TechTarget | LeMagIT E-handbook

Contenu PRO+

IoT et sécurité : les clés pour comprendre l'évolution des pratiques

Dans ce guide

Introduction.

Dès 2016, les botnets Mirai et ses variantes (Satori, Reaper, entre autres) ont permis de mettre le doigt sur les problématiques de sécurité IoT. Cet épisode particulièrement médiatisé – et qui pourtant n'a jamais pris réellement fin – avait entraîné un début de prise de conscience des industriels, en premier lieu les fabricants des appareils et gateways infectés par de tels réseaux zombies.

Pour autant, de par les particularités de l'internet des objets, assurer la sécurité des parcs d'appareils s'avère complexe. Et si la part des équipements connectés a augmenté dans le grand public ou dans les bureaux, depuis l'industrie s'est emparée du sujet. Il suffit d'observer les efforts des énergéticiens tels EDF ou Suez, mais également des industriels de la défense en la matière pour se rendre compte que la sécurité de l'IoT est devenue un enjeu critique. Or, là où l'intégration des objets connectés les plus courants peut s'apparenter à une problématique purement IT, l'IIoT implique un pont entre IT et OT.

Dans ce guide

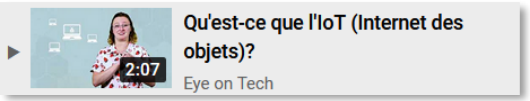
Aussi, dans une usine des équipements et machines de différentes générations cohabitent : il faut prendre en compte les spécificités de plusieurs technologies de communication. Cela veut dire également qu'il n'est pas forcément possible de les mettre à jour une fois déployés. De plus, leurs capacités techniques limitées peuvent empêcher d'y exécuter des microprogrammes de sécurité ou des systèmes de chiffrement. Sans oublier les menaces purement physiques : certains équipements peuvent être installés sur des terrains distants et sont exposés à des risques de manipulation par des attaquants bien réels.

« Il est illusoire de vouloir proposer une lecture unique de la sécurité des objets connectés du fait de la diversité des situations rencontrées », écrivent les spécialistes de l'ANSSI dans un guide intitulé « Recommandations relatives à la sécurité des (systèmes d') objets connectés ». Le document liste des conseils quant aux architectures matérielles et logicielles à mettre en place, l'instrumentalisation de la cryptologie et de l'authentification dans un tel contexte, la manipulation des données sensibles, la sécurité logicielle et matérielle, la

Dans ce guide

protection des réseaux et la gestion du cycle de vie des dispositifs connectés. Mais comme le précise l'ANSSI, tout commence par une analyse des risques de laquelle découle l'application de ces diverses mesures plus ou moins strictes.

Or les entreprises se frottent à l'apparition de nouveaux concepts de sécurité qui, dans la bouche des éditeurs et fournisseurs, sont censés remplacer les anciens. Pourtant, en réalité, des solutions existantes en matière de gestion d'identité et de surveillance du réseau ont toute leur place dans une démarche de sécurisation de l'IoT. D'autres paradigmes, comme la supervision des logiciels, s'étendent désormais aux firmwares des objets connectés, même s'ils concernent en majorité des déploiements greenfield. C'est justement tout l'objet de ce guide essentiel qui vise à explorer les évolutions de ces trois volets – la gestion des identités, la surveillance du réseau et la supervision des vulnérabilités – au regard des pratiques des entreprises les plus conscientes de ces enjeux.



Dans ce guide

IoT : comment la PKI s'est imposée pour l'identité des objets connectés

Malgré des interrogations – il y a quelques années –, des défis, voire des divergences persistantes, les infrastructures à clé publique (PKI) se sont imposées dans le monde des objets connectés.

Valéry Rieß-Marchive, Rédacteur en chef

C'est à l'automne 2015 qu'OpenTrust a décidé de se recentrer sur l'identité numérique, cédant son activité de certification de documents et de transactions à DocuSign. À cette occasion, l'éditeur français a changé de nom pour IDnomic, afin d'illustrer son recentrage... avant d'être racheté par Atos en 2019.

À l'occasion d'une rencontre avec la rédaction en 2016, Dan Butnaru, toujours directeur marketing d'IDnomic, soulignait l'importance du marché des objets connectés pour IDnomic, avec en particulier le segment de l'automobile. Et de relever qu'il n'avait pas fallu attendre les révélations sur les vulnérabilités relatives à certains véhicules Chrysler ou encore BMW, en 2015 : « cela a commencé avec l'initiative européenne pour les systèmes de transport intelligents ».

Dans ce guide

Le sujet s'articulait autour de trois axes : authentification, confidentialité et intégrité. Mais ces besoins ne sont pas spécifiques à l'automobile et aux systèmes de transport intelligents : « on retrouve les mêmes besoins dans d'autres segments, comme les compteurs intelligents ou l'industrie 4.0, avec les capteurs. Ce sont des concepts sur lesquels on travaille pour l'automobile et que l'on va naturellement reprendre ailleurs », expliquait alors Dan Butnaru.

À l'époque, les interrogations autour de X.509 ne manquaient pas, notamment avec la volumétrie des traitements pour la vérification d'une chaîne de certificats potentiellement longue, en des temps très courts : « le simple fait d'avoir un certificat plus petit [qu'avec X.509] ne va pas suffire. Vérifier mille certificats à la seconde, on n'a pas encore fait », expliquait alors Dan Butnaru.

Mais il y a également la question du renouvellement des certificats côté clients. L'expiration du vieux certificat IdentTrust DST Root X3 de Let's Encrypt, fin septembre 2021, a fourni une illustration du problème. En 2020, Roku a dû alerter d'un risque pour certains flux diffusés par sa plateforme en raison de l'expiration d'un autre certificat. Heureusement, les terminaux de Roku ont pu être mis à jour.

Cette année, Bosch a mis à jour sa plateforme IoT pour s'assurer que les objets connectés développés avec elle ne seraient pas laissés de côté du fait de l'expiration du certificat de Let's Encrypt. Mais quid des autres objets

Dans ce guide

connectés, et en particulier ceux qui ne sont pas – ou ne seront pas, demain – mis à jour ?

Pour autant, c'est bien X.509 qui a remporté la bataille, profitant notamment – très vite – du soutien de poids lourds tels que Microsoft, avec Azure IoT Hub, et AWS. Et selon une récente étude de l'institut Ponemon pour Entrust, la PKI « fournit une technologie d'authentification essentielle pour l'IoT ». Près de la moitié des 2 513 sondés – répartis dans 17 pays ou régions du monde – estime que l'IoT est le principal moteur du déploiement d'applications utilisant la PKI. Mais tout n'est pas réglé pour autant.

La question de la révocation des certificats continue, manifestement, de diviser. Ainsi, le protocole OCSP (Online Certificate Status Protocol) arrive en tête, mentionné par 57 % des sondés, devant les listes de révocation des certificats (CRL), à 42 %. Mais près d'un tiers des sondés ont déclaré ne pas utiliser de technique de révocation de certificat.

Les auteurs de l'étude avancent de potentielles explications : « utilisation d'autres moyens pour supprimer les utilisateurs/dispositifs, utilisation de certificats à courte durée de vie, systèmes fermés, etc. ». Kevin Bocek, ancien vice-président de Venafi, évoquait d'ailleurs la piste des certificats éphémères, lors d'un échange avec LeMagIT, à l'été 2016.

Dans ce guide

FIDO Device Onboarding : forces et faiblesses d'un standard IoT

La FIDO Alliance compte bien convaincre les fabricants avec son standard sécurisé de déploiement IoT, FIDO Device Onboarding. Dans cet article, LeMagIT revient en détail sur le fonctionnement de ce protocole, ses limites et sur les différences avec une architecture PKI, plus classique.

Gaétan Raoul, Journaliste

La FIDO Alliance propose une spécification IoT prévue pour automatiser le provisionnement sécurisé d'équipements de leur fabrication jusqu'à leur installation et leur raccordement à n'importe quel cloud. Son nom ? FIDO Device Onboarding ou FDO.

Basée sur la technologie Intel Secure Device Onboard (SDO), la spécification décrit un processus en six actes.

À l'étape 1, le code FDO est embarqué dans les objets connectés, tout comme les clés de chiffrement nécessaires à sa protection.

« Le système exploite la cryptographie asymétrique pour les paires de clés publiques et privées. Mais nous ne nous appuyons pas sur une autorité de certificat. Nous utilisons la chaîne d'approvisionnement elle-même comme la racine de confiance », précise David Turner, directeur du développement des standards chez la FIDO Alliance.

Six étapes pour un déploiement IoT

À l'étape 2, les équipements sont emballés et distribués. À ce moment-là, un fichier texte appelé justificatif de propriété (intitulé Ownership Voucher) est produit. Ce fichier atteste du transfert de propriété entre le fabricant et son client. « Il se présente sous la forme d'une chaîne de clés publiques signées, chaque signature d'une clé publique autorisant le possesseur de la clé privée correspondante à prendre possession du dispositif ou à transmettre la propriété à un autre maillon de la chaîne », peut-on lire dans la documentation.

Dans le principe, il peut enregistrer la trace de passage d'un fabricant, du distributeur, du revendeur, ainsi que du ou des différents propriétaires d'un équipement. La signature dépend des algorithmes RSA ou ECDSA. Les informations de propriété de l'équipement sont chiffrées via les fonctions Hash SHA256 ou SHA384, vérifiées par les HMAC équivalents. En parallèle, ces clés sont envoyées au fournisseur de services cloud ou à un système de

Dans ce guide

device management pendant que le matériel lui-même est acheminé vers l'installateur ou le client.

Puis vient la troisième étape. « Une fois que le fournisseur de cloud ou le gestionnaire de device management a reçu les clés, il enregistre le bien correspondant à la clé dans un service Rendezvous, qui est essentiellement un service de consultation de type DNS », explique David Turner. Ce service Rendezvous dépend d'un serveur.

La quatrième étape coïncide avec le premier démarrage de l'équipement. À ce moment-là, l'objet exécute le code FDO qui émet un appel vers le serveur Rendezvous. Le service Rendezvous fait le lien entre l'appareil et les identifiants de son propriétaire, lui transfère ces informations et lui associe une adresse IP.

Les échanges de clés entre le serveur Rendezvous, les objets connectés et la plateforme sont baptisés « transferts de propriété ». La spécification FDO comprend trois de ces passages de flambeau (TO0, TO1 et TO2), assimilés à des protocoles. Les transferts de propriété, donc le moment où les clés publiques sont ajoutées à la chaîne de confiance, demandent d'adopter les protocoles HTTPS et TLS. « Une fois l'authentification effectuée, ce canal sécurisé est ensuite exploité pour effectuer le provisionnement afin d'établir une connexion sécurisée », précise le directeur.

Dans ce guide

« Une fois que l'appareil sait où aller, il suit l'étape cinq dans laquelle il communique avec le cloud ou la plateforme IoT sur site. À ce stade, l'équipement et le service de device management partagent leurs clés publiques. C'est une phase d'authentification mutuelle qui permet au service cloud de faire confiance à l'appareil, de s'assurer qu'il s'agit bien de celui que son utilisateur a acheté, mais la machine peut également faire confiance au propriétaire qui essaie de le paramétrer. L'objectif est d'éviter les attaques malveillantes aux deux extrémités du processus », déclare David Turner.

À lire également :

La FIDO Alliance veut sécuriser les déploiements IoT

Ce n'est donc que lors de cette cinquième étape que les informations spécifiques et les détails de configuration liés à l'environnement sont fournis. C'est ce que l'Alliance a appelé une liaison tardive (« late binding ») entre les équipements et la plateforme IoT. Une fois provisionnés et authentifiés, les appareils connectés peuvent collecter et envoyer leurs données vers une plateforme cloud. « Les clés initiales utilisées dans les étapes un à cinq sont supprimées à l'étape six et remplacées par un autre jeu de clés fourni par le service cloud », complète le directeur du développement des standards au sein de la FIDO Alliance. À la fin de ce provisionnement, ce sont les services de type KMS ou HSM associés à l'architecture de l'usager qui administrent les certificats et les clés pour protéger les données recueillies.

Avant cela, tous les renseignements concernant l'appareil sont transférés vers le service de device management, désormais uniquement accessible par son propriétaire. Seules les clés OCDeviceInfo et la Hardware Root of Trust ne sont pas changées. Ce qui veut dire que le certificat de naissance de l'équipement est réduit à sa plus simple expression après l'authentification mutuelle avec la plateforme IoT. La FIDO Alliance considère que ces deux éléments fournissent « suffisamment d'informations pour construire un justificatif de propriété avec zéro entrée ».

FDO est plus adapté aux nouveaux projets IoT

Avec cette spécification, tous les équipements doivent être capables de supporter les attestations et les vérifications à l'aide de moyens cryptographiques répondant aux exigences du protocole EAT (Entity Attestation Token). Pour l'attestation des équipements, l'alliance impose l'algorithme ECDSA (Eliptic Curve Digital Signature Algorithm) ou, SDO oblige, le système de signature sous licence apache 2.0, Intel EPID. Les signatures ESCDSA sont basées sur les courbes elliptiques SECP256R1 ou SEC384R1 encodées via COSEX509 ou le plus traditionnel X509. Intel EPID dispose lui aussi de deux variantes algorithmiques.

Cependant, il est à préciser que cette chaîne de confiance n'est valable que si les équipements sont capables de supporter les opérations de chiffrement et que tous les membres de la chaîne se sont entendus sur le choix d'algorithme, pour crypter les attestations des machines IoT et les parafes indiquant le transfert de propriété. En clair, la spécification prévoit plusieurs options de déploiement, mais il ne faut en choisir qu'une pour chaque protocole et service.

Selon Jon Ferguson, Directeur Product Management chez Entrust, cela signifie que ce type de spécification est davantage compatible avec le déploiement d'un nouveau projet IoT. « Il y a la question des déploiements brownfield et greenfield. Les acteurs de ce marché tentent d'abord de résoudre le problème greenfield, parce que c'est plus facile », déclare-t-il. « Entrust associe à son infrastructure PKI un agent à même l'équipement, pour surveiller son comportement tout au long de son cycle de vie ».

FDO ne met pas les architectures PKI au placard

Tout comme Keyfactor, GlobalSign et d'autres éditeurs de solutions mêlant IoT et une infrastructure à clés publiques (PKI), Entrust mise lui sur une identité unique, un certificat de naissance, supposé immuable, placé au sein d'un appareil qu'une technologie de chiffrement peut vérifier quand il se

connecte à une passerelle ou à un serveur central. Au lieu d'un justificatif de propriété, les éditeurs de PKI fournissent des certificats basés sur la norme X509.

Avec ce modèle, une autorité centrale signe ou valide les certificats d'origine utilisés tout au long du cycle de vie des équipements. L'autre grande différence avec FDO tient dans le fait que la génération des clés privées et publiques est forcément effectuée depuis un HSM. Les clés privées, ici des certificats d'autorité, sont stockées au sein de ce module matériel renforcé associé à un serveur. Les clés publiques sont embarquées dans une zone sécurisée d'un équipement IoT. Ensuite, un système de type Active Directory (voire AD lui-même) est utilisé pour gérer les politiques d'accès aux clés, de gestions et d'audits. Avec FDO, ce rôle est joué en partie par la plateforme IoT. En clair, une architecture PKI peut jouer également ce rôle d'enrôlement des nouveaux équipements, mais les possibilités sont plus nombreuses. Entrust propose par exemple de vérifier par chiffrement les mises à jour de firmwares IoT.

Les composants IoT sont encore trop peu robustes

Si la spécification FDO recommande de stocker les clés publiques au sein d'une zone sécurisée de l'appareil et les clés privées au sein d'une zone

Dans ce guide

protégée d'un serveur, ce choix est « laissé à l'utilisateur final ». « Il y a beaucoup de variations possibles. La façon dont vous [stockez les clés] ne fait pas partie de notre spécification », déclare David Turner.

> **« Il y a beaucoup de variations possibles. La façon dont vous [stockez les clés] ne fait pas partie de notre spécification ».**
>
> **David Turner**
> Directeur du développement des standards, FIDO Alliance

« Les clés peuvent être stockées n'importe où sur le dispositif, que ce soit dans un élément matériel ou logiciel renforcé (de type Trusted Platform Module – TPM ou Trusted Execution Environnement) ou dans un dossier du système de fichiers, potentiellement le moins sécurisé possible. Ainsi, l'une des considérations lors de l'achat d'un dispositif est de savoir si celui-ci est sécurisé. Alors que le protocole lui-même peut être sécurisé, le dispositif peut ne pas être aussi robuste que vous le souhaitez », reconnaît-il. La documentation de SDO est plus stricte et assure que les clés privées doivent être stockées soit dans un élément TPM, soit dans un HSM séparé.

Pour mitiger ce risque, la FIDO Alliance propose des certifications payantes aux fabricants d'équipements. Ces procédures devraient comprendre plusieurs niveaux attestant de la fiabilité d'un appareil.

Dans ce guide

D'après Jon Ferguson, la gestion des clés de chiffrement depuis des objets connectés n'aurait rien d'aisé. « Un des enjeux relatifs à l'IoT est que les équipements sont fortement dépendants de systèmes Linux et de microcontrôleurs. Et ces deux éléments ne sont pas très propices à la gestion et à la génération de clés, car les capacités du processeur sont généralement très faibles et ce n'est que récemment que les accélérateurs de cryptographie ont commencé à devenir plus courants dans ces appareils », constate-t-il.

« Si vous regardez les TPM et les éléments sécurisés, ils sont limités à un très petit nombre de clés et deux algorithmes. Actuellement, toute personne dans l'écosystème Iot qui déploie une solution qui s'appuie sur la cryptographie classique ignore la réalité de l'informatique quantique », ajoute-t-il.

De plus, les distributions Linux embarquées n'auraient pas d'espace de stockage des clés de chiffrement attribué, « contrairement à Windows ou macOS », selon Jon Ferguson. Contre-exemple, Ubuntu tente de son côté de standardiser ces aspects sécuritaires depuis peu.

> **« Actuellement, toute personne dans l'écosystème IoT qui déploie une solution qui s'appuie sur la cryptographie classique ignore la réalité de l'informatique quantique ».**
>
> **Jon Ferguson**
> Directeur, Product Management, Entrust.

Une spécification pensée pour faciliter la tâche des fabricants et des distributeurs

Mais la FIDO Alliance veut surtout retirer une épine du pied aux fabricants en proposant une solution de déploiement censée être plus sécurisée et plus rapide que les protocoles existants.

« Lorsqu'un fabricant usine un produit IoT, il n'a pas besoin de savoir à l'avance quel sera l'environnement physique ou virtuel où il sera installé. Souvent, le manufacturier doit fournir des informations caractéristiques dans l'objet connecté au moment de la confection, afin qu'il puisse être employé avec une plateforme IoT et dans un environnement particulier, ce qui peut inclure des exigences de sécurité distinctives et des détails de configuration associés à certains logiciels de gestion IoT », explique David Turner. « Avec notre spécification, cette décision n'intervient pas avant le processus d'embarquement lui-même. Donc les fabricants peuvent maintenant produire beaucoup d'appareils sans avoir à dire que ces dix mille unités sont destinées à cet utilisateur final ».

« La principale raison pour laquelle j'ai rejoint Entrust il y a cinq ans, c'est que je travaillais beaucoup avec des fabricants d'équipements IT/OT dans l'aérospatial, des spécialistes des systèmes SCADA et de réponses à incidents », raconte Jon Ferguson. « À l'époque la notion de sécurité était

Dans ce guide

repoussée au niveau du réseau ou fondée sur des clés prépartagées, groupées, codées en dur, etc. avec beaucoup de choses basées sur l'obfuscation. Ces cinq dernières années, il y a eu une prise de conscience que l'obfuscation n'est efficace que si vos ventes sont mauvaises. Quand vous commencez à déployer beaucoup de matériels IoT sur le terrain, vous devenez une cible de choix ».

Et d'ajouter : « si ces objets sont connectés, leur capacité rudimentaire les expose à différents risques, d'autant que certains fabricants ont longtemps considéré la configuration de sécurité comme optionnelle ».

En l'état, FDO représente un pas en avant et sûrement une étape complémentaire à une architecture PKI ou tout autre dispositif pour protéger de bout en bout une flotte d'équipements IoT. Mais la FIDO Alliance doit convaincre l'ensemble de l'écosystème IoT. Un exercice loin d'être aisé.

« Quand vous commencez à déployer beaucoup de matériels IoT sur le terrain, vous devenez une cible de choix ».

Jon Ferguson
Directeur, Product Management, Entrust.

Dans ce guide

Industrie 4.0 : Fives CortX déploie Wallix Bastion sur ses gateways

Filiale dédiée au Big Data et à l'IoT du groupe Fives, Fives CortX a fait le choix de la solution Bastion de Wallix pour accroître le niveau de sécurité de sa solution d'analyse des données industrielles.

Alain Clapaud, Journaliste

Le groupe d'ingénierie industrielle français Fives mène plusieurs initiatives dans le domaine de l'industrie 4.0. Ainsi, en 2016, sa filiale Intralogistics a lancé une start-up interne sur la valorisation des données issues des process et des machines. Baptisé CortX, ce projet est devenu une filiale à part entière en décembre 2017, avec pour vocation de développer des solutions prédictives pour les filiales du groupe industriel et leurs clients.

Ses ingénieurs ont créé des modèles d'IA dédiés à la qualité industrielle et la maintenance prédictive, mais aussi une architecture de collecte des données de fonctionnement des machines et des process dont une gateway qui s'installe en pied de machine. « Outre l'algorithmique, notre valeur ajoutée se situe sur l'ensemble de la chaîne d'acquisition des données, depuis la captation, sa mise en forme, son traitement et jusqu'à sa restitution », résume David Zak, CEO de Fives CortX.

Dans ce guide

Une approche Edge Computing pour collecter les données

La brique d'acquisition qui est déployée sur le terrain, dans les ateliers, doit faire le pont entre les systèmes de production industriels, l'OT (Operational Technology) et l'IT. Cette gateway collecte les données de fonctionnement et va alimenter une chaîne de traitement comprenant des briques de stockage, de calcul et de restitution qui peuvent être soit en Edge Computing, donc sur le site industriel, soit déportées dans le cloud. « Selon le domaine d'activité que l'on sert, selon le client lui-même, nous sommes autorisés ou pas à avoir un accès réseau dans leurs installations industrielles et utiliser des services cloud. C'est une contrainte d'architecture forte et c'est aussi la raison pour laquelle nous travaillons énormément sur le volet cybersécurité de cette chaîne d'acquisition de données », ajoute le responsable.

> **« Selon le domaine d'activité que l'on sert, selon le client lui-même, nous sommes autorisés ou pas à avoir un accès réseau dans leurs installations industrielles et utiliser des services cloud. »**
>
> **David Zak**
> CEO, Fives CortX

Parmi les choix techniques réalisés par l'équipe projet, les données collectées étant généralement

Dans ce guide

des données temporelles, la solution met en œuvre des bases de données de type « Time Series », à commencer par InfluxDB. Des bases de données orientées document comme MongoDB permettent de stocker des images. D'autres données sont stockées dans des SGBD relationnels classiques. « Pour analyser ces données, nous mettons en œuvre Hadoop Spark et très récemment nous avons fait le choix de la plateforme Dataiku afin de nous aider à industrialiser les traitements et analyses réalisés sur les données ».

David Zak, CEO Fives CortX.

Les experts de Fives CortX adaptent leurs choix techniques en fonction de chaque client, car David Zak estime qu'il n'est pas possible de déployer des solutions « sur étagère » pouvant répondre aux attentes de l'ensemble des clients de CortX, même si les briques techniques mises en œuvre sont classiques. « Nous assemblons ces briques afin de constituer des solutions sur-mesure adaptées au domaine d'activité de chaque client », conclut le responsable.

En outre, la solution est dotée d'un portail d'accès développé par l'éditeur Visiativ avec qui Fives CortX a créé une joint-venture pour proposer des solutions packagées aux fabricants de machines. Baptisée Up&Run, la solution est constituée du portail applicatif dans lequel s'exécutent les

modèles prédictifs créés par les Data Scientists de Fives CortX : quand le modèle détecte une panne, celle-ci est historisée sur le portail plutôt que d'apparaître sous la seule forme d'une alerte qui ne va pas être traitée immédiatement. Les concepteurs estiment qu'il est plus efficace de proposer un portail où tous les tickets sont listés, ainsi que les interventions et la gestion des pièces de rechange, jusqu'à la tournée des techniciens de maintenance. L'éditeur propose un écosystème complet pour la maintenance des machines. « Nos clients sont ceux de Fives, donc essentiellement des grandes entreprises industrielles, des logisticiens. Avec notre co-entreprise avec Visiativ, nous visons désormais les constructeurs de machines, les PME ».

La clé de développement des outils Industrie 4.0 : la cybersécurité

Si les industriels de l'aéronautique ou de la défense se montrent plutôt réticents à connecter leurs systèmes Industrie 4.0 au cloud, ils sont aussi extrêmement prudents lorsqu'il s'agit de déployer des gateways au cœur de leur outil industriel. « La cybersécurité est un levier majeur pour le développement de ces solutions », estime David Zak. « Les attaques informatiques se sont multipliées sur les systèmes industriels et c'est une préoccupation forte de beaucoup de nos clients ».

Dans ce guide

Si les grandes entreprises testent depuis plusieurs années des applications de maintenance prédictive, celles-ci passent enfin du stade de proof-of-concept isolé à des déploiements à beaucoup plus large échelle. La cybersécurité est beaucoup plus étudiée ; les DSI sont désormais embarqués dans ce type de projet et demandent désormais aux éditeurs de leur présenter les solutions mises en œuvre pour sécuriser les infrastructures industrielles.

Si le CEO de Fives CortX se montre peu disert sur les briques de sécurité embarquées dans sa gateway, il précise que la sécurité de l'architecture de collecte des données est assez classique, avec notamment un firewall d'origine Open Source intégré à la gateway afin de filtrer les flux.

Les échanges de données sont par ailleurs chiffrés. Récemment, Fives CortX a annoncé l'intégration de ses briques logicielles avec le Bastion Wallix, notamment le logiciel de connexion qui implémente les protocoles industriels des automates.

« Dans ce cadre, l'offre Bastion de Wallix apparaissait comme idéale pour compléter la sécurité de note gateway. L'intégration technique a été menée afin d'intégrer la solution dans le hardware beaucoup plus contraint de notre gateway en pied de machine, isolée, afin de sécuriser les flux vers la base de données lorsqu'elle est dans le cloud, mais aussi les flux à destination des commandes numériques, des automates, des réseaux de capteurs ».

Deux fonctionnalités du Bastion sont mises à profit par la gateway. Wallix Bastion assure d'une part la gestion des accès afin d'isoler le plus possible les différents systèmes. En cas de compromission de la plateforme, les attaquants ne pourront pas accéder aux équipements qui lui sont connectés. Tous les mots de passe des équipements sont protégés par le Bastion, de même que les accès à la base de données. En outre, l'intégrité du système de fichier de la gateway est surveillée en permanence par la solution Wallix. La gateway se verrouille automatiquement en cas de modification du système de fichiers.

Tous les mots de passe des équipements sont protégés par le Bastion, de même que les accès à la base de données.

La gateway pourrait jouer le rôle de plateforme de sécurité OT

Pour l'heure, la gateway Fives CortX n'embarque pas de solution de surveillance et d'analyse du trafic réseau. « Nous sommes ouverts à embarquer d'autres briques de sécurité sur notre gateway et c'est notre ambition de le faire un jour », précise David Zak. « Nous proposons une solution de terrain qui pourrait être un rempart pour améliorer la sécurité. Nos clients nous demandent quelles solutions de sécurité sont mises en

Dans ce guide

œuvre et ces choix sont validés par leur DSI, mais pour l'instant nous n'avons pas eu de requête afin d'installer des outils de sécurité particuliers ».

Le responsable le reconnaît, l'essentiel des déploiements de la gateway sont réalisé en mode edge, c'est-à-dire sans connexion réseau. Nul doute qu'avec l'essor de la 5G la situation pourrait changer... si la sécurité de l'accès est garantie. « Nous suivons le lancement de la 5G de très près. Cela reste encore des pistes de réflexion pour nous et le déploiement de la 5G dans l'IoT nous simplifiera la vie, mais cela imposera certainement de mettre en œuvre de nouvelles briques cyber sur nos appliances ».

> **« Nous sommes ouverts à embarquer d'autres briques de sécurité sur notre gateway et c'est notre ambition de le faire un jour. »**
>
> **David Zak**
> CEO, Fives CortX

Pour 2021, Five CortX met la priorité sur le développement de nouveaux algorithmes dédiés à la qualité industrielle, en améliorant ses modèles avec de nouvelles sources de données, notamment issues de la vision industrielle. La vidéo est une source de données potentiellement intéressante dans le domaine de la qualité, mais aussi pour capter des données vibratoires avec des caméras spécifiques.

Dans ce guide

Pour EDF, la cybersécurité des SI industriels a besoin de coopération

Olivier Ligneul, le directeur cybersécurité d'EDF, en est convaincu : la protection des systèmes industriels passe nécessairement par une coopération au sein de l'écosystème. Les entreprises d'une même supply chain doivent en outre accepter de partager des données.

Christophe Auffray, Journaliste

Pendant des années, la sécurité des systèmes SCADA, l'informatique industrielle, a fait parler d'elle en matière de cybersécurité, moins pour ses bonnes pratiques que pour ses déboires. En 2015 encore, les pratiques des industriels ignoraient trop souvent la sécurité dans la gestion de leurs opérations.

Trois ans plus tard, la prise de conscience semblait bien amorcée et les risques mieux pris en compte. La législation est venue accentuer les efforts des entreprises dans ce domaine, en particulier en définissant des obligations pour les opérateurs d'importance vitale (OIV). C'est le cas notamment dans l'énergie, un secteur à la fois sensible et très ciblé par les attaquants.

Dans ce guide

Un SoC exploitant des données externes

L'énergéticien français EDF en sait quelque chose. Le groupe recensait 10 millions d'attaques par an en 2016. Pour faire face à ces tentatives d'intrusion, l'entreprise dispose, depuis plusieurs années déjà, d'un SOC interne. EDF peut compter également sur son propre CERT.

Cette stratégie d'internalisation est motivée par une volonté affirmée de « garder la maîtrise », comme l'expliquait lors de l'édition 2021 du FIC, en septembre, son directeur cybersécurité, Olivier Ligneul. Mais cette maîtrise n'exclut pas des coopérations cependant. Au contraire, l'expert appelle à une approche en écosystème de la sécurité des systèmes industriels.

Cette ouverture se retrouve d'ailleurs au niveau du SOC d'EDF. Il est important, souligne Olivier Ligneul, que le centre de sécurité opérationnel dispose d'une « vision à 360° ». Cela signifie qu'il doit être en mesure de croiser des données sur un périmètre le plus large possible, « y compris grâce à des données venant de l'extérieur, dont des CERTs ».

La coopération est plus que jamais essentielle en matière de cybersécurité. Et cela pour au moins deux raisons majeures. La première tient à l'interdépendance des systèmes industriels entre eux. Une attaque contre un acteur d'une filière peut avoir des impacts sur d'autres entreprises d'une même *supply-chain*.

Dans ce guide

Des attaquants qui « commencent à comprendre nos métiers »

Car pour Olivier Ligneul, c'est bien cela : il faut « penser écosystème et dépendances opérationnelles ». Une seconde raison justifie une approche coopérative au sein des filières : les stratégies des attaquants eux-mêmes. Tous n'adoptent pas une approche visant à maximiser leurs gains grâce à un ransomware. Certains cyberattaquants déploient des approches plus discrètes destinées à leur permettre de récolter le plus d'information possible sur les entreprises cibles, afin de comprendre leur fonctionnement industriel. Une attaque peut ainsi constituer les prémices d'autres intrusions dans les SI d'entreprises de sa supply chain.

Cette réalité de la menace doit encourager une coopération approfondie, juge donc Olivier Ligneul. « Lorsqu'on est attaqué, la moindre des choses, c'est de prévenir les acteurs de sa supply chain, en amont et en aval, de manière à

> **« Lorsqu'on est attaqué, la moindre des choses, c'est de prévenir les acteurs de sa supply chain, en amont et en aval, de manière à les alerter d'un danger potentiel. »**
>
> **Olivier Ligneul**
> Directeur cybersécurité, EDF

les alerter d'un danger potentiel », exhorte-t-il en référence à des risques de propagation ou de réutilisation des informations collectées.

En matière de coopération, la marge de progression reste significative. « J'ai malheureusement un peu trop de discussions avec des membres de Comex » à ce sujet, regrette ainsi le RSSI du groupe EDF. Ce dernier plaide donc en faveur de la création d'écosystèmes « flexibles et coopératifs pour échanger des informations » liées à la cybersécurité.

Le CERT EDF connecté à des écosystèmes

Car la menace est bien réelle. L'énergéticien fait état d'une augmentation sur un an de 70 % du nombre de ses partenaires touchés par des attaques. La réponse passe donc par la création d'un « réseau de confiance ». EDF se dit prête à y contribuer. L'entreprise y participe même déjà, déclare Olivier Ligneul. Son CERT interagit avec différents écosystèmes, dont le Comité Stratégique de Filière (CFS) dont il dépend.

« Nous sommes tous dans le même bateau. Si un élément de la supply chain est touché, c'est toute la supply chain qui risque de tomber », insiste-t-il. Un partenaire du secteur victime d'une attaque peut donc bénéficier de l'aide du CERT EDF, en accompagnement après un incident ou pour la surveillance des évènements de sécurité.

Dans ce guide

Son responsable cybersécurité se défend toutefois de brosser un tableau totalement noir. Il assure ainsi que les progrès sont très significatifs au niveau de l'approche écosystème ; avec des actions communes et des projets à venir développés en coopération, afin de permettre d'autres avancées futures. Le RSSI se félicite aussi des efforts consentis par les fournisseurs de solutions industrielles en matière de vulnérabilités. « Ils ont amélioré leur gestion de la qualité », relève-t-il. C'est une avancée. D'autres sont encore nécessaires, comme le mentionnait le 13 octobre le DSI de la Stime (Les Mousquetaires), à l'occasion de l'assemblée générale du Cigref. Christophe Leray estimait ainsi que la lutte contre la cybercriminalité passait en particulier par des efforts accrus en faveur de « l'avènement de solutions numériques de confiance ». Là aussi, le DSI et vice-président du Cigref conditionnait ces progrès à une démarche collective. Le collectif est plus que jamais le mot d'ordre dans l'univers de la cybersécurité.

> **« Nous sommes tous dans le même bateau. Si un élément de la supply chain est touché, c'est toute la supply chain qui risque de tomber. »**
>
> **Olivier Ligneul**
> Directeur cybersécurité, EDF

Dans ce guide

Pour Parrot, la cybersécurité est un devoir et un atout concurrentiel

Le fabricant de drones Parrot adopte une approche security by design et privacy by design pour ses développements logiciels. Outre des audits, Parrot renforce la sécurité de ses produits via le recours à un programme de bug bounty.

Christophe Auffray, Journaliste

Bien connu dans l'univers des drones civils, le constructeur Parrot faisait son entrée en 2017 sur le marché du B2B. Les usages des drones se multiplient dans différents secteurs afin, par exemple, de mener des inspections critiques dans l'industrie. Mais les applications résident également dans des environnements sensibles, régaliens, dont le militaire.

Ces grands clients se montrent particulièrement sensibles à la sécurité des drones, dont celle des couches logicielles sur lesquelles les drones s'appuient. Pour Parrot, la cybersécurité est donc un enjeu de marché, y compris sur le grand public, souligne Victor Vuillard, le directeur sécurité et CTO Cybersecurity du constructeur.

Dans ce guide

La cybersécurité : un « marqueur » concurrentiel

« La cybersécurité est pour nous une priorité. Elle n'est pas vécue au sein de l'entreprise comme une contrainte, mais une force », assure-t-il. Cet engagement se justifie donc par un recours croissant aux drones pour des usages sensibles. Mais c'est aussi un « marqueur » vis-à-vis de la concurrence, et en particulier du leader chinois DJI.

Victor Vuillard, CSO, CTO Cybersecurity, Parrot.

Par le biais de rétro-ingénierie, Synacktiv identifiait chez ce dernier l'utilisation de mécanismes cryptographiques permettant de dissimuler certaines pratiques, comme des transferts de données vers des serveurs en Chine. En opposition, Parrot s'efforce donc de s'affirmer comme un fabricant de drones de confiance et un acteur affichant un haut niveau de sécurité. Un paramètre critique pour des clients comme la DGA (Direction générale de l'Armement) en France ou le DoD (Department of Defense) aux États-Unis.

Sur le plan de la transparence, l'industriel met ainsi en avant l'usage de protocoles standards et de briques open source ouverts, donc, à des

contrôles externes. Mais Parrot se soumet également à des audits tiers, à sa demande (via Bishop Fox aux États-Unis) et à celle de certains clients. Ces audits portent à la fois sur les WebServices et le logiciel de pilotage des drones.

Dans une logique de complémentarité avec les audits, Parrot décidait en avril dernier de la mise en place d'un bug bounty en partenariat avec YesWeHack. « La principale plus-value, c'est de permettre un audit par un plus grand nombre de chercheurs en sécurité, et potentiellement sur des éléments que nous n'aurions pas envisagé d'examiner », apprécie Victor Vuillard.

Précisons que le périmètre du Bug Bounty réalisé avec YesWeHack comporte quatre volets : le Web standard, avec le site Web et le site marchand ; les drones existants (logiciel du drone, l'application de pilotage et les WebServices) ; les drones en cours de conception et enfin les applications de sa filiale de conception de logiciels de modélisation Pix4D.

Le bug bounty complémentaire des audits

La première phase privée (ouverte à des chercheurs sélectionnés) des programmes de bug bounty a ainsi permis d'identifier « quelques » problèmes « d'une criticité notable » sur des composants hors du périmètre

habituel des audits. Il s'agit par exemple d'anciennes versions logicielles.
« Le chercheur en bug bounty va chercher tous azimuts. Et ces recherches conjointes par des dizaines de personnes produisent des résultats », précise encore le directeur sécurité.

Pour mener ces travaux, « la proximité et l'agilité » de YesWeHack, en comparaison de plateformes concurrentes comme HackerOne, avaient leur importance. Ces caractéristiques ont, par exemple, permis d'envoyer directement des prototypes de drones à des experts en sécurité triés sur le volet. « La flexibilité de YesWeHack a été primordiale. Ils nous ont accompagnés dans la définition du périmètre, dans le choix des chercheurs et dans l'identification de ceux disposant des bonnes compétences », tient à signaler Victor Vuillard.
Une première phase du bug bounty a été menée auprès de « dizaines de chercheurs ». Durant l'été et jusqu'à octobre sont venus s'ajouter « des lots de quelques dizaines de chercheurs » sur les différents programmes. Parrot réfléchit actuellement à l'ouverture en public du programme sur les drones existants. « C'est imminent à présent », confie le cadre du constructeur.

Ces audits de sécurité en crowdsourcing ont donc permis, à ce stade, « des remontées intéressantes », avec des « améliorations appréciables » à la clé. Aucune de significative, cependant, ne porte sur les drones. La gestion des remontées est traitée soit directement par les équipes, comme les

développeurs de Pix4D, qui ont accès aux rapports, ou par l'intermédiaire du directeur sécurité, qui procède à un tri des retours des chercheurs.

Sécurité corrective et aussi intégrée dans les développements

« Certaines équipes ont un degré d'expertise moindre en cybersécurité et ont besoin de plus d'accompagnement pour leur expliquer le principe de l'attaque et la manière de corriger. C'est notamment cette philosophie qui s'applique sur la partie Web », détaille Victor Vuillard.

Audit et bug bounty s'inscrivent cependant dans une approche réactive de la sécurité. Parrot embarque donc également la cybersécurité dans ses processus opérationnels. Cela se traduit par l'intégration de fonctionnalités de sécurité dans ses produits, comme le chiffrement des données du disque embarqué par le drone. C'est aussi, en matière de confidentialité, l'ajout en 2019 d'une

> **« La sécurité, c'est de la répétition, la base de toute pédagogie. C'est donner du sens aussi en expliquant, [...] pourquoi la sécurité est importante. Et enfin, la sécurité, c'est une vigilance quotidienne. »**
>
> **Victor Vuillard**
> CSO, CTO Cybersecurity, Parrot

Dans ce guide

fonction permettant aux clients de supprimer l'ensemble des données partagées avec Parrot.

Mais la sécurité doit aussi s'intégrer aux développements, « à tous les développements ». Pour cela, des opérations de sensibilisation ont été menées auprès des développeurs. Des outils et des processus interviennent aussi dans la sécurisation : analyse statique de code, revue du code à plusieurs (systématique pour toute mise à jour du firmware du drone), etc.

Au niveau de la supply chain, la sécurité peut également aller, en fonction des clients, jusqu'à exclure certains composants, notamment en provenance de Chine. Ce critère figurait parmi le cahier des charges du Département américain de la Défense dans le cadre de son programme Blue sUAS (small Unmanned Aircraft Systems). C'est d'ailleurs ce programme qui a donné naissance au micro-drone ANAFI USA, adopté par la suite par la DGA.

« La sécurité, c'est de la répétition, la base de toute pédagogie. C'est donner du sens aussi en expliquant, du PDG jusqu'au développeur, pourquoi la sécurité est importante. Et enfin, la sécurité, c'est une vigilance quotidienne », conclut le patron de la cybersécurité de Parrot.

Dans ce guide

Accéder à plus de contenu exclusif PRO+

Vous avez accès à cet e-Handbook en tant que membre via notre offre PRO+ : une collection de publications gratuites et offres spéciales rassemblées pour vous par nos partenaires et sur tout notre réseau de sites internet.

L'offre PRO+ est gratuite et réservée aux membres du réseau de sites internet TechTarget.

Profitez de tous les avantages liés à votre abonnement sur : https://www.lemagit.fr/eproducts

Images : Adobe Stock (Fotolia)

Dans ce guide

TechTarget | LEMAGIT

Le document consulté provient du site www.lemagit.fr

David Castaneira | *Editeur*
TechTarget
29 rue du Colisée, 75008 Paris
www.techtarget.com