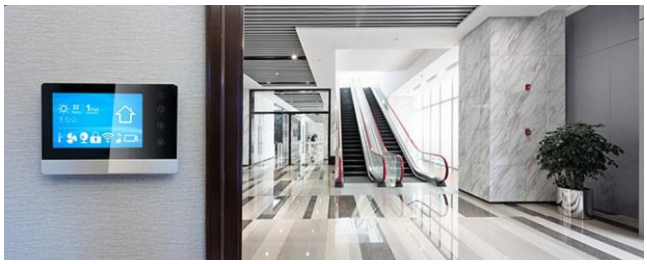
5.1.1.2. Comment l'automatisation est-elle utilisée ?

- **La domotique intelligente :** Pour beaucoup, l'environnement domestique est devenu un environnement plus automatisé. Des dispositifs tels que HomeKit d'Apple, Alexa d'Amazon et Google assistant nous permettent de donner des commandes vocales pour contrôler des choses telles que les lumières, les serrures, les portes, les thermostats, les prises, les interrupteurs, les systèmes d'alarme, les couvertures de fenêtre, les capteurs du système d'arrosage, et plus encore... Même les appareils de cuisine et les fonctions de soins des animaux domestiques sont automatisés. Des entreprises fabriquent chaque jour de nouveaux produits destinés à fonctionner avec ces systèmes domotiques.



- **Bâtiments intelligents :** des entreprises de tous types utilisent la technologie intelligente pour automatiser les processus de construction. Les bâtiments intelligents déploient un grand nombre des mêmes technologies que les maisons intelligentes. Ces procédés permettent d'assurer un éclairage, une énergie, un chauffage, une climatisation et une sécurité efficaces. Par exemple, un bâtiment intelligent peut réduire les coûts énergétiques grâce à des capteurs qui détectent le nombre d'occupants d'une pièce et ajustent le chauffage ou la climatisation de manière appropriée.

Les bâtiments intelligents peuvent également se connecter et communiquer avec le réseau intelligent. Cela permet une gestion plus efficace des systèmes énergétiques.

- **IoT industriel et usines intelligentes :** L'IoT industriel (IIoT), rassemble des machines, des analyses avancées et des personnes. Il s'agit d'un réseau de dispositifs de fabrication et de capteurs connectés par des technologies de communication sécurisées et à haut débit. Il en résulte des systèmes capables de surveiller les processus, de collecter, d'échanger et d'analyser des données, et d'utiliser ces informations pour ajuster en permanence le processus de fabrication.

Nous sommes actuellement dans la quatrième révolution industrielle, ou ce qui est appelé Industrie 4.0 . Ce terme décrit un environnement dans lequel les machines et les équipements sont capables d'améliorer les processus grâce à l'automatisation et à l'auto-optimisation. L'industrie 4.0 va au-delà du processus de fabrication et s'étend à des fonctions telles que la planification, la logistique de la chaîne t de produits.

- **Villes intelligentes :** Qu'ont en commun Hambourg, Barcelone, Kansas City, Jaipur, Copenhague et Manchester ? Ce sont toutes des "villes intelligentes" qui utilisent la technologie numérique pour faire de leur ville un endroit où il fait bon vivre. Certaines de ces villes utilisent la technologie pour réduire les émissions de carbone ou surveiller les niveaux de C02. D'autres utilisent la technologie pour fournir un accès WI-FI gratuit dans toute la ville, améliorer la sécurité publique ou les options de transport.

- **Technologie des voitures intelligentes : la** plupart des nouveaux véhicules à moteur d'aujourd'hui intègrent une technologie qui aide les conducteurs à être plus sûrs sur la route. Il existe une technologie qui empêche les conducteurs de dériver dans les voies adjacentes ou de faire des changements de voie dangereux. Des systèmes appliquent automatiquement les freins si un véhicule qui les précède s'arrête ou ralentit soudainement. Les technologies de sécurité utilisent une combinaison

L'évolution continue de ces technologies a donné naissance aux systèmes de conduite automatisée (ADS), qui peuvent prendre en charge la totalité de la tâche de conduite lorsque nous ne voulons ou ne pouvons pas le faire nous-mêmes. Les véhicules à conduite autonome peuvent désormais fonctionner de manière totalement autonome, sans l'intervention d'un conducteur.

- **Magasins et services : Les** tâches qui étaient autrefois effectuées par des personnes sont aujourd'hui de plus en plus souvent réalisées par des machines. Les restaurants à service rapide installent des bornes en libre-service pour la prise de commande, les banques se tournent de plus en plus vers les guichets automatiques ou les applications conçues pour fonctionner sur les téléphones intelligents, et les supermarchés et les grands magasins ont installé des caisses en libre-service.
Des systèmes ont même été conçus pour surveiller le niveau des stocks et passer automatiquement des commandes afin d'adapter précisément l'offre à la demande et d'éliminer les stocks excédentaires.

- **Diagnostic médical et chirurgie :** La profession médicale s'appuie sur les médecins et les infirmières pour effectuer des tests et poser un diagnostic en fonction des résultats. Des systèmes ont été mis au point qui utilisent la technologie pour effectuer ces tests médicaux de manière précise et automatique. Ces systèmes effectuent ensuite des recherches dans des bases de données complètes en effectuant un grand nombre de calculs et de comparaisons. Le résultat est un diagnostic et un régime de traitement plus précis que ce que l'on pourrait imaginer.
possible à partir d'un seul individu. De plus, les machines sont maintenant utilisées pour contrôler plus précisément le traitement, ce qui minimise les dommages périphériques pour le patient.

- **Le pilote automatique d'un avion :** Les avions d'aujourd'hui sont construits pour voler eux-mêmes. Un ensemble complexe de systèmes automatise les opérations d'un avion. Après la saisie d'une trajectoire de vol, le système de pilotage automatique recueille des informations sur la route, l'emplacement, la vitesse de l'air, l'altitude et la poussée des moteurs. Il effectue des ajustements pour maintenir la sécurité de l'avion sur la trajectoire prévue. La redondance dans la conception des systèmes permet de s'assurer qu'une défaillance d'un seul système ne compromettra pas la sécurité des passagers.

5.1.1.3. Quand les choses commencent à penser

Les choses peuvent-elles penser ? Un dispositif peut-il apprendre de son environnement ? Dans ce contexte, il existe de nombreuses définitions du mot "penser". Une définition possible est la capacité de relier une série d'éléments d'information connexes, puis de les utiliser pour modifier un plan d'action.

Par exemple, lorsque nous sommes jeunes, nous n'avons aucune idée qu'un feu est chaud et que placer notre main dans le feu nous fera souffrir. Un feu peut sembler visuellement agréable et nous inciter à essayer de toucher les flammes. Nous apprenons rapidement que le feu peut causer des blessures. Nous commençons alors à associer l'image du feu à la douleur qu'il peut causer. À partir de ce moment, nous commençons à penser aux conséquences du contact avec le feu et nous basons nos actions sur cette information acquise.

De nombreux appareils intègrent désormais une technologie intelligente pour modifier leur comportement dans certaines circonstances. Cela peut être aussi simple qu'un appareil intelligent réduisant sa consommation électrique pendant les périodes de pointe ou aussi compliqué qu'une voiture à conduite autonome.

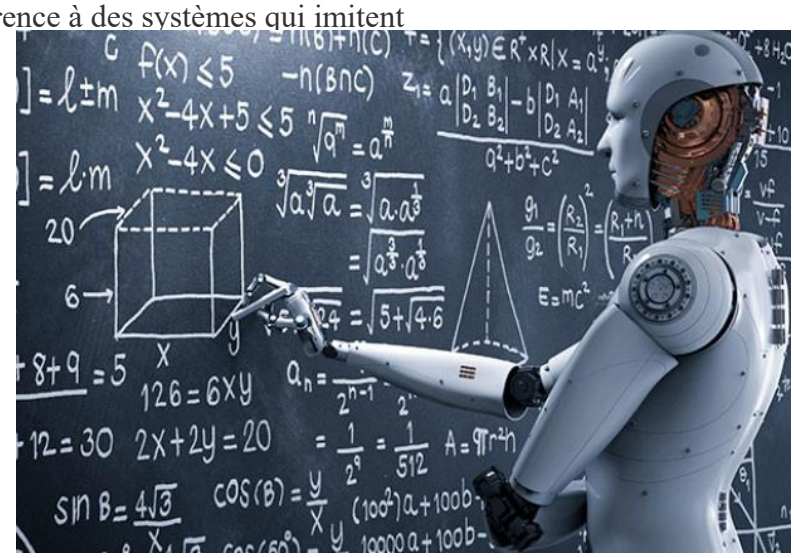
Lorsqu'une décision ou une action est prise par un appareil sur la base d'une information extérieure, cet appareil est qualifié d'appareil intelligent. De nombreux appareils avec lesquels nous interagissons ont désormais le mot "intelligent" dans leur nom. Cela signifie que l'appareil a la capacité de modifier son comportement en fonction de son environnement. Avec quelles technologies et quels appareils intelligents avez-vous interagi aujourd'hui ?

	Automation	Not Automation
The temperature and lighting in your home or business is adjusted based on your daily routine.		
You use a remote device to start your car.		
You use online banking to pay a bill.		
Robots are used in dangerous conditions such as mining, firefighting, and cleaning up industrial accidents, reducing the safety risk to humans.		
Production levels are automatically tied to demand eliminating unneeded product and reducing the impact on the environment.		
You adjust the volume on the television set with a remote control.		
Your GPS recalculates the best route to a destination based on current traffic congestion.		
A refrigerator senses that you are out of milk and places an order for more.		

5.1.2. Intelligence artificielle et apprentissage automatique

5.1.2.1. Qu'est-ce que l'intelligence artificielle et l'apprentissage automatique ?

L'intelligence artificielle (IA) est l'intelligence dont font preuve les machines. Elle s'oppose à l'intelligence naturelle, qui est l'intelligence dont font preuve les organismes vivants. L'IA utilise des agents intelligents qui peuvent percevoir leur environnement et prendre des décisions qui maximisent la probabilité d'atteindre un but ou un objectif spécifique. L'IA fait référence à des systèmes qui imitent les fonctions cognitives normalement associées à l'esprit humain, comme l'apprentissage et la résolution de problèmes.



Parmi les tâches qui, à l'heure actuelle, sont considérées comme nécessitant un certain degré d'IA, citons les voitures autonomes, le routage intelligent dans les réseaux de diffusion de contenu, les jeux stratégiques et les simulations militaires.
Avec le développement de la technologie, de nombreuses tâches qui, à une certaine époque, nécessitaient l'IA sont devenues routinières. Nombre de ces tâches sont passées de l'IA à l'apprentissage machine (ML).

La ML est un sous-ensemble de l'IA qui utilise des techniques statistiques pour donner aux ordinateurs la capacité d'"apprendre" de leur environnement. Cela permet aux ordinateurs d'améliorer une tâche particulière sans être spécifiquement programmés pour cette tâche.

Cela est particulièrement utile lorsque la conception et la programmation d'algorithmes spécifiques sont difficiles ou infaisables. Parmi les exemples de tâches de ce type en informatique, citons la détection de codes malveillants, la détection d'intrus dans les réseaux, la reconnaissance optique de caractères, la reconnaissance vocale par ordinateur et la vision par ordinateur.
L'un des objectifs de l'apprentissage est d'être capable de généraliser à partir de l'expérience. Pour les machines, cela implique la capacité d'exécuter avec précision de nouvelles tâches inédites après avoir acquis de l'expérience avec un ensemble de données d'apprentissage. L'ensemble de données d'apprentissage doit provenir de données représentatives d'un ensemble de données plus vaste. Cet ensemble de données permet à la machine de construire un modèle général sur ces données, ce qui l'aidera à faire des prédictions précises.

5.1.2.2. Le ML dans l'IoT

L'une des caractéristiques de l'IdO est qu'il permet de collecter des pools de données extrêmement importants qui peuvent "apprendre" aux programmes comment réagir dans certaines conditions. Parmi les utilisations les plus courantes de la technologie ML, citons :

- **Reconnaissance vocale** - De nombreuses entreprises proposent désormais des assistants numériques qui vous permettent d'utiliser la parole pour communiquer avec un système informatique. Apple, Microsoft, Google et Amazon proposent tous ce service. Ces sociétés permettent non seulement de donner des commandes verbalement, mais offrent également des capacités de conversion de la parole en texte.

- **Recommandation de produits** - Les systèmes établissent un profil de client et recommandent des produits ou des services en fonction des habitudes antérieures. Les utilisateurs d'Amazon et d'eBay reçoivent des recommandations sur des produits. Des organisations telles que LinkedIn, Facebook et GooglePlus recommandent des utilisateurs avec lesquels vous pourriez souhaiter entrer en contact.

- **Reconnaissance de formes** - Il existe des programmes qui permettent de convertir des diagrammes et des notes grossièrement dessinés à la main en diagrammes et textes plus formels. Cela permet de convertir les formes et les lignes de l'écriture manuelle en un texte plus formel qui peut ensuite être recherché et analysé.

- **Détection des fraudes par carte de crédit** - Un profil est établi sur les habitudes d'achat d'un client. Tout écart par rapport à ces habitudes déclenche une alerte et le système prend automatiquement des mesures. Cette action peut aller du refus de la transaction à la notification aux autorités. Parmi les événements qui sont détectés et qui pourraient indiquer une transaction frauduleuse, citons l'achat de produits qui ne sont pas achetés normalement, les achats dans une zone géographique différente, l'achat rapide de nombreux produits différents et l'achat d'articles à prix élevé.

- **Reconnaissance faciale** - Les caméras de sécurité sont partout, des magasins aux rues en passant par les aéroports et les centres de transport. Ces caméras scrutent en permanence les foules, normalement à l'affût d'activités dangereuses ou illégales, mais elles peuvent également être utilisées pour identifier et suivre des individus. Le système construit un modèle de caractéristiques faciales spécifiques et guette ensuite une correspondance avec ces modèles faciaux, ce qui déclenche une action.

Pensez à vos interactions avec des systèmes en ligne et hors ligne au cours de la semaine dernière. Avec combien d'applications ML avez-vous interagi ?

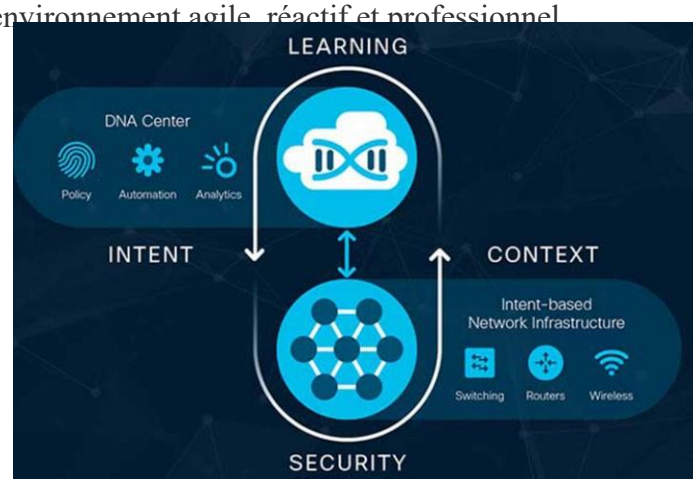
5.1.3. Mise en réseau basée sur les intentions

5.1.3.1. Qu'est-ce qu'un réseau basé sur l'intention (IBN)

Pour qu'une entreprise survive, elle doit être agile et répondre rapidement aux besoins et aux demandes de ses clients. Les entreprises sont de plus en plus dépendantes de leurs ressources numériques pour répondre aux demandes des clients. Le réseau informatique sous-jacent doit donc également être suffisamment réactif pour s'adapter rapidement à ces exigences. Cela implique normalement des ajustements de nombreux systèmes et processus. Ces ajustements peuvent inclure des modifications des politiques et procédures de sécurité, des services et applications d'entreprise et des politiques opérationnelles.

Avec les réseaux traditionnels, de nombreux composants différents doivent être ajustés manuellement pour répondre à des exigences commerciales en constante évolution. Cela exige que différents techniciens et ingénieurs veillent à ce que les systèmes soient modifiés de manière à ce qu'ils puissent travailler ensemble pour atteindre leur objectif. Cela entraîne parfois des erreurs et des retards, et souvent des performances réseau non optimales.

Le nouveau réseau d'entreprise doit intégrer de manière transparente et sécurisée les appareils IoT, les services basés sur le cloud et les bureaux distants dans un environnement agile, réactif et professionnel de manière pertinente. En outre, le réseau doit protéger ces nouvelles initiatives numériques contre les menaces en constante évolution.



Pour répondre à ce besoin, l'industrie informatique a entrepris de créer une approche systématique pour lier la gestion de l'infrastructure à l'intention de l'entreprise. Cette approche est connue sous le nom de mise en réseau basée sur l'intention. La figure illustre l'idée générale du réseautage basé sur l'intention. Avec ce nouveau paradigme, les besoins de l'entreprise sont automatiquement et continuellement traduits en exécution de l'infrastructure informatique.

5.1.3.2. Comment sont liés Ml, AI et IBN ?

Le réseau basé sur l'intention exploite la puissance de l'automatisation, de l'IA et du ML pour contrôler la fonction d'un réseau afin d'accomplir un objectif spécifique, ou intention.

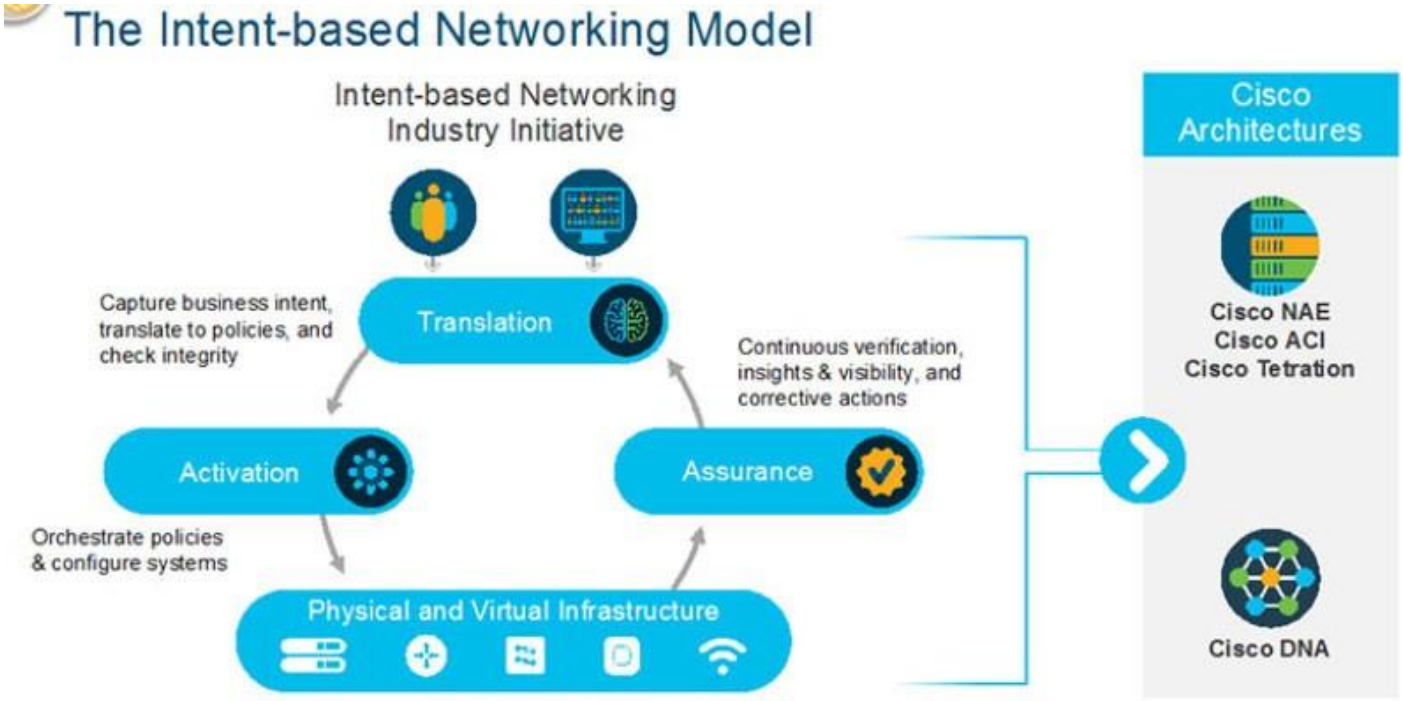
La mise en réseau basée sur les intentions permet à l'équipe informatique de spécifier, en langage clair, ce qu'elle veut exactement que le réseau accomplisse et le réseau s'en charge. Le réseau est capable de traduire l'intention en politiques, puis d'utiliser l'automatisation pour déployer les configurations appropriées requises sur le réseau. Le réseau basé sur l'intention utilise l'IA et le ML pour s'assurer que tous les services déployés respectent le niveau de service requis. S'ils ne respectent pas le niveau de service, le réseau basé sur l'intention peut émettre des alertes et fournir des suggestions d'amélioration. Dans certains cas, le réseau basé sur l'intention peut reconfigurer automatiquement le réseau pour respecter les niveaux de service.

Le modèle de mise en réseau basé sur l'intention présenté dans la figure se compose de trois éléments clés :

- **Assurance** - L'élément assurance est une vérification de bout en bout du comportement du réseau. Il prédit les résultats de tout changement, suit la conformité avec l'intention initiale et formule des recommandations ou des ajustements en cas de décalage entre l'intention et le résultat. Cette étape s'appuie fortement sur l'IA et le ML. Les systèmes font partie d'une boucle fermée qui surveille en permanence les performances et la sécurité du réseau, et reconfigure le réseau pour assurer la conformité.

- **Traduction** - L'élément de traduction est la capacité d'appliquer l'intention de l'entreprise à la configuration du réseau. L'intention est ce que vous souhaitez accomplir, et non la manière de l'accomplir. Cette intention est spécifiée en langage clair et utilisée par le système pour créer des politiques à travers le système. Par exemple, l'intention peut être de segmenter le trafic invité du trafic d'entreprise ou de permettre l'accès aux utilisateurs distants.

- **Activation** - L'élément d'activation intervient après que l'intention a été spécifiée et que les politiques ont été créées. C'est à ce moment que les dispositifs individuels sont provisionnés pour correspondre aux politiques basées sur l'intention. Il peut s'agir d'un mode automatisé ou semi-automatisé qui permet à l'équipe réseau de vérifier la configuration avant le déploiement des dispositifs.



Un réseau basé sur les intentions crée un réseau agile et réactif, qui évolue facilement et s'adapte aux besoins de l'entreprise. Il utilise efficacement des ressources hautement qualifiées et permet à l'homme et à la machine de travailler ensemble pour optimiser l'expérience du client. En outre, la mise en réseau basée sur l'intention offre une expérience numérique plus sûre en automatisant les processus longs ou compliqués. Le déploiement des politiques de sécurité s'en trouve grandement facilité.

5.1.3.3. Cas d'utilisation des réseaux basés sur l'intention

Le réseautage basé sur les intentions permet à l'entreprise de se concentrer sur ses objectifs commerciaux. Il fournit un système automatisé qui comprend les besoins de l'organisation et les concrétise.

L'architecture de réseau numérique Cisco (Cisco DNA) est un exemple de réseau basé sur l'intention. Il s'agit d'une architecture ouverte, extensible et pilotée par logiciel. Elle accélère et simplifie les opérations du réseau d'entreprise, tout en réduisant les coûts et les risques.

L'automatisation et l'assurance Cisco DNA reposent sur un contrôleur de réseau défini par logiciel (SDN), des analyses contextuelles riches, la virtualisation du réseau et l'évolutivité illimitée du cloud.

5.2. Résumé

Ce chapitre a débuté par une discussion sur l'automatisation. On entend par automatisation tout processus qui s'autoalimente et réduit, puis éventuellement élimine, le besoin d'intervention humaine. L'IdO ouvre un nouveau monde dans lequel des tâches nécessitant auparavant une intervention humaine peuvent être automatisées. De nombreux appareils intègrent désormais une technologie intelligente pour modifier leur comportement dans certaines circonstances. On trouve des exemples de technologies intelligentes dans les maisons et bâtiments intelligents, les villes, les réseaux électriques intelligents et les voitures intelligentes.

Ensuite, le chapitre détaille l'intelligence artificielle (IA). L'IA est l'intelligence dont font preuve les machines. Avec le développement de la technologie, de nombreuses tâches qui nécessitaient autrefois l'IA sont devenues routinières. Un grand nombre de ces tâches sont passées de l'IA à l'apprentissage machine (ML). L'apprentissage automatique est un sous-ensemble de l'IA qui utilise des techniques statistiques pour donner aux ordinateurs la capacité "d'apprendre" de leur environnement. Parmi les exemples de ML dans l'IdO, citons la reconnaissance vocale et faciale, la recommandation de produits et la détection de fraudes par carte de crédit.

Le sujet suivant de ce chapitre portait sur la mise en réseau basée sur les intentions (IBN). Le nouveau réseau d'entreprise doit intégrer les appareils IoT, les services basés sur le cloud et les bureaux distants d'une manière pertinente et réactive pour l'entreprise. Le réseau doit sécuriser ces nouvelles initiatives numériques face à un paysage de menaces en constante évolution. L'IBN est une approche systématique visant à lier la gestion de l'infrastructure à l'intention de l'entreprise.

Enfin, ce chapitre a abordé la manière dont le réseau basé sur l'intention utilise l'IA et le ML pour garantir que tous les services déployés respectent le niveau de service requis. Un modèle de réseau basé sur l'intention contient trois éléments, à savoir l'assurance, la traduction et l'activation. L'architecture de réseau numérique Cisco (Cisco DNA) est un exemple de réseau basé sur l'intention. Il s'agit d'une architecture ouverte, extensible et pilotée par logiciel.

6. Tout doit être sécurisé

6.1. La sécurité dans un monde numérisé

6.1.1.

6.1.1.1. Types de données

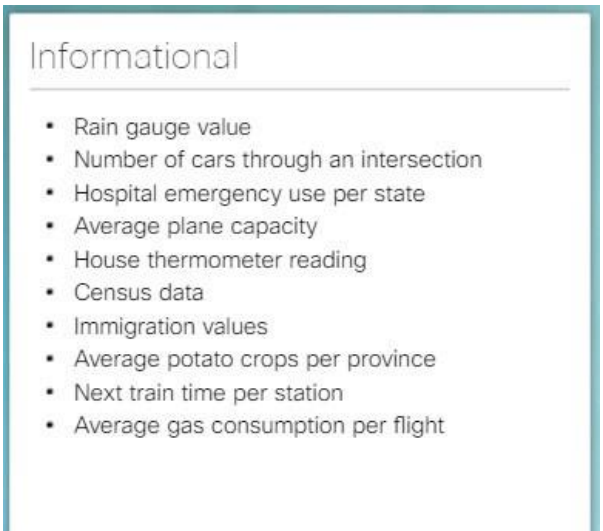
Les données ont-elles vraiment changé ? Eh bien, techniquement non, les données générées par les ordinateurs et les appareils numériques sont toujours des groupes de 1 et de 0. Cela n'a pas changé. Ce qui a changé, c'est la quantité, le volume, la variété et l'immédiateté des données générées.

Historiquement, les entreprises avaient accès à nos informations recueillies dans des formulaires, des feuilles de calcul, des applications, des achats par carte de crédit et d'autres types de fichiers. La plupart de ces informations étaient stockées et analysées ultérieurement. Les données sensibles étaient toujours collectées, stockées et analysées mais, historiquement, les pirates étaient plus intéressés par le piratage des systèmes pour obtenir les secrets des entreprises ou des gouvernements.

Aujourd'hui, les données recueillies prennent de nouvelles caractéristiques. Le monde numérisé a ouvert les vannes de la collecte de données. Les appareils dotés de capteurs IoT collectent de plus en plus de données à caractère personnel. Les trackers de fitness portables, les systèmes de surveillance du domicile, les caméras de sécurité et les transactions par carte de débit collectent tous des données personnelles ainsi que des données commerciales et environnementales. Les données sont souvent combinées à partir de différentes sources et les utilisateurs peuvent ne pas en avoir conscience. En combinant les données de surveillance de la condition physique avec les données de surveillance de la maison, on pourrait obtenir des points de données permettant de cartographier les mouvements ou l'emplacement d'un propriétaire. Ce nouveau type de collecte et d'agrégation de données peut être utilisé à bon escient pour aider l'environnement. Il accroît également les risques d'atteinte à la vie privée, d'usurpation d'identité et d'espionnage industriel.

Les informations personnellement identifiables (PII) ou les informations personnelles sensibles (SPI) sont toutes les données relatives à un individu vivant qui peuvent être utilisées seules ou avec d'autres informations pour identifier, contacter ou localiser un individu spécifique. Les données recueillies par les entreprises et les institutions gouvernementales peuvent également contenir des informations sensibles concernant des secrets d'entreprise, des brevets de nouveaux produits ou la sécurité nationale.

La collecte et le stockage de quantités exponentielles de données sensibles et informatives ont accru le besoin de sécurité supplémentaire pour protéger ces informations contre les catastrophes naturelles, les pirates informatiques et les abus.



6.1.1.2. Qui veut vos données ?

Les Bons Gars

Les entreprises légitimes ont mis en place un accord qui leur donne la permission d'utiliser les données collectées à votre sujet dans le but d'améliorer leur activité. Vous vous souvenez de ces documents intitulés "Conditions générales" ou "Conditions de service et accords" auxquels nous disons oui mais que nous ne lisons généralement pas ? La prochaine fois qu'on vous en présente un, prenez le temps de le lire. Son contenu pourrait vous surprendre.
D'autres utilisateurs légitimes de nos données seraient les entreprises qui utilisent des capteurs sur leurs propres appareils ou véhicules. Les gouvernements qui disposent de capteurs environnementaux et les villes qui ont installé des capteurs sur les trains, les bus ou les feux de circulation ont également un droit sur les données qu'ils génèrent.

Certains hackers, appelés white hat hackers, sont payés par des entreprises et des gouvernements légitimes pour tester la sécurité d'un appareil ou d'un système. Leur objectif n'est pas de voler ou de modifier des données, mais d'aider à les protéger.

Les méchants

D'autres pirates, appelés "black hat hackers", veulent accéder aux données collectées pour de nombreuses raisons infâmes :

- vendre les informations à un tiers.
- Pour modifier les données ou désactiver une fonctionnalité sur un appareil.
- Pour perturber ou porter atteinte à l'image d'une entreprise légitime.
- Accéder à des dispositifs, des pages web et des données pour créer une agitation politique ou faire une déclaration politique.
- Pour accéder aux identifiants et aux mots de passe des utilisateurs afin de voler des identités.
- Accéder à des données pour commettre un crime.
- Pour pirater les systèmes afin de prouver qu'ils peuvent le faire.


The Good Guys
Corporations
Government
The Bad Guys

6.1.1.3. Des données entre de mauvaises mains

- Les pirates informatiques ont accédé aux données de nombreuses entreprises au fil des ans. L'impact est important et a entraîné la diffusion sur le web des données de millions d'utilisateurs.

- Selon des informations récentes, les identifiants de connexion et d'autres données personnelles liées à plus d'un million de comptes yahoo et gmail seraient proposés à la vente sur le marché du dark web.
  Les comptes en ligne mis en vente sur le Dark Web auraient contiennent des noms d'utilisateur, des courriels et des mots de passe en clair. Les comptes ne proviennent pas d'une seule violation de données, mais de plusieurs cyberattaques majeures.

- Des cybercriminels ont pénétré dans Equifax (EFX), l'une des plus grandes agences d'évaluation du crédit, en juillet 2017 et ont volé les données personnelles de 145 millions de personnes. Elle a été considérée comme l'une des pires brèches de tous les temps en raison de la quantité d'informations sensibles exposées, notamment les numéros de sécurité sociale.
  La société n'a révélé le piratage que deux mois plus tard. Il pourrait avoir un impact pendant des années, car les données volées pourraient être utilisées pour le vol d'identité.

- La brèche de 2018 a touché environ 150 millions d'utilisateurs de son application d'alimentation et de nutrition, MyFitnessPal. L'enquête indique que les informations affectées peuvent inclure des noms d'utilisateur, des adresses e-mail et des mots de passe hachés.

- San Francisco (fin 2016) - Uber a révélé mardi que des pirates avaient volé 57 millions de comptes de conducteurs et de passagers et que l'entreprise avait gardé la violation de données secrète pendant plus d'un an après avoir payé une rançon de 100 000 dollars. La violation a coûté à Uber de l'argent et de la réputation.

- Anatomie d'une attaque IoT : https://cisco-netacad.wistia.com/medias/jjnqkypamu

6.1.2. Protéger le web d'entreprise

6.1.2.1. Meilleures pratiques en matière de sécurité

La sécurisation du réseau implique l'ensemble des protocoles, technologies, dispositifs, outils et techniques qui sécurisent les données et atténuent les menaces. La sécurité des réseaux est largement motivée par la volonté de garder une longueur d'avance sur les pirates informatiques mal intentionnés. Tout comme les médecins tentent de prévenir les nouvelles maladies tout en traitant les problèmes existants, les professionnels de la sécurité des réseaux tentent de prévenir les attaques potentielles tout en minimisant les effets des attaques en temps réel. Les réseaux font régulièrement l'objet d'attaques. Il est courant de lire dans les journaux qu'un autre réseau a été compromis.

Les politiques, procédures et normes de sécurité doivent être respectées lors de la conception de tous les aspects du réseau dans son ensemble. Cela doit inclure les câbles, les données en transit, les données

stockées, les dispositifs de mise en réseau et les dispositifs finaux.

Quelques bonnes pratiques en matière de sécurité :

- **Effectuez une évaluation des risques :** Connaître la valeur de ce que vous protégez vous aidera à justifier les dépenses de sécurité.
- **Créez une politique de sécurité :** Créez une politique qui décrit clairement les règles de l'entreprise, les fonctions et les attentes.
- **Mesures de sécurité physique :** Restreindre l'accès aux actifs du réseau dans les armoires de réseau et les emplacements des serveurs. Installer des systèmes d'extinction d'incendie appropriés.
- **Mesures de sécurité des ressources humaines :** Les employés doivent faire l'objet d'une recherche appropriée avec vérification des antécédents.
- **Effectuer et tester les sauvegardes :** Effectuez des sauvegardes régulières et testez la récupération des données à partir des sauvegardes.
- **Maintenir les correctifs et les mises à jour de sécurité :** Mettez régulièrement à jour le système d'exploitation et les programmes des serveurs et des périphériques réseau.
- **Mettre en place des contrôles d'accès :** Configurez les rôles des utilisateurs et les niveaux de privilège ainsi que l'authentification forte des utilisateurs.
- **Testez régulièrement la réponse aux incidents :** Employez une équipe de réponse aux incidents et testez les scénarios de réponse d'urgence.
- **Mettre en œuvre un outil de surveillance, d'analyse et de gestion du réseau** : Choisissez une solution de surveillance de la sécurité qui s'intègre à d'autres technologies.
- **Mettre en œuvre des dispositifs de sécurité réseau :** Utilisez des routeurs de nouvelle génération, des pare-feu et d'autres dispositifs de sécurité.
- **Mettez en œuvre une solution complète de sécurité des points d'extrémité :** utilisez un logiciel anti-malware et antivirus de niveau entreprise.
- **Former les utilisateurs :** Formez les utilisateurs et les employés aux procédures de sécurité.
- **Cryptage des données :** Cryptez toutes les données sensibles de l'entreprise, notamment

6.1.2.2. Sécurité physique

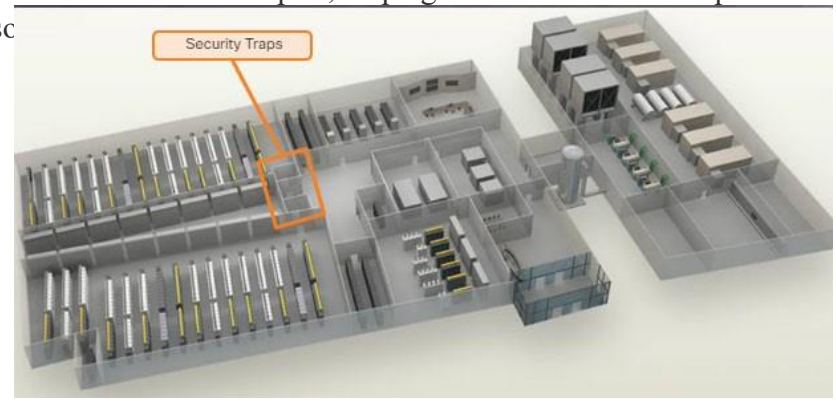
Les centres de données d'aujourd'hui stockent de grandes quantités d'informations sensibles et critiques pour l'entreprise ; la sécurité physique est donc une priorité opérationnelle. La sécurité physique protège non seulement l'accès aux locaux, mais aussi les personnes et les équipements. Par exemple, des alarmes incendie, des gicleurs, des baies de serveurs renforcées contre les séismes et des systèmes redondants de chauffage, ventilation et climatisation (CVC) et d'alimentation sans coupure sont en place pour protéger les personnes et les équipements.
La figure 1 montre une représentation d'un centre de données. Liste des éléments :

- **Baies de serveurs renforcées contre les séismes :** Pour protéger les personnes et les équipements en cas de tremblement de terre.
- **Agents de sécurité sur site :** Contrôle et application des politiques de sécurité.
- **Clôtures et portails :** Assurer la sécurité du périmètre pour empêcher les intrus d'entrer
- **Surveillance vidéo continue :** Fournir une surveillance de la sécurité en temps réel
- **Détecteurs de mouvement électroniques :** Fournissent des détecteurs de sécurité à l'intérieur.
- **Alarmes de violation de la sécurité : Les** alarmes générées dans le centre de contrôle de l'installation informent le personnel du centre de données d'un accès physique non autorisé à l'installation.
- **Pièges de sécurité :** Système intérieur permettant d'enfermer un intrus, également appelé piège à hommes.
- **Capteurs biométriques d'accès et de sortie :** Fournit deux formes d'authentification.

- **Systèmes d'extinction d'incendie à base de gaz :** Pour protéger les personnes et les équipements en cas d'incendie.
- **Environnement contrôlé HVAC redondant :** Pour protéger les personnes et les équipements en cas de panne du système CVC primaire.
- **Onduleur de secours :** Pour protéger les personnes et les équipements pendant une panne de courant.

La sécurité physique au sein du centre de données peut être divisée en deux zones, l'extérieur et l'intérieur.

- **Sécurité du périmètre extérieur** - Il peut s'agir d'agents de sécurité sur place, de clôtures, de barrières, de vidéosurveillance permanente et d'alarmes en cas de violation de la sécurité.
- **Sécurité du périmètre intérieur** - Il peut s'agir d'une surveillance vidéo continue, de détecteurs de mouvement électroniques, de pièges de sécurité et de capteurs biométriques d'accès et de sc



Les trappes de sécurité permettent d'accéder aux salles où sont stockées les données du centre de données. Comme le montre la figure, les trappes de sécurité sont similaires à un sas. Une personne doit d'abord entrer dans le piège de sécurité à l'aide de la carte de proximité de son badge d'identification. Une fois que la personne est à l'intérieur du piège de sécurité, la reconnaissance faciale, les empreintes digitales ou d'autres vérifications biométriques sont utilisées pour ouvrir la deuxième porte. L'utilisateur doit répéter le processus pour sortir du hall de données.

Cette figure montre les exigences biométriques du centre de données Cisco Allen, à Allen, au Texas.

6.1.2.3. Les défis de la sécurisation des dispositifs IoT.

Les dispositifs IoT sont développés avec les capacités de connectivité réseau nécessaires, mais souvent, ils ne mettent pas en œuvre une sécurité réseau forte. La sécurité du réseau est un facteur critique lors du déploiement de dispositifs IoT. Des méthodes doivent être prises pour garantir l'authenticité, l'intégrité et la sécurité des données, le chemin entre le capteur et le collecteur, et la connectivité à l'appareil.

Non-Traditional Location of Devices - Some connected IoT devices are able to interact with the physical world. They are now located in appliances, in automobiles, on or in our bodies, and in our homes. Sensors may gather data from the refrigerator or the heating system. They could also be located in city lampposts or attached to tree trunks. These non-traditional locations make physical security difficult or impossible to achieve. The devices should be manufactured to be resistant to tampering, and they should be placed so that they are not obvious and are very difficult to access.

Increasing Number of Devices - The number of interconnected sensors and smart devices is growing exponentially, increasing the opportunity for attacks. Sensors and smart devices tend to be small devices, with varying operating systems, CPU types, and memory. Many of these entities are expected to be inexpensive, single-function devices with rudimentary network connectivity.

Lack of Upgradeability - IoT sensor-enabled devices may be located in remote and/or inaccessible locations where human intervention or configuration is almost impossible. The devices are often designed to be in service many years longer than is typical for conventional high-tech equipment. Some IoT devices are intentionally designed without the ability to be upgraded, or they might be deployed in situations that make it difficult or impossible to reconfigure or upgrade. New vulnerabilities are uncovered all of the time. If a device is non-upgradeable, then the vulnerability will exist for the rest of its lifetime. If a device is upgradeable, the typical consumer may not have a technology background, therefore, the upgrade process should perform automatically or be easy enough to be performed by a layperson.

6.1.2.4. Utilisation sécurisée du Wi-fi

Les réseaux sans fil sont populaires dans les entreprises de tous types et de toutes tailles car ils sont faciles à installer et pratiques à utiliser. Pour les employés et les invités, l'entreprise doit offrir une expérience sans fil qui permet la mobilité et la sécurité. Si un réseau sans fil n'est pas correctement sécurisé, les pirates à portée de main peuvent y accéder et s'infiltrer dans le réseau.

Mesures à prendre pour protéger le réseau sans fil de votre entreprise :

- **Modifiez le mot de passe administrateur par défaut :** les mots de passe forts doivent comporter plus de 8 chiffres et être composés de lettres, de chiffres et de caractères spéciaux.
- **Modifiez le SSID du réseau :** le nom d'un réseau sans fil est appelé identifiant de l'ensemble des services. Les routeurs sans fil sont généralement livrés avec un SSID par défaut, ce qui rend le réseau vulnérable aux attaques.
- **Ne pas publier le nom du SSID :** la plupart des routeurs sans fil publient le nom du SSID. Les employés auraient connaissance du nom du SSID par l'intermédiaire de l'entreprise.
- **Créez un réseau filaire pour les invités :** Pour les entreprises qui ont besoin d'un accès invité, il est important de séparer le réseau invité du réseau des employés.
- **Activez le pare-feu intégré :** La plupart des routeurs sans fil ont un pare-feu intégré, mais il arrive qu'ils soient livrés avec le pare-feu désactivé. Assurez-vous que le pare-feu du routeur est activé.
- **Configurez le routeur sans fil pour utiliser le cryptage WPA2-AES :** Chaque routeur sans fil propose un cryptage qui brouille vos données et les rend illisibles pour tous, sauf pour le destinataire prévu. L'accès protégé Wi-Fi 2 (WPA2) est le meilleur car il utilise l'algorithme de cryptage le plus difficile à percer.

- **Maintenez le micrologiciel du routeur sans fil à jour** : Lorsque vous mettez à jour le micrologiciel de votre routeur sans fil, les bogues et les vulnérabilités connus sont corrigés, ce qui rend votre routeur plus sûr.
- **Utilisez le filtrage des adresses MAC** : Si seuls les employés utilisent un réseau sans fil particulier, configurez votre routeur sans fil pour qu'il vérifie les adresses MAC des appareils qui tentent de s'y connecter et qu'il n'autorise que les connexions des appareils qu'il reconnaît.
- **Désactivez la fonction de gestion à distance du routeur sans fil** : De nombreux routeurs sans fil disposent d'une fonction qui
  vous permet de les gérer à distance. Malheureusement, elle rend souvent les routeurs vulnérables aux attaques. Désactivez la gestion à distance si vous n'avez pas besoin d'utiliser cette fonction.
- **Protégez physiquement le routeur sans fil** : Assurez-vous que le routeur se trouve dans un endroit sûr et qu'il est seulement
  accessible par le personnel autorisé.

6.1.2.5. Protection des dispositifs

- **Maintenez le pare-feu actif :** Qu'il s'agisse d'un pare-feu logiciel ou d'un pare-feu matériel sur un routeur, le pare-feu doit être activé et mis à jour pour empêcher les pirates d'accéder à vos données personnelles ou à celles de votre entreprise.

- **Gérez votre système d'exploitation et votre navigateur :** Les pirates tentent toujours de tirer parti des vulnérabilités de vos systèmes d'exploitation et de vos navigateurs web. Pour protéger votre ordinateur et vos données, réglez le paramètre de sécurité de votre ordinateur et de votre navigateur sur moyen ou supérieur. Mettez à jour le système d'exploitation de votre ordinateur, y compris vos navigateurs web, et téléchargez et installez régulièrement les derniers correctifs logiciels et mises à jour de sécurité des fournisseurs.

- **Utilisez un antivirus et un antispyware : Les** logiciels malveillants, tels que les virus, les chevaux de Troie, les vers, les rançongiciels et les logiciels espions, sont installés sur vos appareils informatiques sans votre permission, afin d'avoir accès à votre ordinateur et à vos données. Les virus peuvent détruire vos données, ralentir votre ordinateur ou prendre le contrôle de votre ordinateur. Ne téléchargez des logiciels qu'à partir de sites Web fiables pour éviter de contracter des virus et des logiciels espions. Un logiciel antivirus est conçu pour analyser votre ordinateur et les courriers électroniques entrants à la recherche de virus et les supprimer. Parfois, un logiciel antivirus comprend également un anti logiciel espion. Maintenez votre logiciel à jour pour protéger votre ordinateur contre les logiciels malveillants les plus récents.

- **Protégez tous vos appareils :** Vos appareils informatiques, qu'il s'agisse de routeurs, de PC, d'ordinateurs portables, de tablettes ou de smartphones, doivent être protégés par un mot de passe pour éviter tout accès non autorisé. Les informations stockées doivent être cryptées, en particulier pour les données sensibles ou confidentielles. Pour les

appareils mobiles, ne stockez que les informations nécessaires, au cas où ces appareils seraient volés ou perdus lorsque vous vous absentez de votre domicile. Si l'un de vos appareils est compromis, les criminels peuvent avoir accès à toutes vos données par l'intermédiaire de votre fournisseur de services de stockage en nuage, comme Icloud ou Google drive.

6.1.3 Sécuriser les données et les dispositifs personnels

6.1.3.1. Maisons intelligentes

La technologie de la maison intelligente est devenue très populaire et sa popularité augmente chaque année à mesure que la technologie évolue. Qui ne trouve pas attrayant d'augmenter ou de diminuer le thermostat de sa maison pendant qu'il est au travail, ou de demander à son réfrigérateur de commander des courses qui seront livrées à son retour à la maison ? N'est-ce pas génial de pouvoir surveiller le chien ou de vérifier que vos adolescents font leurs devoirs après l'école en activant les caméras de sécurité de votre maison ?

En installant de plus en plus de capteurs intelligents dans nos maisons, nous augmentons le risque de problèmes de sécurité. Souvent, les capteurs sont connectés au même réseau que les appareils de notre foyer ou de notre petite entreprise, de sorte qu'une faille dans un appareil peut se propager et affecter tous les appareils connectés. Les capteurs peuvent également permettre aux pirates de pénétrer dans notre réseau domestique et d'accéder à tous les PC et à toutes les données qui y sont connectés.
Même les assistants virtuels tels que Apple SIRI, Amazon Echo ou Google Home peuvent présenter des risques pour la sécurité. Les gens utilisent ces appareils pour mettre de la musique, régler la température d'une pièce, commander des produits en ligne et obtenir des indications sur leur destination. Cela peut-il causer des dommages ? Il est possible que des informations personnelles telles que des mots de passe ou des informations sur les cartes de crédit soient divulguées.

Heureusement, bon nombre des failles de sécurité des premiers capteurs de la technologie intelligente ont déjà été découvertes. Les développeurs s'efforcent de corriger ces failles et d'améliorer les mesures de sécurité pour protéger leurs systèmes contre les attaques. Avant d'acheter un système de sécurité domestique, il est très important de faire des recherches sur le développeur et sur les protocoles de sécurité et de cryptage mis en place pour ses produits.

6.1.3.2. Points d'accès publics

Lorsque vous n'êtes pas chez vous, un hot spot Wi-Fi public vous permet d'accéder à vos informations en ligne et de surfer sur Internet. Parmi les activités courantes sur un Wi-Fi public, citons la connexion à un compte de messagerie personnel, la saisie d'informations d'identification personnelle, la connexion à des médias sociaux et l'accès à des informations bancaires ou financières. Toutes ces informations peuvent être volées si la connexion Wi-Fi n'est pas sécurisée.

Règles de sécurité à suivre si vous utilisez un point d'accès Wi-Fi public ou non sé

- N'accédez pas et n'envoyez pas d'informations personnelles sensibles sur un réseau public sans fil.
- Vérifiez si votre ordinateur est configuré pour le partage de fichiers et de médias, et s'il requiert une authentification de l'utilisateur avec chiffrement.
- Utilisez des tunnels et des services de réseau privé virtuel (VPN) cryptés. Le service VPN vous fournit un accès sécurisé à l'Internet, avec une connexion cryptée entre votre ordinateur et le serveur VPN du fournisseur de services VPN. Avec un tunnel VPN crypté, même si une transmission de données est interceptée, elle n'est pas déchiffrable.

De nombreux appareils mobiles, tels que les smartphones et les tablettes, sont équipés du protocole sans fil

Bluetooth. Cette capacité permet aux appareils compatibles Bluetooth de se connecter les uns aux autres et de partager des informations. Malheureusement, Bluetooth peut être exploité par des pirates pour écouter certains appareils, établir des contrôles d'accès à distance, distribuer des logiciels malveillants et vider les batteries. Pour éviter ces problèmes, désactivez la fonction Bluetooth lorsque vous ne l'utilisez pas.

6.1.3.3. Configurer un VPN sur les Smartphones

Un VPN est un réseau sécurisé utilisant une connexion Internet cryptée qui agit comme un "tunnel" sécurisé pour les données. Il peut être créé sur la connexion Internet publique pour permettre aux utilisateurs de cacher leur identité lorsqu'ils utilisent l'Internet. Vous devriez utiliser un service VPN lorsque vous vous connectez à un réseau Wi-Fi qui n'est pas le vôtre (par exemple, à la bibliothèque ou dans un café). Il empêche les autres personnes présentes sur ce réseau public d'écouter votre utilisation du Web lorsque vous utilisez des sites Web ou des communications non sécurisés.

De nombreuses entreprises exigent un accès VPN à leurs réseaux internes si les employés travaillent à distance ou sont mobiles. L'employé recevra le client VPN, ainsi que les informations relatives à l'ID utilisateur et au mot de passe. Pour ceux qui n'ont pas accès à un VPN d'entreprise, il existe de nombreuses applications de service VPN pour smartphone que vous pouvez télécharger gratuitement ou moyennant un abonnement mensuel. Exemples de ces applications VPN
incluent : ExpressVPN, NordVPN, et TunnelBear.

Si vous disposez d'un VPN professionnel ou si vous téléchargez une application de service VPN, ils vous fourniront les informations et l'assistance nécessaires pour configurer votre VPN.

How to manually set up a VPN from the Android settings

Step 1 • Unlock your phone.
Step 2 • Open the **Settings** app.
Step 3 • Under the **Wireless & networks** section, select **More**.
Step 4 • Select **VPN**.
Step 5 • At the top-right corner you will find a plus sign (+), tap it.
Step 6 • Your network administrator will provide you with all your VPN information.Simply select your desired protocol and 'enter all the information.
Step 7 • Tap **Save**.
Step 8 • You can connect by going back to the VPN settings and selecting your VPN of choice. You will be asked to enter a username and password.
Step 9 •You can also hit the 3-dot menu button to set your VPN to always be on.

How to manually set up a VPN on your iPhone or iPad

Step 1 • Launch **Settings** from your Home screen.
Step 2 • Tap **General**.
Step 3 • Tap **VPN**.
Step 4 • Tap **Add VPN Configuration**. If you have one already configured, select the **VPN client** you want to use and toggle the **Status** switch on.
Step 5 • Tap **Type**.
Step 6 • Select your **VPN type** from IKEv2, IPsec, or L2TP
Step 7 • Tap **Add Configuration** in the upper left corner to go back to the previous screen.
Step 8 • Enter the **VPN settings information** including description, server, and remote ID
Step 9 • Enter your **authentication login** including your username (or certificate), and password.
Step 10 • If you use a proxy, enable it by tapping **Manual** or **Auto**, depending on your preferences.
Step 11 • Tap **Done**.
Step 12 • Under VPN Configurations, toggle the **Status** switch on.

6.2. Résumé

Ce chapitre a débuté par une discussion sur les types de données. Les informations personnellement identifiables (PII) ou les informations personnelles sensibles (SPI) sont toutes les données relatives à une personne vivante qui peuvent être utilisées seules ou avec d'autres informations pour identifier, contacter ou localiser une personne spécifique. Les entreprises légitimes disposent d'un accord (conditions générales ou conditions de service) qui leur donne la permission d'utiliser les données collectées à votre sujet dans le but d'améliorer leurs activités. D'autres utilisateurs légitimes de nos données seraient des entreprises qui utilisent des capteurs sur leurs propres appareils ou véhicules. Les gouvernements qui disposent de capteurs environnementaux et les villes qui ont installé des capteurs sur les trains, les bus ou les feux de circulation ont également un droit sur les données qu'ils génèrent.

Certains hackers, appelés white hat hackers, sont payés par des entreprises et des gouvernements légitimes pour tester la sécurité d'un appareil ou d'un système. Leur objectif n'est pas de voler ou de modifier des données, mais d'aider à les protéger. Les hackers "black hat" veulent accéder aux données collectées pour de nombreuses raisons, notamment pour les vendre, porter atteinte à la réputation d'une personne ou d'une entreprise et provoquer des troubles politiques.

Ensuite, le chapitre détaille les meilleures pratiques en matière de sécurité. La sécurité comprend la sécurisation physique des périmètres extérieurs et intérieurs des lieux, tels que les centres de données, où les données sont stockées. La sécurisation des dispositifs IoT est un défi en raison de leur nombre, du fait qu'ils se trouvent dans des endroits non traditionnels et que beaucoup d'entre eux ne peuvent pas être mis à niveau.

Les pirates informatiques accèdent fréquemment aux réseaux Wi-Fi disponibles. Il existe de nombreuses mesures que vous pouvez prendre pour protéger le réseau sans fil de votre entreprise. Pour protéger les appareils, gardez le pare-feu activé, gérez votre système d'exploitation et votre navigateur, et utilisez un antivirus et un antispyware.

Règles de sécurité à suivre si vous utilisez un point d'accès Wi-Fi public ou non sécurisé :

- N'accédez pas et n'envoyez pas d'informations personnelles sensibles sur un réseau public sans fil.
- Vérifiez si votre ordinateur est configuré pour le partage de fichiers et de médias, et s'il requiert une authentification de l'utilisateur avec chiffrement.
- Utilisez des tunnels et des services de réseau privé virtuel (VPN) cryptés. Le service VPN vous fournit un accès sécurisé à l'Internet, avec une connexion cryptée entre votre ordinateur et le serveur VPN du fournisseur de services VPN. Avec un tunnel VPN crypté, même si une transmission de données est interceptée, elle n'est pas déchiffrable.

En installant de plus en plus de capteurs intelligents dans nos maisons, nous augmentons le risque de problèmes de sécurité. Souvent, les capteurs sont connectés au même réseau que les appareils de notre foyer ou de notre petite entreprise, de sorte que la violation d'un appareil peut se propager et affecter tous les appareils connectés.

7. Complément d'information

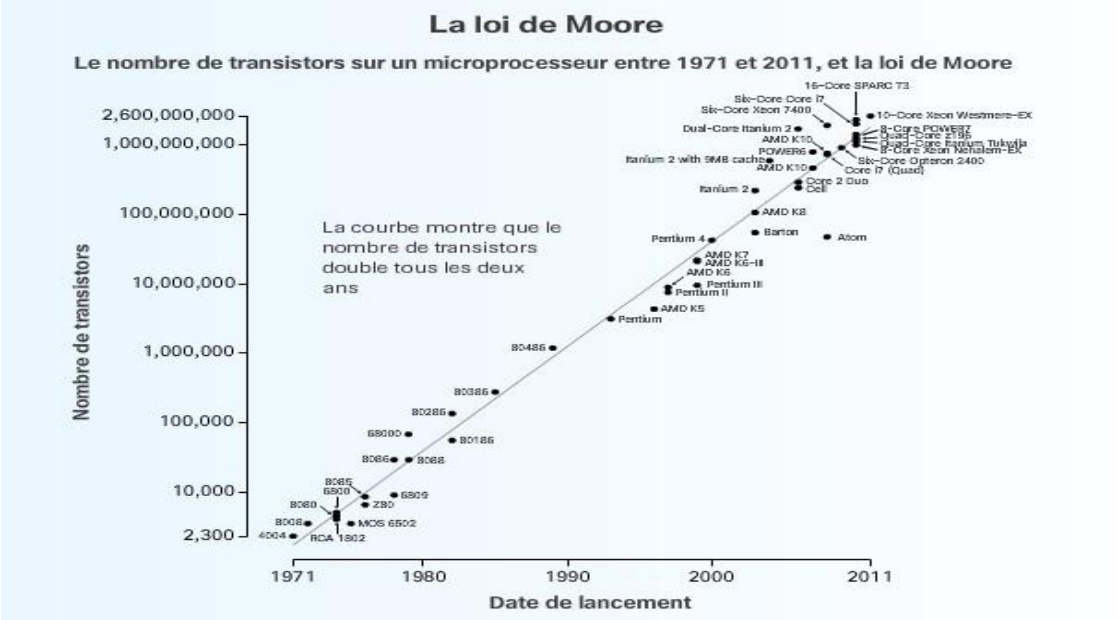
7.1. Les lois

7.1.1. Croissance technologique

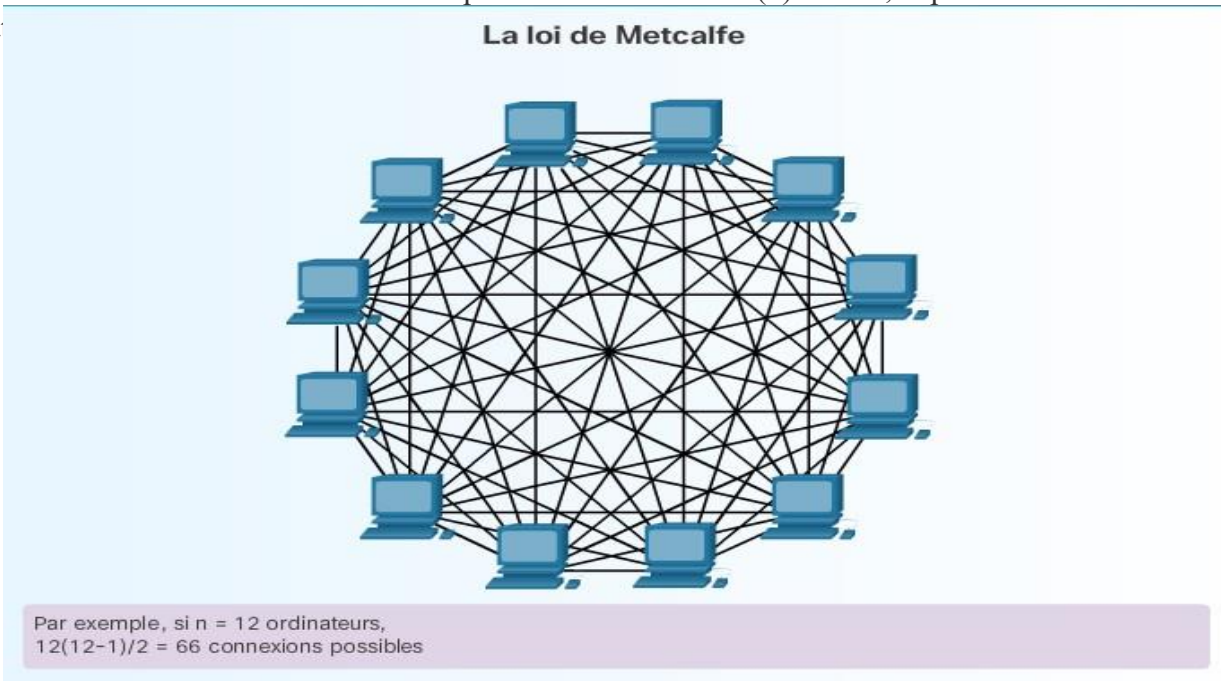
Aujourd'hui, le rythme de la croissance technologique s'accélère de manière exponentielle. Pour conserver un avantage concurrentiel, les organisations doivent être en mesure de tenir compte de cette croissance.

Il existe trois principes fondamentaux, appelés lois, que les organisations et les experts peuvent utiliser pour les aider à planifier leurs besoins technologiques :

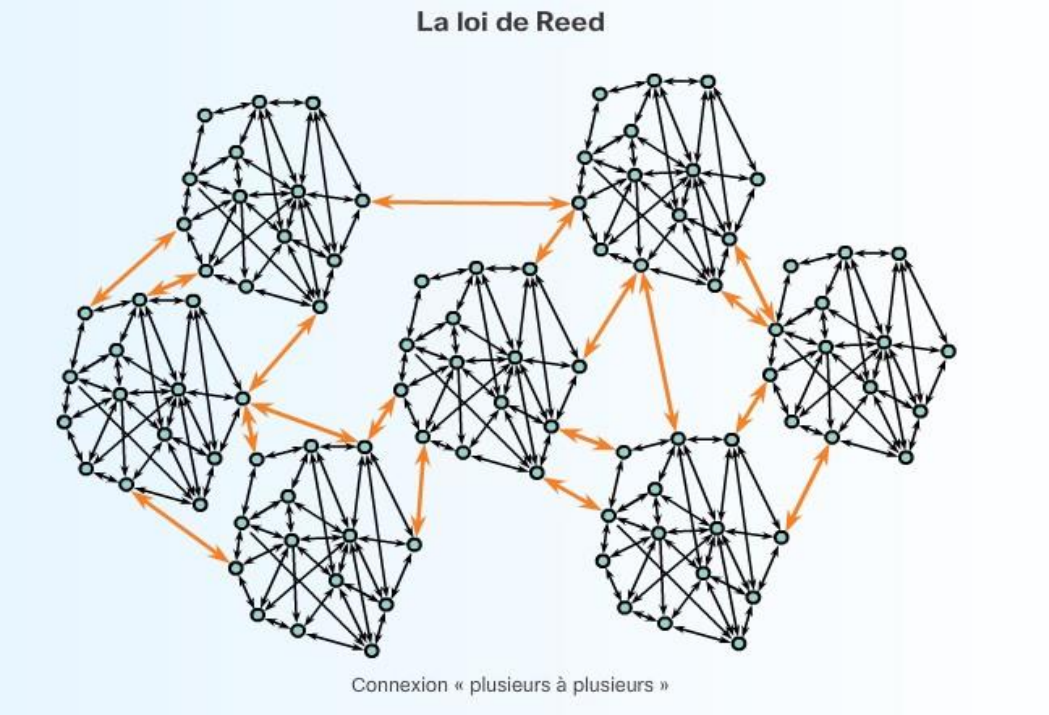
- **La loi de Moore :** Cette loi a été proposée par Gordon E. Moore, cofondateur d'Intel, en 1965. Elle stipule que le nombre de transistors sur les circuits intégrés a tendance à doubler tous les deux ans, ce qui augmente la capacité de traitement.



- **Loi de Metcalfe :** Cette loi est attribuée à Robert Metcalfe. Elle stipule que la valeur d'un réseau donné est proportionnelle au carré du nombre d'utilisateurs qui y sont connectés. La loi de Metcalfe concerne le nombre de connexions uniques dans un réseau de (n) nœuds, exprimé ma



- **La loi de Reed :** Cette loi a été proposée par David Reed. Elle stipule que la valeur du réseau croît de manière exponentielle si l'on additionne tous les groupes potentiels de deux personnes, de trois personnes, etc. que les membres pourraient former.

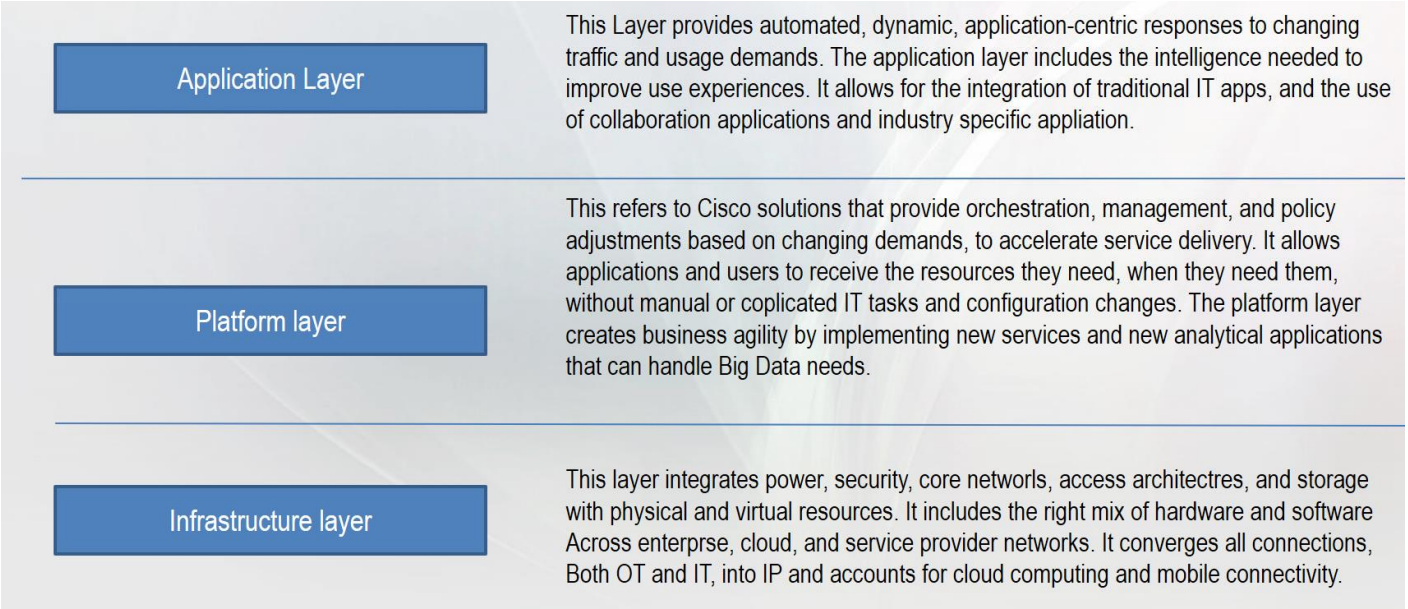


La loi de Metcalfe est fréquemment mentionnée pour expliquer la croissance explosive de l'internet. Ensemble, les lois de Metcalfe et de Moore constituent une base solide pour expliquer la présence et la valeur sans cesse croissantes des technologies de l'information dans la vie quotidienne des gens.

7.1.2. L'approche architecturale IoE

L'approche architecturale de Cisco pour l'IoE est organisée en trois couches fonctionnelles. La couche application dépend de la couche plate-forme, qui dépend de la couche infrastructure. Cliquez sur chaque couche de la figure pour plus d'informations sur son rôle dans l'approche architecturale de l'IoE.

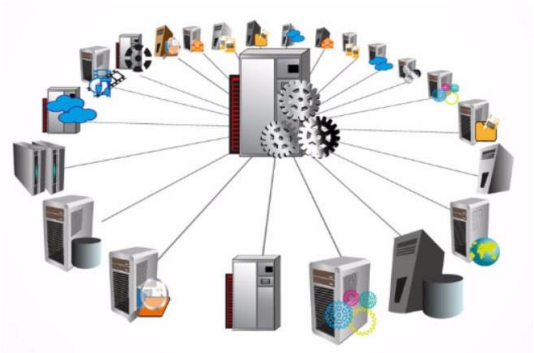
Cette approche architecturale reflète les modèles de services du modèle de l'informatique en nuage, en tirant parti du logiciel en tant que service (SaaS), de la plate-forme en tant que service (PaaS) et de l'infrastructure en tant que service (IaaS).



7.1.3. Stockage des données

Trois principaux types de stockage de données :

- **Données locales :** Désigne les données auxquelles on accède directement, par des dispositifs locaux. Les disques durs, les lecteurs flash USB et les disques optiques sont des exemples de stockage de données locales.



- **Données centralisées** : Données qui sont stockées et partagées à partir d'un seul serveur centralisé. Ces informations peuvent être consultées à distance par de multiples dispositifs sur le réseau ou sur Internet. L'utilisation d'un serveur de données centralisé peut entraîner des goulots d'étranglement et des inefficacités, et peut devenir un point de défaillance unique.

- **Données distribuées** : Données qui sont gérées par un système de gestion de bases de données distribuées (DDBMS).
  Les données distribuées sont des données qui sont répliquées et stockées à plusieurs endroits. Cela permet un partage facile et efficace des données. L'accès aux données distribuées se fait par le biais d'applications locales et globales. Avec un système distribué, il n'y a pas de source unique de défaillance. En cas de panne de courant sur un site, les utilisateurs peuvent toujours accéder aux données stockées sur les autres sites.