologie WAN. Dans la plupart des cas, le terme WAN désigne le fournisseur de services Internet du concessionnaire.

Ver : Un ver est un virus qui se réplique automatiquement et qui n'altère pas les fichiers mais se duplique. Il est fréquent que les vers ne soient remarqués que lorsque leur réplication non contrôlée consomme les ressources du système, ralentissant ou arrêtant 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 équipés de la technologie Wi-Fi.

WPA (Wi-Fi Protected Access - accès Wi-Fi protégé) : Protocoles de sécurité et programmes de certification de la sécurité développés par l'Alliance Wi-Fi pour sécuriser les réseaux informatiques sans fil. L'Alliance Wi-Fi l'a conçu comme une mesure intermédiaire en prévision de la disponibilité du WPA2, plus sûr et plus complexe. Le WPA n'est pas sécurisé et ne doit pas être utilisé par les revendeurs.

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

Réseau local sans fil (WLAN) : Utilisant la technologie des radiofréquences (RF), les WLAN transmettent et reçoivent des données sans fil dans une certaine zone. Cela permet aux utilisateurs d'une petite zone de transmettre des données et de partager des ressources, telles que des imprimantes, sans être physiquement connectés à l'appareil.