CCN-CERT

BP/05

Internet des objets

RAPPORT DE BONNES PRATIQUES

JUIN **2021**

ccn-cert centro criptológico nacional
CCN centro criptológico nacional

Édits:

Index

1. À propos de CCN-CERT

Le CCN-CERT est la capacité de réponse aux incidents de sécurité de l'information du Centre National de Cryptologie, CCN, rattaché au Centre National d'Intelligence, CNI. Ce service a été créé en 2006 en tant que CERT gouvernemental national espagnol et ses fonctions sont définies dans la loi 11/2002 réglementant le CNI, dans le RD 421/2004 réglementant le CCN et dans le RD 3/2010, du 8 janvier, réglementant le schéma de sécurité nationale (ENS), modifié par le RD 951/2015 du 23 octobre.

Sa mission est donc de contribuer à l'amélioration de la cybersécurité espagnole, en étant le centre national d'alerte et de réponse qui coopère et aide à répondre rapidement et efficacement aux cyberattaques et à faire face activement aux cybermenaces, y compris la coordination au niveau public de l'État des différentes capacités de réponse aux incidents ou des centres opérationnels de cybersécurité existants.

F de la loi 11/2002) et des informations sensibles, défendre le patrimoine technologique de l'Espagne, former du personnel spécialisé, appliquer des politiques et des procédures de sécurité et utiliser et développer les technologies les plus appropriées à cette fin.

Conformément à ce règlement et à la loi 40/2015 sur le régime juridique du secteur public, le CCN-CERT est responsable de la gestion des cyber-incidents affectant tout organisme ou entreprise publique. Dans le cas des opérateurs critiques du secteur public, la gestion des cyber-incidents sera assurée par le CCN-CERT en coordination avec le CNPIC.

Le CCN-CERT est la capacité de réponse aux incidents de sécurité de l'information du Centre national de cryptologie.

2. Introduction

Le terme “Internet des objets” désigne des réseaux d’objets physiques: artefacts, véhicules, bâtiments, appareils ménagers, vêtements, implants, logiciels... bref, des capteurs dotés d’une connectivité réseau qui leur permet de collecter des informations de toutes sortes.

Une étude de IOT Analytics[1] montre qu’à la fin de 2019, il y avait 9,5 milliards d’appareils IoT connectés dans le monde, hors mobiles et ordinateurs. Au cours des prochaines années, la demande devrait s’envoler pour atteindre 28 milliards en 2024 et 40 milliards en 2027. Il n’est pas difficile d’imaginer comment un tel nombre d’objets représente un immense champ d’exposition social et industriel jamais vu auparavant.

Dans le même rapport, un graphique montrant le nombre de plateformes IoT dans le monde de 2015 à 2019 montre que fin 2019, il y avait 620 plateformes de l’Internet des objets (IoT) dans le monde, soit plus du double du nombre compté en 2015.

Alors que les médias et les experts en sécurité mettent constamment en garde contre les risques de cyberattaques, les risques liés à l’Internet des objets sont rarement mentionnés.

La sécurité de l’IoT n’est pas encore sous les feux de la rampe, même pour les entreprises qui ont beaucoup à perdre en cas de violation de la sécurité. Dans une enquête menée en 2017 par le cabinet de conseil américain Altman Vilandrie & Company, près de la moitié (48 %) des entreprises américaines utilisant un réseau de l’internet des objets (IoT) avaient rencontré au moins un problème de sécurité IoT.

L’Internet est passé par quatre (4) phases distinctes au cours des 30 dernières années (phases académique, commerciale, transactionnelle

1. https://iot-analytics.com/iot-2020-in-review/

et sociale), et a maintenu une mise en œuvre et une amélioration stables pendant de nombreuses années, mais néanmoins, on ne peut pas dire qu'il ait beaucoup changé d'un point de vue architectural. En fait, il s'agit essentiellement de la même entité qui a été conçue à l'époque d'ARPANET .

Dans ce contexte, l'IdO est la première véritable évolution de l'internet, un saut qui pourrait entraîner des changements très importants dans notre façon de vivre, d'apprendre, de travailler, de nous divertir et de nous socialiser. L'aspect le plus transcendant de l'IdO est qu'il donne des capteurs et une sensibilité à l'internet, permettant à une réalité d'exister de manière autonome au-delà d'elle-même, du monde physique, et de nous et des nôtres en son sein.

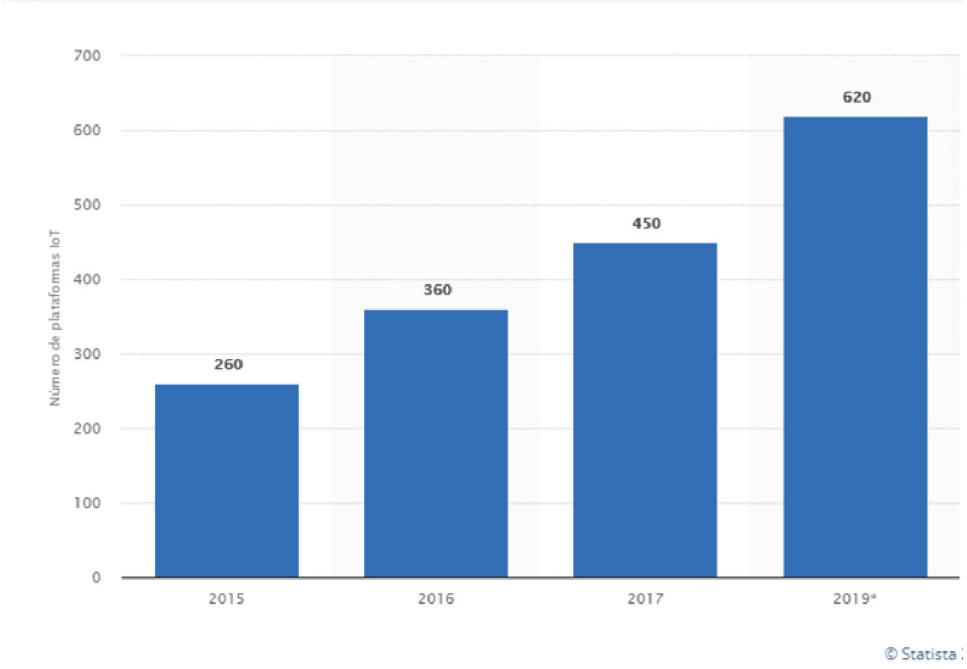


Figure 1 Nombre de plateformes IoT dans le monde 2015-2019

Alors que les médias et les experts en sécurité mettent constamment en garde contre les risques de cyberattaques, les risques liés à l'Internet des objets sont rarement mentionnés.

2. Voir https://sistemas.com/arpanet.php

2. Introduction

L'IdO désigne tous les appareils ou objets du quotidien adaptés qui sont connectés entre eux ou à l'internet. L'IdO est un concept relativement nouveau et, pour cette raison, le domaine de la cybersécurité n'est pas encore prêt à faire face à toutes les menaces qu'il représente, qui ont déjà émergé et émergeront sans aucun doute dans un avenir proche.

L'un des plus grands avantages reconnus de ces appareils est leur connexion à l'internet, mais cette capacité est aussi l'une de leurs plus grandes faiblesses, car cette connectivité peut menacer la sécurité de l'ensemble du système en augmentant considérablement son exposition aux cyberattaques.

Par exemple, s'il n'y avait pas de contrôle d'accès sur l'appareil ou s'il y avait une faille dans l'appareil, un attaquant pourrait accéder à distance à l'appareil et modifier sa configuration, voire toutes ses fonctionnalités. Un tel accès pourrait se produire à tout moment et de n'importe où, de sorte que l'on ne pourrait pas faire confiance à l'intégrité et aux fonctionnalités du dispositif IoT installé à l'origine et utilisé régulièrement au quotidien.

La surface d'attaque croissante est dominée par des points de contrôle non traditionnels, allant d'un élément aussi inoffensif qu'un jouet connecté à l'internet à un élément aussi critique que les capteurs connectés qui contrôlent la production d'énergie dans une centrale nucléaire.

2.1 Tendances de l’internet des objets

Une connectivité sans précédent est à la fois le meilleur de l’Internet des objets et le pire, car elle crée à la fois de grandes opportunités et des risques considérables. Dans un environnement qui va des capteurs aux applications et services en nuage, un écosystème IoT de bout en bout est essentiel pour saisir les opportunités sans compromettre la sécurité, la gérabilité et l’interopérabilité.

Les **applications potentielles** de l’internet des objets couvrent un large éventail de secteurs représentant plusieurs milliards de dollars, allant de la sécurité et de la santé au style de vie et aux jeux.

Par exemple, Microsoft développe des plans de travail de cuisine capables de reconnaître les aliments et d’afficher les recettes qui les incluent. Il existe des matelas intelligents qui surveillent les habitudes de sommeil de l’utilisateur en mesurant sa respiration et son rythme cardiaque. Il existe désormais un certain nombre de serrures intelligentes qui s’ouvrent lorsque vous vous approchez de la porte et qui peuvent être programmées à distance pour laisser entrer vos amis ou vos invités.

Les applications potentielles de l’internet des objets couvrent un large éventail de secteurs représentant plusieurs milliards de dollars, allant de la sécurité et de la santé au style de vie et aux jeux.

Le potentiel de la "vie assistée", qui est particulièrement important pour les personnes âgées ou dépendantes, suscite un enthousiasme réservé. Plusieurs projets en cours prévoient de vastes déploiements de l'IdO pour une meilleure gestion des villes et des systèmes.

On peut citer Songdo , en Corée du Sud, qui est le premier exemple de **ville intelligente** entièrement équipée. Pratiquement tout dans

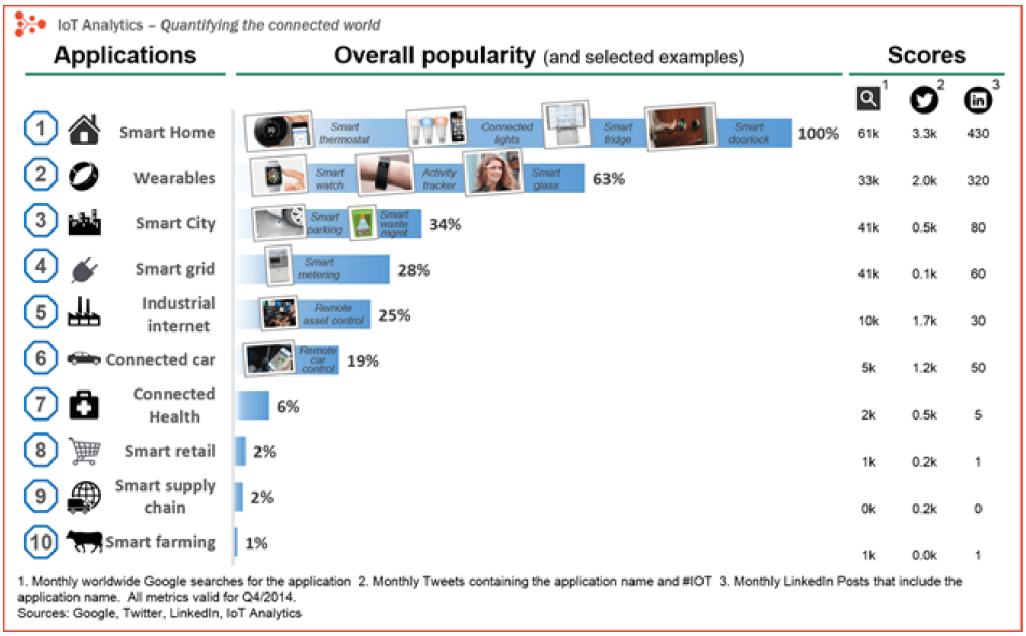


Figure 2.- Popularité des dispositifs IoT.

la ville est câblé, connecté et transformé en une source continue de données qui peuvent être surveillées et analysées par une multitude d'ordinateurs avec peu ou pas d'intervention humaine.

Un autre aspect à prendre en compte est celui des **cycles** rapides **de mise à jour et d'obsolescence** qui sont courants dans le monde des technologies de l'information. Si ces technologies doivent être intégrées au bâtiment et à l'architecture, nous pourrions nous retrouver avec des bâtiments, des maisons et des usines truffés d'éléments complètement obsolètes, sans support et sans maintenance possible.

Avec l'IoT, nos maisons deviennent de plus en plus *piratables* à mesure que le nombre d'appareils connectés augmente. Les cauchemars des experts en cybersécurité sont des armées de *botnets* utilisant des grille-pain intelligents pour développer des attaques par déni de service distribué (DDoS) ou pour cacher du code et des exécutables à l'abri des regards des chercheurs.

3. Voir https://www.bbc.com/mundo/noticias-57030345

2. Tendances de l'internet des objets

Avec l'internet des objets, la maison et les autres environnements intelligents deviennent une extension de notre travail. Tout comme un dispositif *portable* compte nos pas, notre rythme cardiaque ou notre respiration, nos maisons surveilleront et mesureront tout le reste.

Les préoccupations les plus évidentes ont trait à **la vie privée**. La collecte massive de nos données et métadonnées revient peut-être à installer des caméras de surveillance, mais il s'agit d'une forme de surveillance numérique encore plus dangereuse pour notre vie privée et notre liberté que la simple observation visuelle.

À l'avenir, l'internet des objets pourrait être un immense réseau ouvert dans lequel des entités et des objets virtuels (avatars) interagiront entre eux de manière indépendante en fonction du contexte, des circonstances et de l'environnement.

Les entreprises devront adapter leurs pratiques de gestion des risques et élargir la portée des évaluations des risques pour inclure tous les appareils connectés. Dans ce contexte, l'un des principaux défis pour les organisations sera de savoir comment stocker, suivre, analyser et donner du sens à la grande quantité de données générées par l'inclusion de l'IdO dans le processus d'évaluation des risques.

2.2 Relations avec le nuage

Aujourd'hui, nombre de ces appareils domestiques utilisent des services de sauvegarde basés sur le cloud pour surveiller leur utilisation et permettre aux utilisateurs de contrôler ces systèmes à distance. Ceux-ci permettent aux utilisateurs d'accéder aux données et de contrôler l'appareil par le biais d'une application mobile ou d'un portail web.

Compte tenu de l'importance que les fournisseurs de services en nuage auront dans les différentes phases du développement de l'IdO, il est absolument nécessaire de vérifier la sécurité de leur interface :

Déterminez si les valeurs par défaut de l'utilisateur et du mot de passe peuvent être modifiées au cours du processus d'installation initiale du produit.

Déterminer si un compte est verrouillé après plusieurs échecs de connexion

Déterminez si les comptes valides peuvent être identifiés à l'aide de mécanismes de récupération de mots de passe.

Examiner la résilience de l'interface web contre les attaques de type cross-site scripting (XSS), cross-site request forgery (CSRF), injection SQL (SQLi) et autres attaques similaires

Examinez les interfaces avec le cloud pour détecter toute vulnérabilité potentielle (interfaces API et interfaces web des systèmes cloud).

2.2 Relations avec le nuage

La sécurisation de l'interface avec le cloud nécessite:

- Changez le mot de passe et même le nom d'utilisateur pendant l'installation du produit IoT.
- Veillez à ce que les comptes des utilisateurs ne puissent pas être découverts grâce à des fonctionnalités telles que la récupération des mots de passe.
- Assurez-vous que l'accès à un compte est temporairement bloqué après plusieurs échecs d'accès.
- Veillez à ce que les informations d'identification (noms d'utilisateur, mots de passe, jetons d'accès, cookies, etc.) ne soient pas exposées à l'Internet lorsqu'elles y transitent. Utilisez toujours des connexions cryptées avec authentification TLS.
- Mettez en place, si possible, une authentification utilisant une vérification à deux ou plusieurs facteurs.
- Détecter et bloquer les demandes anormales ou les tentatives d'accès au système/appareil.

4. Par exemple, voir https://bitacoralinux.es/fail2ban-o-como-prevenir-ataques-de-fuerza-bruta/

2.3 Les infrastructures critiques et l'internet des objets

Ces dernières années, l'électronique industrielle et son informatique étaient très spécifiques et uniquement présentes dans leurs domaines fermés. Les systèmes SCADA sont un type de système de contrôle industriel (ICS), tout comme les systèmes de contrôle distribués (DCS) .

Dans les systèmes industriels, les données sont reçues de stations distantes et celles-ci génèrent des réactions qui, automatiquement ou avec l'aide d'opérateurs, sont traduites en actions exécutives qui sont envoyées aux dispositifs sur le terrain, contrôlant ainsi l'ensemble du système. Ces dispositifs sont ceux qui contrôlent réellement les opérations locales (ouverture ou fermeture des vannes, réglage ou retrait des freins, collecte des données des capteurs, surveillance de l'environnement, réglage du niveau d'alarme, etc.)

Les technologies SCADA sont celles qui contrôlent les processus industriels et toutes ces installations ont la caractéristique essentielle de ne pas pouvoir être arrêtées sans causer de grands dommages aux populations et aux systèmes qu'elles desservent, ni sans entraîner des pertes économiques importantes et difficiles à supporter.

Les protocoles de communication SCADA sont propres à chaque fabricant, mais nombre d'entre eux sont largement utilisés sur les réseaux TCP/IP grâce à des extensions ultérieures des protocoles d'origine. Cela brouille dangereusement la frontière entre les réseaux industriels et les réseaux à usage général tels que l'Internet. Dans tous les cas, cette migration vers les réseaux TCP/IP constitue un risque en soi, car elle ne tient pas compte des différences importantes entre un réseau industriel et un réseau à usage général.

5. SCADA (Supervisory Control And Data Acquisition). Ver https://www.wonderware.es/hi-scada/que-es-scada/
6. Voir https://www.industriasgsl.com/blog/post/que-es-un-sistema-de-control-industrial
7. Voir https://www.cursosaula21.com/que-es-un-sistema-de-control-distribuido/

2.3 Les infrastructures critiques et l'internet des objets

Tous ces scénarios et bien d'autres encore, qui constituent le catalogue des **infrastructures critiques**, dépendent, dans une plus ou moins large mesure, des réseaux de contrôle et de surveillance qui sont en train de migrer pour fonctionner sur des réseaux TCP/IP et utilisent donc la même électronique de réseau qu'Internet, le tout sans évaluation préalable quant à leur sécurité effective.

La prise en compte de la sécurité des systèmes SCADA a radicalement changé depuis l'attaque Stuxnet contre les systèmes de contrôle industriel d'une usine iranienne d'enrichissement de l'uranium à Natanz . En conséquence, la société industrialisée a pris conscience de ce que la menace d'un code malveillant peut signifier pour les opérations de sabotage .

8. Voir https://www.businessinsider.es/10-anos-stuxnet-primer-ciberataque-mundo-fisico-657755
9. Voir https://www.bbc.com/news/world-middle-east-56722181
10. Kim Zetter: "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon" Crown Publisher, ISBN-13: 978-0770436179

3. Visibilité en ligne

Grâce à la croissance rapide d'Internet, de plus en plus d'outils sont mis à la disposition de tous, et l'un d'entre eux est le célèbre moteur de recherche.

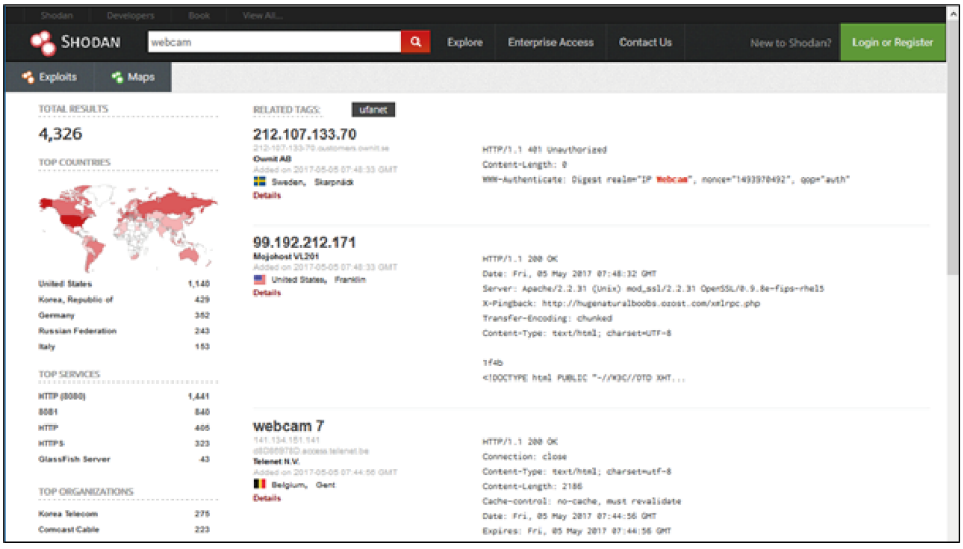


Figure 3.-Recherche de dispositifs IoT dans Shodan

3. Visibilité en ligne

Les services proposés sur le web se sont développés, tout comme les moteurs de recherche, avec l'émergence de moteurs de recherche tels que **Shodan** , qui permet de trouver très facilement des appareils IoT connectés directement à internet.

Ce moteur de recherche fournit à l'utilisateur une foule de détails sur l'appareil lui-même et lui permet d'effectuer une recherche par type d'appareil, par exemple "webcams". Comme le montre la figure 3, cette simple recherche permet de trouver jusqu'à 4 326 webcams directement connectées à Internet à ce moment-là.

Vous pouvez également filtrer les recherches par d'autres termes tels que le port qu'ils ont exposé au réseau. Par exemple, vous pouvez trouver tous les appareils qui autorisent les connexions au port 22, qui est le port des terminaux SSH, et le résultat de la recherche renvoie jusqu'à 8 860 281 éléments directement accessibles à distance avec ce type de communication sur Internet.

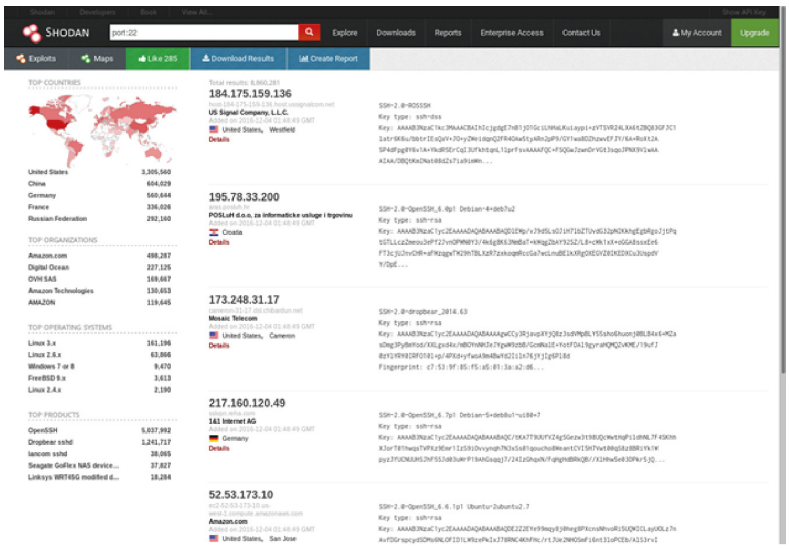
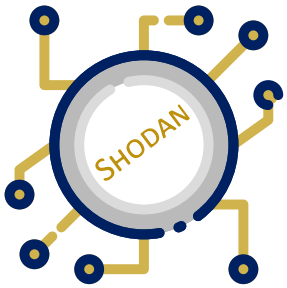


Figure 4.- Recherche de dispositifs IoT dans Shodan par port.

11. https://shodan.io

3. Visibilité en ligne

Outre Shodan, il existe de nombreuses autres méthodes de recherche automatique qui sont directement connectées à Internet. Parmi les plus connues, citons Scans.io et ZMap .



Il ne faut pas oublier que les appareils IoT peuvent également être connectés entre eux ou à d'autres appareils via des connexions radio , notamment des connexions Wi-Fi, BlueTooth (BT) ou même NFC. Dans ces cas, le contrôle des appareils est également susceptible d'être confié à des utilisateurs malveillants.

Dans le rapport "Combatting the Ransomware Blitzkreig", un chapitre est consacré aux appareils IoT liés au domaine médical qui sont connectés à d'autres appareils via des liaisons Bluetooth, comme les stimulateurs cardiaques implantés chez les patients, ce qui met en évidence les risques de sécurité encourus.

Dans tous les cas, il est conseillé aux utilisateurs de rechercher leurs appareils dans les moteurs de recherche susmentionnés, car ils constituent l'une des principales sources d'information pour les attaquants qui cherchent à localiser les appareils vulnérables.

12. https://scans.io/
13. https://zmap.io/
14. https://www.postscapes.com/internet-of-things-protocols/

4. Lorsque les appareils sont la cible

Une fois qu'un attaquant a trouvé un moyen d'automatiser la recherche de cibles potentielles auxquelles il peut accéder et qu'il peut gérer à distance, il ne lui reste plus qu'à le faire et à en prendre le contrôle total afin de les utiliser pour mener les activités illicites qui l'intéressent.

Ce réseau de machines et de dispositifs sous le contrôle d'une seule personne est appelé "botnet", et les nœuds qui le composent sont appelés "bots" ou "zombies".

Lorsqu'un attaquant a accès à un appareil, il y installe généralement un logiciel malveillant qui lui permet de le contrôler de manière synchrone avec d'autres appareils, pouvant même lancer des commandes simultanément, de sorte que tous les ordinateurs infectés agissent de la même manière, ou de manière coordonnée, contre la même cible.

L'attaque de ce type la plus populaire ces dernières années est **l'attaque par déni de service distribué (DDoS),** qui, en établissant des connexions massives et simultanées à partir de différentes sources, cherche à désactiver un service ou un site web de sorte que personne ne puisse accéder au site attaqué.

Il est intéressant de noter que les dispositifs IoT compromis sont de plus en plus utilisés pour de telles attaques, principalement les enregistreurs vidéo numériques (DVR) et les caméras IP.

4. Lorsque les appareils sont la cible

Les raisons de lancer des campagnes DDoS sont multiples. Certaines sont clairement motivées par des raisons politiques, de protestation ou de militantisme, etc. Dans d'autres cas, il s'agit simplement de démontrer le pouvoir que peut avoir un groupe de cybercriminels lorsqu'il s'agit de désactiver un site web. Parfois, il s'agit d'une extorsion dans laquelle on demande de l'argent à l'entreprise pour ne pas désactiver ses serveurs sur Internet et affecter gravement ses activités commerciales.

Les botnets sont également utilisés pour mener des campagnes de spam, qui consistent à envoyer des courriers électroniques de masse non sollicités, ou pour modifier les résultats de sondages et d'enquêtes en ligne. Ces botnets sont généralement loués à des tiers en tant que plate-forme pour mener les activités de leur choix, qui sont généralement totalement illégales.

Actuellement, l'un des botnets les plus célèbres et les plus utilisés est le botnet Mirai . Ce botnet est largement utilisé depuis que, à la mi-octobre 2016, son code source a été publié sous la forme d'un code gratuit que tout le monde peut utiliser. En outre, il convient de souligner que ce code malveillant présente des caractéristiques qui permettent d'infecter des appareils et de se développer en tant que botnet vraiment facilement.

Tout d'abord, Mirai scanne l'Internet, principalement à la recherche de caméras et de routeurs. Il tente ensuite d'accéder au panneau d'administration de l'appareil en utilisant une liste d'utilisateurs et de mots de passe par défaut. Lorsqu'il obtient l'accès à l'appareil, il s'héberge sur celui-ci et vérifie qu'il n'est pas déjà infecté par un autre code malveillant et, si c'est le cas, il se charge de l'éjecter. Il tente ensuite de faire croître l'infection, et donc le botnet, à partir de cet appareil en recherchant de nouvelles machines vulnérables.

Une fois que le processus d'infection d'une machine est terminé, vous obtenez une machine zombie qui est continuellement prête à être utilisée dans une attaque distribuée aux ordres des serveurs de commande et de contrôle.

Une nouvelle version de Mirai a récemment été découverte, équipée d'avantage d'exploits, ce qui la rend plus dangereuse et plus facile à propager. De plus, cette nouvelle version ne cible pas seulement ses victimes habituelles (caméras IP, routeurs, etc.), mais aussi les appareils IoT des entreprises.

15. https://www.akamai.com/es/es/multimedia/documents/white-paper/akamai-mirai-botnet-and-attacks-against-dns-servers-white-paper.pdf
16. https://www.kaspersky.es/blog/mirai-enterprise/18065/

Les botnets peuvent facilement être créés en quelques heures sur la base du nombre croissant de dispositifs IoT non sécurisés qui sont connectés à Internet.

La planification de l'atténuation des attaques DDoS doit prendre en compte des taux d'attaque pouvant atteindre 1,5 Tbps (térabit par seconde).

4.1 Recommandations

La première mesure à prendre avec tous les appareils, en particulier les appareils IoT, devrait être de **changer le mot de passe, en en choisissant un qui soit vraiment sécurisé** pour tous vos profils, en particulier ceux qui gèrent cet appareil. Si, pour une raison quelconque, cela n'est pas possible, **cet appareil ne devrait jamais être connecté à un autre appareil et, dans la mesure du possible, ne devrait pas être utilisé.**

Une autre possibilité serait de modifier les ports de connexion TCP par défaut afin de ne pas donner aux navigateurs des informations sur le service offert par le dispositif à travers eux.

Si possible, il est également conseillé d'utiliser un élément qui joue le rôle d'intermédiaire séparant le réseau de dispositifs IoT du reste d'Internet. Cet élément pourrait être le routeur lui-même utilisé pour accéder à Internet, auquel cas il devrait être **correctement configuré et des mesures de sécurité** et de **contrôle d'accès activées** pour sécuriser les réseaux de dispositifs IoT auxquels il fournit une connectivité.

Utilisez un élément qui sert d'intermédiaire séparant le réseau de dispositifs IoT du reste de l'Internet.

La première étape sur tous les appareils est de changer le mot de passe et d'en choisir un qui soit vraiment sûr.

5. Quand vous êtes la cible

Bien que le concept de ransomware soit actuellement plus orienté vers le kidnapping d'informations et le paiement de la rançon correspondante, il ne fait aucun doute qu'avec l'expansion de l'IoT, de nouvelles formes d'extorsion des utilisateurs vont apparaître.

Si l'efficacité des ransomwares sur les ordinateurs personnels repose sur la mise à profit de la valeur sentimentale des fichiers privés capturés et de la valeur de ces informations (environnement professionnel) pour le fonctionnement de l'entreprise, dans le cas des dispositifs IoT, l'objectif ne sera pas, en principe, les informations qui peuvent y être stockées, mais le déni de service permanent en attendant une rançon.

Pour certains appareils, la réinstallation du micrologiciel d'origine et la réinitialisation du système aux paramètres d'usine par défaut peuvent suffire à répondre à l'attaque et à rétablir le fonctionnement d'origine, mais selon l'appareil, cela pourrait être une tâche compliquée et dans certains cas, étant donné la nature du service fourni, l'interruption du bon fonctionnement pourrait être cruciale et même mettre la vie en danger.

Prenons l'exemple d'un **stimulateur cardiaque**. Ce dispositif pourrait être utilisé pour forcer la victime à payer une rançon sous la menace d'une désactivation, ou pour l'obliger à effectuer des opérations de déchargement de la batterie à un rythme accéléré jusqu'à la réception du paiement.

Dans les cas de déni de service de dispositifs ou d'installations IoT, le coût du rétablissement du service pourrait largement dépasser la valeur de la rançon demandée, et celle-ci finirait par être payée.

Dependiendo del dispositivo, la interrupción del funcionamiento correcto podría ser crucial y llegar a costar vidas.

Il faut également garder à l'esprit que, dans certains cas, ce processus de retour aux paramètres d'usine par défaut peut être impossible à réaliser dans le court laps de temps fixé par l'attaquant. Dans ces cas, le paiement de la rançon peut devenir la seule option viable qui ne mette pas la vie de la personne touchée en danger.

Un autre exemple d'attaque pourrait être l'infection du système de contrôle général d'un **système domotique.** En prenant le contrôle du contrôleur central de la maison, l'attaquant pourrait déterminer à tout moment le fonctionnement et le comportement de tous les appareils connectés de la maison, et permettre diverses actions contre ses habitants.

Par exemple, les actions que l'attaquant pourrait entreprendre pourraient aller de la manipulation de l'alarme d'un réveil pour qu'il se déclenche quand il ne devrait pas et reste silencieux quand il le devrait, à la commande du régulateur de température d'un appareil pour qu'il atteigne des niveaux extrêmes qui pourraient mettre en danger son intégrité. L'attaquant pourrait aussi, par exemple, accéder aux caméras de surveillance pour obtenir des images compromises des habitants de la maison et les utiliser ensuite pour faire chanter ses victimes.

Il peut également s'agir d'une opération plus secrète, où l'agresseur souhaite simplement connaître les habitudes et l'emploi du temps de la victime afin de planifier le meilleur moment pour un vol ou un enlèvement.

Dans le cas des dispositifs IoT, l'objectif ne sera pas, en principe, les informations qui peuvent y être stockées, mais le déni de service permanent en attendant d'obtenir une rançon.

5.1 Recommandations

Cette situation pose une nouvelle série de menaces que l'utilisateur n'aura aucun moyen de combattre. Par conséquent, la principale recommandation est de **se passer de l'accès à Internet sur les appareils IoT**, évitant ainsi la possibilité d'attaques à distance et le vol d'informations privées qui pourraient causer de graves problèmes à l'avenir.

Dans le cas où cet accès depuis Internet est absolument nécessaire, il est essentiel de faire preuve d'une extrême prudence et de prendre des mesures de sécurité lorsqu'il s'agit d'établir **qui peut se connecter (contrôle d'accès), depuis quel appareil** (mobile, tablette, etc.) et à **quel moment** de la journée, de la semaine ou de l'année.

L'inertie en tant qu'utilisateurs des technologies de l'information nous fait penser que l'augmentation du nombre de fonctionnalités des systèmes et des dispositifs est toujours bonne et bienvenue, mais dans le cas de l'IoT, il est nécessaire de réfléchir si ces fonctionnalités sont nécessaires et vont réellement être utilisées et, surtout, si elles compensent les risques qu'elles comportent.

Toute fonctionnalité qui n'est pas désactivée est une occasion de plus pour l'attaquant de prendre le contrôle de l'ensemble du système.

La principale recommandation est de se passer de l'accès à Internet sur les appareils IoT, si cela se produit, il est impératif de faire preuve d'une extrême prudence et de prendre des mesures de sécurité : qui peut se connecter, depuis quel appareil et à quel moment.

6. Surfaces d'attaque

Compte tenu du large éventail de solutions IoT que l'industrie propose et qui devrait s'accroître dans les années à venir, il est intéressant d'identifier très tôt les espaces ou les fenêtres par lesquels les attaques peuvent se produire.

Voici quelques-unes des vulnérabilités sur chacun des fronts par lesquels un attaquant peut avoir accès à une infrastructure IoT ou aux données qu'elle collecte.

Surface d'attaque	Vulnérabilité
Contrôle d'accès à l'écosystème	Confiance implicite entre tous les composants du système. (In)Sécurité dans l'enregistrement des composants (*inscription*). Le retrait ou la mise hors service d'équipements (*déclassement*). Perte des identifiants d'accès et des procédures.
Mémoire du dispositif	Effacez les noms d'utilisateur et les mots de passe. Les informations d'identification des tiers sont claires. Clés de cryptage en clair.

6. Surfaces d'attaque

Surface d'attaque	Vulnérabilité
Interfaces physiques de l'appareil	Extraction du micrologiciel. Interface de ligne de commande pour les utilisateurs et l'administrateur. Possibilités d'escalade de privilèges. *Réinitialisation* à un état non sécurisé. Retrait des supports de stockage. (Non)Résistance à la manipulation physique de l'appareil. Présence de ports de débogage (par exemple, JTAG). Exposition du numéro de série ou de l'identité de l'appareil.
Interface Web du dispositif	Injection SQL, scriptage intersite et falsification de requête intersite. Extraction et liste des noms d'utilisateurs valides. La présence de mots de passe faibles. Possibilité de bloquer des comptes. Existence d'informations d'identification par défaut.
Le micrologiciel du dispositif	*Des informations d'identification codées en dur.* Divulgation d'URL et d'informations sensibles. Présence de clés de cryptage en clair. Altération du chiffrement lui-même (symétrique et asymétrique). Affiche la version du micrologiciel et/ou la date de la dernière mise à jour. Comptes d'utilisateurs oubliés agissant comme des portes dérobées. Services actifs vulnérables (web, ssh, tftp, etc.). Exposition des API de sécurité de l'appareil. Possibilité de revenir à une version antérieure non sécurisée.
Services de réseau de dispositifs	Diffusion de l'information. Interface en ligne pour les utilisateurs et pour l'administrateur. Possibilités d'injection de code. Déni de service. L'existence de services non cryptés. L'utilisation d'un cryptage mal mis en œuvre. Présence de services de test et/ou de développement non supprimés ou non désactivés dans les scénarios de production. Problèmes de dépassement de tampon dans les logiciels. UPnP et services UDP vulnérables. Les chances de succès des attaques DoS (*Denial of Service*). La mise à jour *en direct* (OTA) du micrologiciel de l'appareil. Les chances de réussite des attaques de Replay. Absence de vérification des téléchargements de données ou de codes. Absence de vérification de l'intégrité des messages, qu'il s'agisse de données ou de commandes.

17. Voir https://study.com/academy/lesson/joint-test-action-group-jtag-definition-uses-process.html
18. Voir https://www.redeszone.net/tutoriales/internet/upnp-problema-seguridad-red/

6. Surfaces d'attaque

Surface d'attaque	Vulnérabilité
Interface administrative	Injection SQL, scriptage intersite et falsification de requête intersite. Mécanismes de découverte des noms d'utilisateur valides. La présence de mots de passe faibles et d'informations d'identification par défaut connues. La possibilité de bloquer les comptes. L'absence d'options de sécurité/chiffrement et de *journalisation* sécurisée. Pas d'authentification à deux facteurs. Impossibilité *d'effacer* l'appareil en toute sécurité.
Stockage local des données	La presencia de datos no cifrados y/o el cifrado con claves comprometidas. La falta de controles de integridad de los datos. El uso de una misma clave de cifrado/descifrado de todos los datos.
Interface Web vers le nuage	Injection SQL, scriptage intersite et falsification de requête intersite. La découverte de noms d'utilisateurs valides. La présence de mots de passe faibles et d'informations d'identification par défaut. Le blocage éventuel de comptes. Le non-cryptage de ce qui est transporté ou communiqué. La présence d'un mécanisme non sécurisé de récupération des clés et des mots de passe. Absence d'authentification à deux facteurs.
API dorsale tierce partie	Transmission non cryptée d'informations personnelles ou d'identification. Comment les informations personnelles et d'identification sont cryptées. Divulgation d'informations internes au dispositif. Divulgation de l'emplacement de l'appareil..
Mécanisme de mise à jour	Que les mises à jour sont envoyées sans être cryptées. Les mises à jour ne sont pas correctement signées. L'URL des mises à jour peut être modifié. Vérification inexistante ou inefficace des mises à jour, ou absence d'authentification des mises à jour. La possibilité d'installer des mises à jour malveillantes. La perte temporaire ou permanente du mécanisme de mise à jour. L'absence d'un mécanisme de mise à jour manuelle.
Application mobile	L'existence d'informations d'identification par défaut et/ou l'acceptation ou l'utilisation de mots de passe faibles. Stockage non sécurisé des données. Absence ou insuffisance de cryptage de ce qui est transporté. Un mécanisme peu sûr de récupération des mots de passe et des clés. L'absence d'authentification à deux facteurs.
Backend de l'API du vendeur	Accepter comme confiance inhérente aux applications en nuage ou mobiles. Mécanismes d'authentification faibles. Contrôles d'accès faibles ou inexistants. La probabilité de réussite des attaques par injection. La présence de services cachés et de fonctionnalités non documentées.

6. Surfaces d'attaque

Surface d'attaque	Vulnérabilité
Communication sur les écosystèmes	L'absence ou l'abus de contrôles de l'état de santé à l'échelle du système. Tests du bon fonctionnement (Heartbeats) du système. L'(in)sécurité des commandes qui font fonctionner l'écosystème. Déprovisionnement des ressources ou des capacités. Le forçage des mises à jour.
Trafic réseau	La propia Red de Área Local (LAN). Le réseau local (LAN) lui-même. Le saut du réseau local vers l'Internet (routeur, proxy, pare-feu, etc.). Liaisons aériennes court-courrier. Non-standardisation des protocoles et/ou des procédures. Les réseaux sans fil eux-mêmes (Wi-Fi, Z-wave, Zigbee, Bluetooth). La possibilité d'analyser les dispositifs avec les techniques de fuzzing du protocole.
Authentification et autorisation	Divulgation des valeurs liées à l'authentification/autorisation des clés de session, jetons, cookies, etc. Réutilisation des clés de session, des jetons, etc. L'absence d'authentification de dispositif à dispositif. Authentification nulle ou faible de l'appareil à l'application et entre l'appareil et le nuage, et vice versa. Non-authentification de l'application avec le nuage, et vice versa. Manque d'authentification des applications web avec le système en nuage. Absence de techniques d'authentification dynamique.
Vie privée	Divulgation des données de l'utilisateur. La publication de la localisation de l'utilisateur par le biais du suivi de son appareil. La possibilité de systèmes à confidentialité différentielle, où quelques personnes surveillent tout le monde et personne ne les surveille.

La sécurité de l'infrastructure IoT contre les attaques ci-dessus sera renforcée par toute mesure servant à atténuer les effets de chacune des surfaces d'exposition. Avant d'adopter une technologie ou de mettre en œuvre une architecture basée sur l'IdO, il est conseillé de se poser les questions énumérées dans le tableau ci-dessus.

19. Voir https://www.owasp.org/index.php/Fuzzing

7. Des mesures pour protéger et/ou réduire la surface d'attaque

Dans le cas des architectures IoT, il sera rarement possible d'utiliser les mêmes mesures de sécurité qu'il est recommandé d'avoir dans les systèmes TIC, et avec lesquelles l'utilisateur est le plus familier (antivirus, pare-feu, scanners de malwares, etc.). Cependant, d'autres sont possibles et doivent être prises en compte si vous avez l'intention de travailler, de voyager, de vivre, etc. avec une infrastructure IoT sécurisée.

7.1 Configuration sécurisée

En général, les caractéristiques de chaque dispositif IoT varient fortement de l'un à l'autre, et dans certains cas il est possible d'installer des applications de sécurité (mini pare-feu, anti-malware, etc.) ou au moins de modifier le comportement du dispositif (configuration) pour le rendre plus sûr. Cependant, dans de nombreux autres cas, les **limitations physiques et logiques de l'appareil lui-même rendront ce processus de protection impossible**, et dans de nombreux cas, cette impossibilité est imposée par le fabricant, auquel cas la seule recommandation possible est d'**abandonner l'utilisation de ce type de technologie.**

7.2 Mise à jour

La principale mesure de sécurité à suivre avec tout appareil informatique, qu'il soit IoT ou non, est de **maintenir tous ses logiciels et micrologiciels mis à jour en permanence**, car c'est la seule façon d'avoir les derniers correctifs pour les vulnérabilités qui ont été détectées. Diminuer les vulnérabilités permet toujours de diminuer le risque et l'efficacité des éventuels outils développés par les attaquants.

La mise à jour régulière des systèmes, en plus de favoriser leur bon fonctionnement, rend disponibles les nouvelles fonctionnalités proposées par les fabricants.

En général, le processus de mise à jour dépend du dispositif en question. Certains appareils permettent des mises à jour automatiques par le biais de connexions et de vérifications périodiques sur les serveurs que le fabricant a activé à cet effet, tandis que dans d'autres cas, les mises à jour ne peuvent être effectuées que manuellement et nécessitent donc que l'utilisateur suive les instructions fournies par le fabricant.

7.3 Des mises à jour authentiques

Dans tous les cas, la qualité de l'appareil IoT est également liée aux mesures de sécurité mises en œuvre par le fabricant afin que l'appareil ne puisse installer que des mises à jour authentiques et autorisées.

L'une des procédures d'attaque les plus efficaces sur les dispositifs IoT consiste à les mettre à jour avec une fausse mise à jour, convenablement modifiée par l'attaquant. L'**intégrité et l'authenticité des mises à jour sont des éléments importants à prendre en compte lors de l'achat d'appareils électroniques**, quels qu'ils soient.

Dans tous les cas, les **mises à jour doivent être signées, et ces signatures doivent être correctement vérifiées avant l'**installation. Il convient de noter que le **retour à des versions antérieures, moins sûres, ne devrait pas être autorisé, de sorte que** la mise à jour devrait toujours être postérieure à la version mise à jour.

7.4 Pare-feu et détection des codes malveillants

Comme il n'est pas possible d'installer un logiciel anti-malware ou un pare-feu sur le dispositif IoT lui-même, la prévention des intrusions doit se faire à d'autres couches intermédiaires pour gérer la sécurité de l'ensemble de l'architecture.

La mesure la plus recommandée consiste à c**onfigurer correctement le routeur fournissant l'accès interne**t de l'appareil afin qu'il filtre les connexions vers et depuis les appareils IoT auxquels il fournit une connectivité.

L'objectif est de restreindre l'accès à l'appareil à partir de réseaux externes, de sorte que, par exemple, les paramètres de l'appareil ne soient accessibles qu'à partir d'un ordinateur connecté au même réseau local, ou que les connexions vers et depuis Internet se fassent vers des adresses IP de confiance spécifiques et vérifiées.

Dans ce scénario, le **routeur doit être correctement configuré et des listes d'accès autorisés (listes blanches) doivent** être établies pour des utilisateurs, des domaines et/ou des adresses IP spécifiques.

7.5 Authenticité et intégrité des commandes

Si la connectivité externe des dispositifs et infrastructures IoT doit être maintenue, il convient que le système dispose d'un mécanisme de signature numérique permettant la vérification cryptographique de l'authenticité des commandes et des communications établies.

Le système IoT doit toujours établir si une connexion à distance (Internet) à l'appareil IoT est authentique ou non, et si ce n'est pas le cas, ignorer simplement la demande.

7.6 Connectivité Internet

Il est vivement conseillé de désactiver toute connectivité à distance de l'appareil IoT s'il n'est pas destiné à être utilisé immédiatement. Tant les appareils Bluetooth, qui peuvent être localisés par d'autres appareils à proximité, que les appareils connectés à Internet, qui peuvent apparaître dans des moteurs de recherche spécifiques, sont faciles à découvrir, et la meilleure façon de prévenir une attaque est d'en limiter l'accès.

Dans certains cas, il peut sembler nécessaire qu'un dispositif IoT soit accessible de l'extérieur, depuis n'importe quel coin d'Internet, mais il est toujours utile de répondre à la question de savoir s'il est vraiment nécessaire d'accéder à "mon réfrigérateur" depuis n'importe quel endroit du monde. La réponse n'est presque jamais un oui retentissant.

Une solution d'atténuation des risques consiste à établir quelles sont les conditions exactes dans lesquelles cette connexion doit être autorisée : d'où, à quelle heure, par qui, dans quel but, que va-t-on lui permettre de faire exactement, etc.

7.6 Connectivité Internet

Par exemple, si le besoin est de pouvoir allumer le chauffage dans une résidence secondaire pour que la température soit confortable à l'arrivée, la connexion avec la chaudière est parfaitement définie (commande d'allumage ou d'extinction de la chaudière), elle se fera à partir de dispositifs très spécifiques (adresse IP de la résidence principale, téléphones du propriétaire ou des personnes autorisées), probablement les week-ends et les périodes de vacances (calendrier), à certaines heures plus probables que d'autres (horaire) et dans le cas où la température extérieure est inférieure à une valeur donnée, etc. Grâce à ces informations, il est possible de limiter la plage horaire et l'origine de cette opération à distance dans l'infrastructure IoT.

7.7 Paramètres de sécurité

En raison des exigences liées à la desserte d'un marché plus large, dans la plupart des cas, les systèmes IoT incluent des fonctionnalités qui sont nécessaires à un moment donné pour la mise en service ou pour la maintenance ultérieure. Dans ce cas, toutes les fonctionnalités inutiles doivent être désactivées dans le scénario opérationnel.

Pour ce faire, il existe des **mécanismes de configuration** qui permettent de déterminer la fonctionnalité à développer par l'appareil dans chaque scénario. Il est très important de vérifier que les degrés de liberté disponibles dans le processus de configuration sont suffisants. Cette vérification comprend :

7.7 Paramètres de sécurité

- Consultez l'interface d'administration de l'appareil pour connaître les options permettant de renforcer la sécurité du système, par exemple en **imposant des mots de passe forts.**
- Trouvez un moyen, dans l'interface administrative, de **séparer les profils d'administrateur des profils d'utilisateur normaux.**
- Passez en revue l'interface administrative pour les **options de cryptage.**
- Vérifiez dans la console de gestion les options permettant d'**activer la journalisation sécurisée de divers événements de sécurité.**
- Vérifiez s'il existe un moyen de **déclencher des alertes et des notifications** à l'utilisateur final de tous les événements liés à la sécurité dans le système.

7.7 Paramètres de sécurité

Pour que la configuration d'un appareil soit suffisamment sécurisée, il faut :

- Assurez-vous que les utilisateurs normaux peuvent être isolés des administrateurs.
- Garantir la capacité de chiffrer les données au repos et en transit.
- Veillez à ce que l'utilisation de politiques de mots de passe forts puisse être appliquée.
- Assurez-vous de pouvoir activer l'enregistrement des événements de sécurité.
- Garantir la capacité de notifier aux utilisateurs finaux l'apparition d'événements liés à la sécurité.

7.8 Intégrité du logiciel/ micrologiciel

Le fait que les règles du marché de la microélectronique requièrent d'énormes volumes de ventes d'un seul article pour être économiquement viables, implique l'émergence de scénarios d'IdO caractérisés par des dispositifs matériels polyvalents, dont la fonctionnalité opérationnelle spécifique est dictée par le logiciel ou le micrologiciel qu'ils exécutent.

Il est très important que ces dispositifs universels, dès le début (boot) et à partir de la fin (run), **puissent vérifier l'intégrité des éléments logiciels qu'ils exécutent** et ne puissent pas être modifiés de telle sorte qu'ils finissent par faire des choses pour lesquelles ils n'ont pas été conçus.

Le contrôle de toute architecture IoT dépend inévitablement, d'une part, de la capacité à mettre à jour le logiciel et, d'autre part, de la possibilité de modifier physiquement le fonctionnement du matériel lui-même (*firmware*).

7.8 Intégrité du logiciel/micrologiciel

La vérification de la **présence de mises à jour de logiciels/ micrologiciels non sécurisés** comprend:

- Vérifiez que le fichier de mise à jour ne contient pas d'informations sensibles susceptibles d'être exposées, même si elles sont masquées.
- Examiner la production des fichiers de mise à jour afin qu'ils mettent en œuvre un cryptage correct à l'aide d'algorithmes et de procédures approuvés.
- Examinez la sortie du fichier de mise à jour et vérifiez qu'il est toujours correctement signé.
- Examiner la sécurité et la robustesse de la méthode de communication utilisée pour transmettre les mises à jour et faire connaître leur existence. Il faut éviter que des systèmes ne soient pas mis à jour parce qu'ils ne savaient pas qu'ils étaient censés l'être.
- Vérifiez le serveur de mise à jour sur le réseau pour vous assurer que les méthodes de cryptage des communications sont à jour et correctement configurées, et que le serveur de mise à jour lui-même n'est pas vulnérable.
- Vérifiez que le périphérique valide ou signe correctement les fichiers de mise à jour.

7.8 Intégrité du logiciel/micrologiciel

La sécurisation du logiciel/micrologiciel fonctionnant sur un appareil nécessite:

- Assurez-vous que l'appareil a la capacité réelle de se mettre à jour. Dans l'IoT, il est très important que tout dispose d'un mécanisme de mise à jour sécurisé.
- Assurez-vous que le fichier de mise à jour est crypté à l'aide de méthodes et d'algorithmes reconnus comme sûrs.
- Assurez-vous que le fichier de mise à jour est transmis par une connexion cryptée et que le processus d'installation ou de configuration se termine par une phase d'auto-test positive. S'il n'est pas positif, le processus de mise à jour doit être complètement inversé.
- Assurez-vous que le fichier de mise à jour n'expose pas de données sensibles.
- Assurez-vous que le fichier de mise à jour est signé et vérifié avant que la mise à jour ne soit publiée, distribuée et appliquée.
- Assurez-vous que le serveur de mise à jour est complet et sécurisé.
- Mettez en place un démarrage sécurisé du dispositif si possible et de sa chaîne de confiance.

7.9 Sécurité physique

Certaines attaques nécessitent un accès physique à l'appareil et ne peuvent donc pas être réalisées à distance. Cela sera particulièrement facile dans l'IdO, car les appareils seront à côté de ce qu'ils mesurent ou font fonctionner, et n'auront donc généralement rien de physique pour les protéger.

Puisque l'attaquant pourra accéder à l'appareil, ou s'en approcher aussi près qu'il le souhaite, il est nécessaire de vérifier si les mesures prises par chaque fabricant sont suffisantes pour assurer la **sécurité physique de l'**appareil:

- Examinez la facilité avec laquelle le dispositif peut être démonté et **ses supports de stockage accessibles ou retirés.**
- Examinez l'utilisation de **ports externes**, tels que le port USB, pour déterminer si les données contenues dans le dispositif sont accessibles sans démontage.
- Vérifiez si tous les ports physiques externes **sont nécessaires** au fonctionnement de l'appareil.
- Vérifiez l'interface d'administration pour déterminer si les ports externes, tels que les ports USB, **peuvent être désactivés.**
- Examinez l'interface administrative pour déterminer si les capacités de l'administrateur peuvent être l**imitées au niveau local.**

7.9 Sécurité physique

Une protection physique adéquate nécessite:

- Assurez-vous que les supports de stockage ne peuvent pas être facilement retirés.
- Assurez-vous que les données stockées sont **cryptées au repos.**
- Veillez à ce que les ports USB et autres ports externes ne puissent pas être utilisés pour accéder à l'appareil de manière nuisible.
- Assurez-vous que l'appareil **ne peut pas être facilement démonté**.
- Assurez-vous que seuls les ports externes, tels que les ports USB, réellement nécessaires au bon fonctionnement de l'appareil sont autorisés.
- Assurez-vous que le produit a la **possibilité de limiter les capacités administratives.**

8. Conclusions

La cybersécurité est confrontée à un nouveau défi provenant des objets quotidiens qui nous entourent, l'Internet des objets (IoT). Des machines à café et des réfrigérateurs aux assistants virtuels et aux caméras vidéo, les consommateurs utilisent une nouvelle vague d'appareils connectés, mais envisagent rarement les vulnérabilités qu'ils peuvent apporter.

Les attaques IoT exposent les entreprises à des pertes de données et de services, et peuvent rendre les appareils connectés dangereux pour les clients, les employés et le grand public. Les vulnérabilités potentielles continueront de croître à mesure que le nombre d'appareils dépendant d'internet augmente.

Avec peu de réglementation en place pour responsabiliser les fabricants d'objets connectés, ces appareils offrent une **voie directe pour accéder à des données personnelles, industrielles ou d'entreprise, souvent très sensibles.**

Pendant ce temps, les équipes de sécurité s'efforcent de faire face à un **paysage de menaces** de plus en plus **complexe**, où tout appareil peut faire l'objet d'attaques sophistiquées.

La plupart des **appareils IoT ne sont pas conçus et construits en pensant à leur sécurité et à celle des autres**, mais sont conçus pour leur fonctionnalité, leur facilité d'utilisation et leur mise sur le marché rapide. Ces appareils sont généralement bon marché, utiles et, si nécessaire, simples à configurer, ce qui a souvent un coût pour la sécurité.

Les vulnérabilités potentielles continueront de croître à mesure que le nombre d'appareils dépendant d'Internet augmente.

8. Conclusions

La nature naissante de ce nouveau paradigme, et le fait que la plupart des attaques IoT n'ont été que de simples preuves de concept sans conséquences graves, ne signifie pas que les attaquants du cyberespace ne se concentreront pas sur ce marché à l'avenir.

Une étude de Hewlett-Packard a révélé que 70 % des appareils IoT les plus utilisés contiennent une multitude de vulnérabilités pouvant être exploitées par des attaquants. En outre, 80 % de ces appareils posent de sérieux problèmes de confidentialité, car ils collectent des données particulières, le plus souvent inutiles, **sur l'utilisateur et sa situation.**

Pour l'instant, seule **la demande de sécurité de la part de l'utilisateur final et de la société dans son ensemble** pourra imposer aux fabricants et au marché la nécessité de considérer tous ces aspects **avant de lancer un produit sur le marché**. Cette même demande obligera les autorités et les différents secteurs professionnels à opter pour des **mesures réglementaires afin de protéger les citoyens et la société en général** des conséquences d'un peuplement de la planète par des milliards d'appareils non sécurisés.

Contrairement aux cyberattaques traditionnelles, les incidents liés à l'IdO ne se limitent pas à l'extraction d'informations, mais peuvent être utilisés pour c**auser des dommages physiques** et exploités par des cyberattaquants parrainés par des États pour causer de graves dommages.

Sécuriser la "chose" n'est peut-être pas la solution, car il y aura toujours trop d'éléments à gérer. Au lieu de cela, l'observation et la surveillance permettront d'accroître la visibilité, ce qui, associé à l'analyse et à une réponse rapide, fournira une approche pragmatique pour réduire les risques inhérents à la croissance des dispositifs IoT. À ce titre, les aspects à prendre en compte seraient les suivants :

Ces dispositifs offrent un moyen direct d'accéder à des données personnelles, industrielles ou d'entreprise, souvent très sensibles.

15. Voir http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en

8. Conclusions

Concentrez-vous sur ce que vous pouvez voir. Les appareils IoT ont souvent un point de contrôle, qu'il s'agisse d'un routeur, d'un pare-feu ou d'un proxy au périmètre du réseau ou dans le cloud. La visibilité doit être obtenue et, si possible, contrôlée.

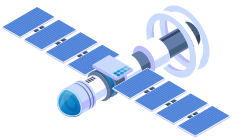
L'analyse comme meilleur ami. Les appareils IoT partagent une caractéristique souvent négligée : leur comportement est prévisible. L'application de l'apprentissage automatique pour la modélisation comportementale est extrêmement efficace pour profiler les risques, détecter les anomalies et réagir.

Disposer d'un personnel de sécurité dédié. La surveillance, les enquêtes et les mesures correctives ne doivent jamais s'arrêter, et un personnel capable d'analyser la situation doit être disponible pour formuler une réponse appropriée.

Le succès se résume à l'établissement d'une base de surveillance et de contrôle pour réduire l'exposition aux risques et à l'application de techniques intelligentes à la population croissante d'appareils IoT.

9. Décalogue des recommandations

Voici dix (10) recommandations en matière de sécurité pour *l'architecture IoT.*



Décalogue de sécurité puor les architectures IoT

1. Évitez d'utiliser les dispositifs IoT lorsqu'ils ne sont pas strictement nécessaires.
2. N'utilisez pas, dans la mesure du possible, de dispositifs IoT qui transmettent des informations à des serveurs externes (le Cloud), même s'il s'agit de ceux du fabricant.
3. Changez les mots de passe par défaut sur les appareils et utilisez des mots de passe vraiment forts qui ne figurent dans aucun dictionnaire, qui sont suffisamment longs et donc difficiles à deviner.
4. Maintenez les appareils à jour avec les dernières versions de logiciels et de micrologiciels disponibles.
5. Désactivez toutes les connexions à distance (internet) des appareils lorsqu'elles ne sont pas strictement nécessaires.
6. Ne gardez ouverts que les ports de communication qui sont vraiment nécessaires et modifiez les ports d'écoute si possible.
7. Si les dispositifs IoT ne permettent pas de configurer leur sécurité, faites-les toujours fonctionner sur un réseau local (LAN) derrière un dispositif (routeur) correctement configuré qui assure cette sécurité.
8. Dans la mesure du possible, assurez l'authenticité, la confidentialité et l'intégrité de toutes les communications locales (LAN), surtout si elles sont effectuées par des liaisons radio (Wi-Fi, Bluetooth, etc.).
9. Vérifier périodiquement et sans préavis la configuration de la sécurité de tous les éléments de l'architecture IoT et de ses dispositifs de communication avec le monde extérieur.
10. Vérifiez la visibilité de vos propres dispositifs dans les moteurs de recherche de dispositifs IoT tels que Shodan.

CCN centro criptológico nacional

CCN cert centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es