COMPRENDRE L'EXPLOSION DE L'IoT ET SON IMPACT SUR LA SÉCURITÉ DES ENTREPRISES

Les entreprises et les organismes publics adoptent une transformation numérique qui réinvente les modèles de vente pour mieux servir les clients et dynamiser la croissance. L'adoption rapide des nouvelles technologies et des innovations contribue à repenser les processus de vente de manière globale et à créer de nouvelles façons de générer de meilleurs résultats opérationnels et des améliorations de la qualité de vie. Ce phénomène s'appelle la 4ème révolution industrielle. Il s'agit d'une période d'amélioration soutenue de la productivité résultant de l'innovation et de la combinaison de technologies qui fait apparaître de nouveaux modèles de vente.

À l'ère de l'industrie 4.0, les processus industriels et les machines associées sont de plus en plus intelligents et modulaires, tandis que de nouveaux protocoles, comme l'UPC UA (Open Platform Communications Unified Architecture), permettent à des équipements de commande précédemment isolés, de communiquer entre eux, créant ainsi un réseau hyperconnecté à travers plusieurs écosystèmes industriels. Il en résulte des niveaux d'utilisation supérieurs et une plus grande flexibilité pour répondre à la demande des clients.

L'Internet des objets (IoT), le cloud computing et l'omniprésence du haut débit constituent les principales technologies permettant cette transformation numérique. Les objets intelligents toujours connectés dotés d'un accès instantané aux informations contextuelles, ainsi que les appareils et les applications possédant une intelligence artificielle et conçus pour optimiser les processus et améliorer notre façon de vivre, de travailler et d'interagir les uns avec les autres, permettent tous de modifier notre manière de concevoir, de produire, de fournir et de consommer des biens et des services.

L'industrie 4.0 entraînera des modifications révolutionnaires conséquentes tant au niveau de l'offre que de la demande, car les clients et les entreprises ont une influence et un pouvoir d'achat accru sur un ensemble étendu de fournisseurs. Une plus grande intégration des processus de vente se traduit par une prise de décision accélérée et la nécessité de suivre le rythme de l'évolution rapide du marché. Les entreprises recherchent de plus en plus à accroître plus rapidement leur productivité pour ne pas perdre leur pertinence avec l'émergence de nouveaux concurrents. Le développement mondial d'Uber en tant que leader du transport et la perturbation qui en a découlé chez les services de taxi traditionnels constitue un exemple de la façon dont DX peut radicalement réorganiser les marchés.

DÉFI INHÉRENT À LA SÉCURITÉ DE L'IoT

L'IoT change la donne en matière de sécurité. Tout évolue plus vite que nous ne le pensons et de nombreux fournisseurs de sécurité ne sont pas préparés. Du fait de l'interconnectivité omniprésente entre les appareils, les utilisateurs et les réseaux distribués, ce que nous appelons désormais un écosystème, les appareils de sécurité habituellement compartimentés et ne protégeant qu'un seul emplacement du réseau, s'avèrent de plus en plus inefficaces. Pire encore pour la plupart des équipes informatiques, de nombreuses normes de sécurité traditionnelles et meilleures pratiques ne permettent pas de relever les défis de l'IoT.

Sur le plan de la sécurité, les fabricants d'IoT n'aident pas. Dans la pratique, la plupart des appareils d'IoT ne sont pas conçus d'un point de vue sécuritaire. En fait, la plupart des appareils d'IoT ne disposent pas d'interface graphique et n'ont donc pas de système d'exploitation traditionnel, ou même de mémoire et de puissance de traitement indispensables à l'intégration d'un système de sécurité ou à l'installation d'un client de sécurité.

25 %

des attaques touchant les entreprises cibleront l'IoT

L'EXPLOSION DES DONNÉES D'IoT

Plus d'un million de nouveaux appareils IoT se connectent quotidiennement à Internet et cette tendance s'accélère. Les experts prédisent que 25 à 50 milliards de nouveaux appareils IoT compatibles Internet seront déployés et en ligne d'ici à 2020. L'IoT a ainsi créé une explosion des données conçues pour circuler librement entre les appareils et les emplacements, et entre les environnements réseaux, les bureaux distants, les travailleurs mobiles et les environnements de cloud public, compliquant l'uniformité du suivi et de la sécurisation.

Le trafic traditionnel mondial des datacenters est actuellement mesuré en zettaoctets et devrait plus que tripler pour atteindre 15,3 Zo par an en 2020. Cependant, d'après Forbes, le volume total de données générées par l'IoT atteindra 600 Zo par an d'ici 2020, soit 275 fois plus que le trafic prévu entre les datacenters et les appareils/utilisateurs finaux (2,2 Zo), et 39 fois plus que le trafic total prévu des datacenters (15,3 Zo). Du fait de la vague de données structurées et non structurées qui en résultera, mêmes les plus importantes équipes de sécurité rencontreront des difficultés à identifier un comportement anormal au sein des écosystèmes mondiaux des villes et entreprises intelligentes.

Ces changements ont déjà commencé à mettre à l'épreuve les points d'accès, les réseaux et les datacenters saturés, sans parler du personnel informatique débordé. Les cybercriminels, qui continuent de chercher à exploiter les liaisons les plus faibles de la chaîne de données, n'ont pas manqué de le remarquer. C'est pourquoi, d'ici 2020, plus de 25 % des attaques touchant les entreprises devraient cibler l'IoT.

Comme nous avons pu le constater dans les deux récentes attaques massives contre l'IoT, ces appareils sont vulnérables : collecte des informations qu'ils contiennent, installation d'un piège pour propager des attaques de type DDoS, injection d'un code ciblé, altération physique de leur micrologiciel, attaques de type man-in-the-middle, modification ou désactivation de leurs fonctionnalités par des appareils de contrôle à distance, usurpation d'autres appareils IoT ou simplement dissimulation d'autres logiciels malveillants dans le volume des données IoT.

De plus, les entreprises font désormais converger des réseaux autrefois parallèles (y compris des réseaux informatiques, opérationnels et l'IoT) afin de rationaliser les données et les informations en temps réel. Ceci leur permet d'être plus réactives face aux besoins de leurs clients. Cependant, les modèles de sécurité traditionnels ont du mal à fournir les protections requises car les calculs et les données circulent entre les appareils périphériques et le cloud. Cette convergence de réseaux distribués, du traitement et de la sécurité entraîne la consolidation des périphériques vers des plateformes capables d'automatiser le partage des informations sur les menaces, de collaborer à la détection et à l'isolation des menaces, ainsi que d'orchestrer en temps réel la réponse aux incidents.

TENDANCES EN MATIÈRE D'IoT

La plupart d'entre nous n'ont qu'une vague connaissance de l'IoT. Lorsque nous sommes interrogés, nous pensons majoritairement que les appliances intelligentes et les véhicules connectés fournissent aux utilisateurs des informations connexes. Mais ce n'est que la face la plus visible de l'IoT. Au-delà des personnes qui se connectent à Internet de manière traditionnelle via des réseaux, les réseaux en expansion de milliards d'appareils connectés collectent et partagent des données pour prendre des décisions de manière autonome ou semi-autonome. Ces décisions et micro-transactions automatisées au sein de l'économie numérique commencent à relancer la productivité et la croissance qui constituent la marque de l'industrie 4.0. L'IoT et la convergence connexe de réseaux distribués, du traitement et de la sécurité connectent rapidement chaque facette de nos vies et modifient nos façons de communiquer, de faire du business et de jouer. Voici un bref aperçu de plusieurs tendances émergentes autour de l'IoT, ainsi que des risques potentiels qui en résultent en termes de sécurité.

ANALYSE DES DONNÉES

Le principal avantage de l'IoT pour les entreprises prend la forme d'informations en temps réel et d'analyses des données conduisant à une amélioration des capacités de prise de décision. Une productivité accrue et de nouvelles opportunités commerciales conduiront à une croissance hautement novatrice pour les entreprises et les organismes publics qui pourront ainsi pleinement exploiter la puissance de leurs données. Cependant, ces données dans leur forme brute ne sont pas très utiles. C'est pourquoi, selon ABI Research, les entreprises dépenseront plus de 26 % du coût total de leur solution d'IoT dans des technologies et services de stockage, d'intégration, de visualisation et d'analyse des données d'IoT d'ici à 2020, soit près du double des dépenses actuelles.

L'un des postes à forte demande concernera les analystes de données qui peuvent élaborer des algorithmes pour déchiffrer et analyser ces données afin de recueillir les informations stratégiques. En s'appuyant sur ces mêmes données de recherche, la nature actuellement particulièrement manuelle des activités des analystes de données implique que le coût de l'analyse professionnelle devrait représenter plus d'un tiers des dépenses en analyse et en données d'IoT des entreprises d'ici 2021.

Il est assez facile de prédire que la grande percée dans l'IoT sera l'automatisation d'encore plus d'activités manuelles en rapport avec l'analyse. L'efficacité que l'automatisation peut apporter aux analystes des données permettra de résoudre des problèmes de plus en plus complexes. Ainsi, les employés et les entités commerciales seront mieux armés pour utiliser les données d'analyse afin d'améliorer la productivité et l'efficacité. L'automatisation de l'analyse permettra également aux entreprises novatrices de s'affranchir de la concurrence grâce à une réduction de leurs coûts totaux d'analyse, et d'offrir des offres et des services inégalés, plus réactifs et de qualité.

Bien sûr, l'automatisation de l'analyse requiert une plateforme permettant d'absorber facilement de nouvelles données, d'ajuster les modèles d'analyse en temps réel et même d'automatiser l'analyse prescriptive automatique. Ces solutions seront très onéreuses au départ. De plus, du fait de leur nature propriétaire et du décalage grandissant en termes de disponibilité d'analystes de données compétents, ces processus et données vont naturellement s'imposer comme une cible à haute valeur ajoutée pour les cybercriminels et l'espionnage industriel.

LES APPLICATION ENABLEMENT PLATFORMS

Les Application enablement platforms (AEP) (AEP) ont été créées pour simplifier l'extraction des données des appareils et des machines, transmettre ces données efficacement via le réseau et les convertir en formulaire facilement utilisable par une application d'IoT pour maintenir les stocks en flux tendu, réinitialiser les priorités dans l'usine de fabrication ou fournir des mises à jour stratégiques aux consommateurs des données. Enfin, bon nombre de ces AEP font converger les réseaux opérationnels et informatiques traditionnellement distincts. Les implications en termes de sécurité sont significatives.

Les réseaux opérationnels sont souvent plus vulnérables que les réseaux informatiques. Ils utilisent fréquemment des systèmes d'exploitation et des appareils propriétaires et existants qui n'ont peut-être jamais été conçus pour être compatibles avec un réseau IP; une simple analyse des appareils, sans parler d'un ciblage par un logiciel malveillant pourrait suffire à les interrompre. Si c'est une chose de pirater un site Web ou de voler des données, arrêter une usine de fabrication opérationnelle peut s'avérer désastreux pour une entreprise. Au cours des dernières années, les attaques qui ont provoqué la destruction de fours industriels, de centrifugeuses et d'ordinateurs sont le signe avant-coureur de ce qui peut se produire.

GESTION ET IDENTITÉ DES OBJETS

Le nombre d'appareils IoT augmentant, les entreprises voudront inévitablement que les objets participent à plusieurs écosystèmes, interagissent entre eux et puissent accéder à de nouveaux services. Nous constatons déjà que les fournisseurs de services et d'appareils IoT sur les marchés des systèmes domotiques, des véhicules connectés, des loisirs et de la santé mobile commencent à interconnecter leurs appareils et leurs services.

L'identité des objets est stratégique pour faciliter ces opportunités. En effet, l'identité des objets simplifie la création de services de gestion des objets et peut développer les opportunités disponibles via l'analyse croisée des plateformes d'activation des applications (AEP).

Étant donné qu'il est difficile, voire impossible de sécuriser de nombreux appareils IoT simples, l'identité et l'authentification des objets est en première ligne de la sécurité de l'IoT. Les solutions de sécurité doivent être en mesure d'identifier et d'analyser les objets qui se connectent au réseau à la vitesse

du câble. Elles doivent ensuite déterminer les règles à appliquer à ces objets et les acheminer de manière dynamique vers les segments de réseau appropriés et protégés. Ces informations doivent être partagées au sein de la security fabric afin de pouvoir appliquer les politiques connexes en tout point de l'écosystème distribué, détecter et bloquer rapidement les comportements anormaux, et mettre en œuvre immédiatement les modifications apportées à la politique indépendamment de l'emplacement d'un appareil IoT ou de ses données.

TRAITEMENT PÉRIPHÉRIQUE

Traditionnellement, les données d'IoT sont collectées par un capteur distant et transmises à un environnement cloud, où elles sont conservées ou utilisées à l'aide de règles commerciales ou d'analyses sophistiquées. Une analyse approfondie de ces données d'IoT permet de créer de nouveaux produits et services, ainsi que d'exécuter des analyses prédictives et prescriptives.

Cependant, les lois du marché imposent de plus en plus d'exécuter le traitement sur le site de l'appareil et non via un transit par le datacenter central. Le traitement périphérique permet de limiter la quantité de données renvoyées vers le cloud, réduisant par la même les coûts de connectivité sur les réseaux payants, ainsi que les coûts de stockage des données, d'analyse et d'intégration. Étant donné la nature de certaines applications, comme le freinage automatique des véhicules intelligents qui permet d'éviter les collisions, le traitement périphérique est obligatoire car l'application ne peut pas attendre l'analyse et la réponse du cloud.

En outre, le volume important de données provenant des capteurs et des appareils intelligents submergera rapidement les réseaux et les datacenters si le traitement de toutes les données doit être centralisé. Les capteurs et les autres appareils intelligents génèrent de nombreux petits paquets de données qui ne sont pas toujours gérés de manière optimale en inondant simplement le datacenter.

De même, les modèles de données traditionnels (pour lesquels de nombreuses solutions de sécurité existantes ont été conçues) nécessitent la création d'informations dans le datacenter, puis leur transmission en périphérie pour utilisation par les employés et les clients. Cependant, comme les appareils IoT et les capteurs commencent à fournir une analyse à la périphérie, ils modifient fondamentalement la polarité des données de manière à mieux équilibrer la création et la consommation des données entre la périphérie et les datacenters.

Ces appareils périphériques agrègeront les données, prendront des décisions autonomes ou semi-autonomes, puis seulement, parfois, retransmettront ces données au cloud pour une analyse supplémentaire pouvant entraîner l'envoi de cyber-instructions à un ou plusieurs appareils IoT. L'analyse périphérique devrait ainsi générer presque autant de données que le datacenter.

Voici deux exemples des avantages pouvant résulter du traitement périphérique via l'IoT :

Les véhicules sans conducteur seront reliés de manière bidirectionnelle aux systèmes GPS, météo et de circulation, ainsi qu'à un réseau maillé d'autres véhicules connectés. Ils pourront ainsi prendre des décisions localement en une fraction de seconde, par exemple pour éviter un nid-de-poule, puis partager cette information en temps réel pour permettre aux autres véhicules d'éviter ce même risque et aux municipalités de prévoir une réparation routière d'urgence.

Les villes intelligentes réfléchiront à comment optimiser et redéployer dynamiquement l'énergie et les autres ressources, comme la circulation routière et les places de parking. La collecte et l'analyse des données permettra de déterminer divers paramètres, notamment : est-ce que l'activation des lampadaires plus tôt dans la soirée permet de diminuer la criminalité dans un secteur de la ville ? Est-ce que réduire ou rallonger la durée de stationnement dans les parcmètres en journée génèrera davantage de trafic pédestre et augmentera en conséquence le revenu des commerçants du centre-ville ?

Cette modification de la collecte, du traitement et de l'analyse des données, ainsi que de la prise de décision, étendra également considérablement la surface potentielle d'attaque. Les appareils intelligents connectés peuvent potentiellement télécharger ou répandre des logiciels malveillants notamment capables d'affecter la circulation urbaine, interrompre des infrastructures stratégiques ou mettre les passagers de véhicules en danger. De même, un ransomware distribué pourrait éventuellement arrêter des infrastructures stratégiques ou empêcher l'utilisation de véhicules ou d'appareils médicaux.

Relever ce défi nécessitera que les sociétés de sécurité, les opérateurs de télécommunications/téléphonie et les prestataires de services collaborent car l'IoT devra fonctionner à l'échelle de l'écosystème des réseaux déployés, y compris le Wi-Fi, l'infrastructure sans fil, les réseaux locaux, les réseaux étendus dans le métro et les satellites.

TECHNOLOGIES LPWA ET LORA

Les technologies de connectivité LPWA (Low-Power Wide-Area) et LoRa (Long-Range) sont les dernières d'un portefeuille qui comprend déjà les technologies cellulaire, sans fil à courte portée, satellite et filaire fixe. Les normes LoRa sont entrées récemment en vigueur tandis que les technologies LPWA normalisées devraient être disponibles courant 2017 d'une manière générale.

Outre les opportunités sur les marchés établis comme le comptage intelligent, la domotique et l'automatisation des bâtiments commerciaux, les technologies LPWA et LoRa rendent les solutions d'IoT accessibles aux marchés émergents de la surveillance du suivi des actifs, de l'agriculture et de l'environnement. Ces solutions fournissent une connectivité longue portée supérieure à 15 km, une capacité élevée qui peut actuellement prendre en charge jusqu'à 1 million de nœuds, une durée de vie de la batterie supérieure à 10 ans et une réduction de la surcharge de synchronisation sans rebonds sur des réseaux maillés.

Ces solutions facilitent également les nouvelles idées comme l'émergence de l'économie de partage dans laquelle il est possible de partager des biens personnels au sein de la communauté ou de les prêter moyennant finance à des individus. Dans les économies de partage, il est possible de suivre et de surveiller tous les objets (tondeuses, motoculteurs, planches de surf, bicyclettes, outils, instruments musicaux, etc.) grâce aux technologies LPWA à moindre coût par rapport aux technologies sans fil existantes.

Les risques vont du simple fait de localiser et désactiver des appareils connectés à la détermination de la localisation des biens de valeur pour introduire et répandre rapidement un logiciel malveillant sur ces réseaux d'appareils connectés, et à la transformation en piège de ces biens pour notamment permettre des attaques de type DDoS.

GESTION DES RISQUES

Autre défi auquel de nombreuses entreprises sont confrontées : la multiplication de différents systèmes de sécurité. Des douzaines d'appareils isolés dotés d'une

interface de gestion distincte constituent également une contrainte lorsque les ressources informatiques sont limitées. Au cours des dernières années, les directeurs de la sécurité informatique se sont concentrés sur la consolidation de leurs ressources en matière de sécurité, passant des appareils aux plateformes. De fait, ils ont ainsi réduit le nombre d'appareils de sécurité déployés dans les grandes entreprises de 70 environ à une trentaine. Cependant, avec l'apparation du cloud et de l'IoT, ainsi que la création et la promotion d'outils de sécurité spécialisés pour ces environnements, nous sommes sur le point de connaître une nouvelle expansion du nombre d'appareils de sécurité, virtuels ou matériels, déployés.

Pour que la cybersécurité soit efficace, les entreprises doivent protéger les objets déjà déployés, les objets en cours de déploiement et les objets qui n'ont pas encore été déployés dans des scénarios auxquels elles n'ont encore jamais pensé. Aujourd'hui, elles doivent pouvoir détecter et contrer des menaces avancées en moins de 10 minutes avant de subir un préjudice irréparable. Et ce délai ne cesse de diminuer jour après jour.

Les entreprises doivent comprendre leur profil de risque : quel niveau de risque sont-elles en mesure d'absorber et quel niveau doivent-elles transférer aux MSSP ou aux fournisseurs de cyber-assurance. Comme le nombre de brèches de données très médiatisées augmente, les conseils de direction prennent de plus en plus conscience de leur responsabilité financière et la cybersécurité est devenue un exercice de gestion des risques. Les directeurs de la sécurité informatique se concentrent sur la gestion des risques associés à des objectifs commerciaux qui changent. Ils mesurent ainsi le risque associé aux appareils, services et protocoles qu'ils doivent mettre en œuvre pour satisfaire leurs objectifs, puis expriment leur tolérance à ce risque et mettent en place un plan pour le prévenir.

Enfin, pour être compétitif dans cette nouvelle économie numérique, les entreprises doivent pouvoir rassembler automatiquement les informations inhérentes à ce qui se passe sur leur réseau informatique, des opérations, IoT et de cloud privé et public. La sécurité requiert d'avoir une visibilité sur cet écosystème de réseaux, de collecter et de corréler les informations sur les menaces et d'intervenir automatiquement pour bloquer les menaces quel que soit le chemin d'attaque de l'écosystème emprunté.

À partir de la fin des années 1990, nous avons approché la sécurité en appliquant une stratégie de prévention (construction de murs et de fossés autour des réseaux pour maintenir les acteurs mal intentionnés à l'extérieur et protéger les informations). La sophistication et l'habileté croissantes des menaces à franchir le périmètre nous ont conduit à nous adapter via des améliorations incrémentielles (passage de la sécurité du réseau, à la sécurité des informations, puis à la sécurité des données). Nous savons désormais que même les meilleures défenses ne peuvent pas arrêter des menaces avancées déterminées et des campagnes d'attaque. Le nombre de brèches très médiatisées est une preuve que la prévention, bien qu'importante, n'est tout simplement pas suffisante. La cybersécurité est un domaine opérationnel multidimensionnel. En effet, pour le département américain de la défense et l'OTAN, Internet est le nouveau domaine opérationnel après les airs, la terre et la mer.

Les exigences relatives à la cybersécurité couvrent cinq points clés :

- *L'identification : comprendre le profil de risque et l'état actuel*
- *La protection : appliquer les stratégies de prévention pour contrer les vulnérabilités et les menaces*
- *La détection : détecter les anomalies et les événements*
- *La réponse : réagir face aux incidents, neutraliser et améliorer*
- *La reprise : l'amélioration continue du cycle de vie*

La cybersécurité englobe les trois piliers de la sécurité : la confidentialité, l'intégrité et la disponibilité.. Elle doit toutefois désormais dépasser ces exigences pour prendre en charge les problèmes inhérents à l'environnement, l'état et la sécurité physiques. L'ajout de l'IoT à nos réseaux nécessite notamment la prise en charge de la sécurité physique, de la continuité d'activité et de la reprise après sinistre pour des objets comme les véhicules sans conducteur ou intelligents, les systèmes CVC connectés, les appareils médicaux en ligne (pacemakers, pompes à perfusion, etc.) ou les réseaux urbains interconnectés.

UNE SECURITY FABRIC

Bien que de nombreux défis relatifs à la sécurité accompagnant la transformation numérique, ainsi que l'adoption de l'IoT et du cloud soient nouveaux, il est possible de les gérer en combinant les meilleures pratiques éprouvées, ainsi qu'un cadre de sécurité optimisé. Au cœur de la sécurisation de ces nouveaux écosystèmes hautement distribués figurent l'authentification et la surveillance haut débit ; la segmentation interne conçue pour surveiller et protéger l'interconnexion et le traitement distribués, et pour appliquer et coordonner une sécurité distribuée; et les services de sécurité sur le cloud qui permettent de suivre et de protéger les appareils et les données distribués à travers internet. La sécurité doit rassembler l'intégralité du réseau distribué et connecter les données et les appareils IoT à la périphérie, via le cœur du système et le datacenter, ainsi que vers le cloud.

La sécurisation de l'IoT et la transformation numérique nécessiteront une visibilité automatique du datacenter vers le cloud et l'IoT. Elles devront être combinées à des fonctions de détection avancées gérées par les informations sur les menaces qui facilitent l'intervention pour prévenir les menaces à la vitesse du système. La Fortinet Security Fabric s'adapte aux environnements distribués et intégrés afin de protéger le réseau de bout en bout, d'étendre et de garantir la résilience, et sécuriser les ressources de traitement (y compris le routing et l'optimisation WAN) pour garantir la connexion sécurisée d'un appareil IoT à l'environnement de cloud approprié. Cette approche permet aux entreprises de surveiller efficacement le trafic légitime, de vérifier l'authentification et l'identification, et d'imposer la gestion des accès à l'échelle de l'environnement distribué via une architecture de sécurité intégrée, synchronisée et automatisée.

9 février 2017