Protéger le potentiel de l'Internet des objets

Notre engagement

L'Internet des objets (IoT) est au cœur de l'engagement de Cisco. Nous sommes convaincus que l'IoT va révolutionner notre société grâce aux progrès des soins médicaux, de l'automatisation de la production industrielle, de la fiabilité et de l'efficacité de la distribution d'eau et d'énergie, et bien plus encore.

Chaque année, le cancer du sein tue 500 000 femmes dans le monde. Pourtant, s'il était dépisté suffisamment tôt, les chances de guérison seraient bien plus grandes. Imaginez, par exemple, un vêtement capable d'identifier les premiers signes de la maladie. C'est ce que propose l'iTBra. Ce soutien-gorge intelligent détecte la baisse de l'activité métabolique qui indique la progression du cancer. Les données des capteurs sont transmises vers le cloud pour être analysées et dépister la maladie le plus tôt possible.

Ce n'est plus l'IoT de demain dont il est question ici, mais bien de l'IoT d'aujourd'hui.

La problématique

Pour tenir toutes ses promesses, l'Internet des objets doit être sécurisé. Plus facile à dire qu'à faire. En effet, l'ampleur de la tâche est liée à deux facteurs majeurs : les vulnérabilités intrinsèques et l'évolutivité de l'IoT.

Les failles de sécurité des appareils connectés à l'IoT font l'objet de gros titres alarmistes, et ce n'est pas une surprise. Ce problème de sécurité s'explique de plusieurs façons :

- L'immaturité et la méconnaissance des fabricants en matière de sécurité
- Le manque de ressources système pour assurer la sécurité de manière native
- La pression des marchés et des concurrents, en particulier pour les appareils courants, qui pousse à supprimer des fonctionnalités de cybersécurité

Peu importe les raisons pour lesquelles un appareil ne peut pas se protéger, une vulnérabilité reste une vulnérabilité. Et c'est l'opportunité pour un hacker d'exploiter l'appareil pour accéder à votre réseau, où il pourra installer un programme malveillant, voler votre propriété intellectuelle ou commettre bien d'autres méfaits. Ces menaces sont bien réelles et toujours d'actualité, avec des conséquences diverses et variées :

- **Dommages matériels :** une cyberattaque contre une aciérie en Europe a endommagé un haut-fourneau valant plusieurs millions de dollars. Le malware a contraint les opérateurs à arrêter l'appareil immédiatement pour des raisons de sécurité, contournant ainsi le long processus de refroidissement contrôlé.[1]
- **Interruption de l'infrastructure critique :** suite à une attaque multidimensionnelle, un fournisseur d'électricité a perdu le contrôle de son réseau. Pendant six heures, plusieurs régions d'un pays d'Europe de l'Est ont ainsi été privées d'électricité. Les systèmes de gestion qui commandent le réseau électrique ont notamment été bloqués par un malware.[2]
- **Perturbation des soins de santé :** après avoir arrêté leurs systèmes le temps de trouver une solution pour contrer une infiltration de malware, des hôpitaux britanniques ont été obligés de reporter des opérations chirurgicales, annuler des rendez-vous et réaffecter des patients atteints de traumatismes importants.[3]

Selon nos prévisions, il devrait y avoir 30 milliards d'« objets » connectés d'ici 2020, soit autant d'appareils à protéger. Aujourd'hui, les entreprises sont vraiment exposées. Il suffit d'effectuer une recherche sur Shodan pour le constater. Et nous ne pouvons pas attendre sans rien faire que le problème se résolve de lui-même.

Appliquer aujourd'hui les solutions de demain

Heureusement, des solutions peuvent être mises en œuvre dès aujourd'hui. Pour cela, les problèmes doivent être abordés sous quatre angles majeurs :

- **La segmentation logicielle :** même si les VLAN classiques ont leur utilité, ils ne peuvent pas évoluer de façon à répondre au trafic imposé par l'IoT. Avec une segmentation logicielle évolutive et extensible, accompagnée de politiques applicables en fonction notamment du type d'appareil, du type d'utilisateur, du lieu et de l'heure, les entreprises ont davantage de visibilité, de contrôle et de fonctions d'automatisation pour protéger leur activité et s'adapter aux imprévus.
- **La visibilité et l'analyse :** la détection des appareils, des applications et des utilisateurs, ainsi que l'analyse des paquets de données et l'identification des menaces basée sur les comportements suspects dans l'ensemble de votre environnement, sont autant d'atouts pour repérer rapidement les menaces et y remédier avant qu'elles ne touchent les activités de l'entreprise.
- **L'accès à distance sécurisé :** même si une meilleure connectivité contribue à réduire les coûts de prise en charge des utilisateurs distants, mobiles et tiers, tout en leur permettant d'être plus efficaces, cela présente également des risques. Avec un accès à distance entièrement sécurisé, vous pouvez protéger les communications et contrôler l'activité des utilisateurs connectés au réseau.
- **Les services techniques et de conseil :** une entreprise a toujours besoin de conseils, que ce soit à certaines étapes ou pour l'intégralité d'un projet. Les chances de réussite sont, en effet, bien plus grandes lorsque des services de conseil sont proposés dès le départ.

Segmentation logicielle

Pourquoi segmenter les appareils connectés à l'IoT ? Grâce à la segmentation, les appareils sont hors de portée des cybercriminels et ne peuvent pas servir de passerelle pour parcourir le réseau s'ils sont compromis.

La segmentation du réseau a déjà fait ses preuves et compte parmi les bonnes pratiques en matière de sécurité. Utilisés depuis des décennies, les VLAN occupent toujours une place importante. Toutefois, avec 30 milliards d'objets à protéger, la création de VLAN en nombre suffisant est difficile, voire impossible.

La segmentation logicielle repose sur plusieurs facteurs, notamment le lieu, le type d'appareil, le rôle de l'utilisateur, pour créer une politique appliquée sur l'ensemble du réseau. En outre, elle s'adapte facilement à mesure que votre environnement évolue. L'intégration de solutions tierces offre également plus de contrôle sur votre réseau, plus de capacités d'automatisation de la sécurité et une meilleure utilisation de vos technologies.

Visibilité et analyse

Les menaces évoluent aussi vite que les nouvelles technologies. Vous devez donc réagir vite dès que vous en détectez. Vous devez repérer tous les nouveaux appareils, protocoles, applications et utilisateurs qui tentent d'accéder à votre réseau, quel que soit leur point d'entrée. Il vous faut également détecter les menaces et les bloquer avant qu'elles affectent vos activités.

Pour couvrir les divers vecteurs de menaces, vous avez besoin de fonctionnalités multicouches automatisées afin d'analyser le trafic sur tout le réseau et le trafic entrant/sortant de l'entreprise, mais également de détecter les anomalies, de bloquer les menaces, d'identifier les hôtes compromis et même d'éviter les erreurs des utilisateurs. La détection basée sur des règles permet de repérer les dernières menaces connues, l'analyse des protocoles empêche les erreurs humaines et la détection des anomalies décèle les nouvelles menaces et identifie le « patient 0 ». Enfin, le trafic commande-contrôle des programmes malveillants est bloqué pour les utilisateurs internes et mobiles, tandis que le trafic web est analysé en permanence pour relever les comportements suspects.

Accès à distance sécurisé

Si de nombreux fournisseurs de matériel, que ce soit dans le secteur industriel ou pour la santé, exigent une assistance à distance dans leurs contrats, cela s'explique aisément. L'assistance à distance contribue en fait à diminuer leurs coûts d'exploitation, car ils n'ont plus à envoyer de techniciens sur place. Elle présente également l'avantage pour les clients de réduire le temps d'indisponibilité des équipements puisque les techniciens interviennent immédiatement. Toutefois, quelques inconvénients subsistent :

- L'accès à distance signifie que les réseaux sensibles, comme les réseaux de contrôle industriel, sont accessibles via Internet.
- Or, les clients possèdent généralement des appareils de plusieurs fournisseurs et l'accès doit être accordé à chaque fournisseur séparément, d'où une multiplication des vulnérabilités.
- Souvent, les clients ne savent pas vraiment quels appareils communiquent avec leur environnement, voire si le réseau du fournisseur ne contamine pas le leur.

Pour éviter que des utilisateurs introduisent un malware, il convient donc de sécuriser leurs communications avec le réseau et de s'appuyer sur la segmentation, la visibilité et l'analyse. Avec cette approche, les utilisateurs distants ont uniquement accès aux systèmes qu'ils sont autorisés à employer dans le cadre de leurs attributions.

Services techniques et de conseil

En dépit des progrès technologiques que représente l'IoT, le facteur humain est le plus important. La technologie est juste un outil. Il faut donc sécuriser les environnements IoT. Une bonne planification et des conseils avisés participent grandement à l'efficacité de votre programme de sécurité IoT.

La première étape la plus importante consiste à définir clairement les objectifs. En vous appuyant sur des services techniques et de conseil pour évaluer les risques, développer un plan de préparation et déployer, appliquer ou créer un plan de gestion des incidents, vous augmentez considérablement les chances de succès de vos projets, tout en bénéficiant d'un service d'assistance continu.

Gestion globale

Les menaces sont dynamiques, et vos défenses doivent également l'être. Imaginez un prestataire qui connecte à votre réseau son ordinateur portable infecté par un ver. Immédiatement, le ver tente de se propager, mais une réponse automatique l'en empêche :

1. Le trafic malveillant est détecté et bloqué.
2. L'ordinateur portable est mis en quarantaine hors du réseau.
3. Le compte de l'utilisateur est désactivé.
4. Votre console indique que vos systèmes stratégiques n'ont jamais été en danger.

Vous contrôlez ainsi tout le processus, sans que le ver affecte votre activité, tout simplement parce que vous étiez prêt et que le plan de gestion des incidents que vous aviez préparé s'est parfaitement exécuté.

Pourquoi choisir Cisco ?

Depuis plus de 25 ans, Cisco participe à la conception, au déploiement et à la sécurisation des réseaux. Nous créons des équipements, inventons des technologies et développons des standards qui façonnent Internet ainsi que tous les types de réseaux imaginables. Qui est plus à même de vous aider à relever le défi de l'IoT ?

Voyons ensemble comment vous aider à profiter pleinement d'un environnement l'IoT sécurisé.

Les opérateurs de réseaux stratégiques ne veulent généralement pas entendre parler de cybersécurité automatisée. Même si elle peut convenir aux réseaux informatiques classiques, c'est loin d'être le cas sur bon nombre de réseaux industriels, et nous en sommes parfaitement conscients. Il vous appartient donc de décider dans quelle mesure vous voulez automatiser la sécurité. C'est votre réseau, c'est vous qui le contrôlez. Et nous vous aidons à le faire facilement et en toute sécurité.

Références

1. www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report.
2. www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
3. www.zdnet.com/article/hospitals-across-england-hit-by-cyber-attack-systems-knocked-offline/.

C11-739247-00 06/17