DATALOCKER®
SIMPLY SECURE

LIVRE BLANC

Utilisation sécurisée de l'USB dans un environnement industriel

Ce document explore les risques de l'utilisation de l'USB dans un environnement industriel et présente une solution USB sécurisée à combiner avec une approche de sécurité multicouche afin de protéger les systèmes de contrôle industriels. L'objectif est d'améliorer la sécurité, la fiabilité et la disponibilité du système de contrôle et de se protéger contre les facteurs physiques, économiques et sociaux ainsi que les impacts associés aux défaillances de la sécurité industrielle.

Introduction aux problèmes de sécurité USB dans les systèmes de contrôle industriels

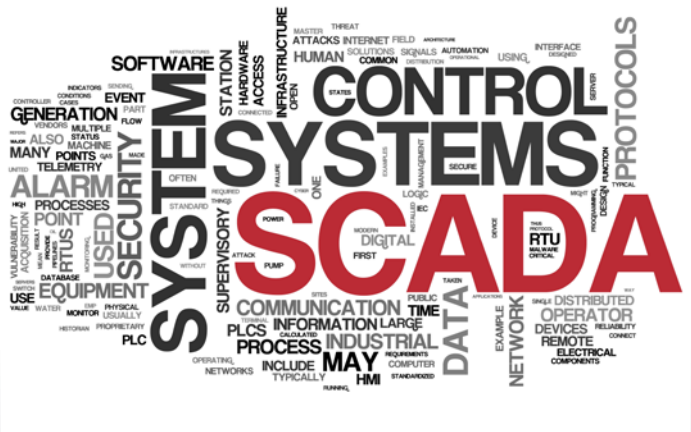
Un technicien en électricité et instrumentation lors d'un dépannage sur le contrôleur logique programmable du système de production de pétrole et de gaz sur une plateforme pétrolière offshore. Par pichitstocker - stock.adobe.com

Un malware que MIT Technology Review qualifie de malware le plus meurtrier au monde et qui est apparu pour la première fois dans le but de faire exploser une usine pétrochimique au Moyen-Orient, il se propagerait désormais en Amérique du Nord et dans le reste du monde. Cela se produit à un moment où plus de 2,5 millions de robots industriels sont employés dans des industries du monde entier allant de l'automobile, l'électricité / l'électronique, le métal / les machines, les plastiques / les produits chimiques à l'alimentation et aux boissons.[1] Tous les systèmes ne sont pas vulnérables à l'attaque spécifique, nommée Triton, mais partagent de nombreuses faiblesses communes. Ces machines et leurs systèmes de support sont généralement équipés de ports USB, une interface que nous connaissons tous et omniprésente sur nos ordinateurs de bureau.

Le port USB offre des possibilités de maintenance, de statistiques et bien plus encore, mais exige également que des procédures et des mesures soient mise en place afin de protéger les organisations qui les utilisent. Mais au-delà des attaques, les enjeux sont élevés, comme le montre cette citation des chercheurs en sécurité informatique[2] dans Wired concernant les conséquences d'une attaque via l'USB:

> *«Sabotage physique: modifier un bras robotique industriel peut coûter des millions d'euros en créant des produits défectueux et éventuellement endommager la machine voire blesser son opérateur.»*[3]

En plus parmi les industries qui utilisent des robots, il y en a beaucoup qui s'appuient également sur des réseaux de technologie opérationnelle (OT) et qui dépendent fortement du port USB. Les industries à forte intensité technologique opérationnelle sont : le pétrole et le gaz, l'électricité et les services publics, la fabrication de produits chimiques, le traitement de l'eau, la gestion des déchets, le transport, l'expérimentation scientifique, les commandes d'éclairage et l'automatisation des bâtiments. De nombreuses normes de sécurité et certifications telles que ISO 27001 exigent que cet espace entre les réseaux informatiques et les réseaux OT soit géré de manière contrôlée. Les réseaux OT contiennent des ICS (Industrial Control Systems) souvent structurés comme un SCADA (contrôle de surveillance et données Acquisition) système / réseau ou DCS (Distributed Control System). Les robots PLC (contrôleurs logiques programmables) et IIoT (Internet des objets industriels) peuvent avoir besoin de recevoir ou de soumettre des chargements de données via une interface de stockage USB.



Scada By MacX – stock.adobe.com

1 https://ifr.org/downloads/press2018/Executive%20Summary%20WR%202019%20Industrial%20Robots.pdf
2 https://robosec.org/downloads/paper-robosec-sp-2017.pdf
3 https://www.wired.com/2017/05/watch-hackers-sabotage-factory-robot-arm-afar/

Problèmes de sécurité USB

L'interface de stockage standard USB offre des contrôles de sécurité très limités. Un périphérique USB qui se présente selon la norme USB aura en général un accès complet aux parties du système, que ce soit un périphérique de stockage ou un clavier.[4] Cette confiance généralement accordée permet par exemple, l'essor des dispositifs OTP (One Time Pass) très utiles tels que le Yubikey qui injecte une chaîne d'authentification via USB via le HID (Human Interface Device). C'est la même confiance qui permet l'introduction d'attaques dénommées BadUSB ou USB Killers que nous allons maintenant explorer. Mais avant d'aller plus loin, identifions les possibles attaques par catégories.

«Un périphérique USB aura en général un accès complet aux parties du système hôte, ce qui représente une possibilité d'attaque.»

Matériel malveillant

Le principal coupable pour avoir brisé la confiance du protocole USB est ce que l'on appelle le BadUSB. Ces appareils sont en réalité des imposteurs. Ils se présentent comme étant des appareils de confiance mais ils sont en fait porteur d'une attaque malveillante qui se présente souvent sous la forme d'une injection de code dans le système. La figure emblématique pour ce type d'attaque est le RubberDucky produit par Hak5.[5] Même le Yubikey pourrait être modifié afin de pouvoir transporter une charge utile malveillante.[6] Ce ne sont bien évidemment pas les seuls coupables, car d'autres ont utilisé des plateformes informatiques telles que l'Arduino[7] ou Raspberry Pi[8] pour monter la même attaque. Il n'est nul besoin de grandes connaissances ni d'un budget colossal aujourd'hui pour lancer une attaque. Il existe même des packs prêts à l'emploi dont les prix commencent à partir de quelques dollars.

Les attaques électriques

L'absence de protection contre les surtensions introduit un problème de confiance supplémentaire pour les interfaces USB qui ont librement accès à une source électrique. Ce phénomène connu porte le nom d'USB Killer.[9] L'appareil utilise l'alimentation fournie par la machine hôte pour se charger puis il la détourne vers l'hôte via les broches d'alimentation du port USB. Ce qui provoque une surtension et souvent une panne électrique complète de l'hôte. L'USB Killer est dangereux car le robot s'éteint sans véritable trace apparente de ce qui s'est passé.

Logiciels malveillants de saut USB

Comment infectez-vous de manière malveillante un réseau hors ligne? Pour les auteurs encore inconnus du malware Stuxnet, la réponse est simple, faites du stop avec n'importe quelle clé USB que vous pouvez trouver et à force le malware trouvera sa cible. Cela peut prendre 10 sauts ou 1000 sauts. Silencieusement, le Stuxnet attend le bon moment pour arriver un jour dans un poste de travail d'ingénierie et atteindre éventuellement les automates programmables de l'installation d'enrichissement d'uranium de Natanz en Iran. L'attaque a détruit environ 1000 centrifugeuses.[10] Les attaques liées à la technologie Stuxnet ont engendré davantage de menaces spécifiques aux ICS,[11] utilisant une clé USB telle que Trisis.[12] Trisis, parfois appelée Triton ou Hatman, est capable de forcer un dysfonctionnement du système instrumenté de sécurité Triconex. (SIS), un contrôleur logique

4 https://www.usb.org/defined-class-codes
5 https://shop.hak5.org/products/usb-rubber-ducky-deluxe
6 https://www.blackhillsinfosec.com/how-to-weaponize-the-yubikey/
7 https://maltronics.com/collections/malduinos
8 https://hackaday.io/project/17598-diy-usb-rubber-ducky
9 https://usbkill.com/
10 https://www.cyberscoop.com/stuxnet-type-attack-airbus-cybersecurity/
11 https://www.msp360.com/resources/blog/triton-malware/
12 https://dragos.com/wp-content/uploads/Past-and-Future-of-Integrity-Based-ICS-Attacks.pdf

«La gestion de la sécurité dans un environnement ICS nécessite généralement une approche ... »

très connu fabriqué par Schneider Electric. Ces contrôleurs sont principalement utilisés pour gérer les équipements physiques des centrales nucléaires, des installations de production de pétrole et de gaz et des usines de papier.[13] Ces attaques peuvent avoir des conséquences extraordinaires et comme l'indique en 2019 le MIT Technology Review: «Le code non autorisé peut désactiver les systèmes de sécurité conçus pour prévenir les accidents industriels catastrophiques. Il a été découvert au Moyen-Orient, mais les pirates derrière cela ciblent désormais les entreprises d'Amérique du Nord et d'autres régions du monde. » Cela a incité MIT Technology Review à le nommer «le malware le plus meurtrier du monde». La raison en est une attaque très médiatisée que TechCrunch a résumée comme une tentative «de faire sauter une usine pétrochimique saoudienne».

La faiblesse PCL généralement utilisée dans ces attaques, provient du manque de vérification de la charge utile des périphériques par le biais de signatures cryptographiques acceptant ainsi plus ou moins ce qui leur est présenté à condition que le format soit correct.

Dans ce contexte, il convient également de noter que tous les ordinateurs de bureau des réseaux OT peuvent bien sûr être infectés par des attaques de logiciels malveillants plus standard. Un exemple est le ransomware Spora qui a été repéré au début 2020 et qui peut se propager à l'aide de clés USB génériques.[14]

Une solution USB de sécurité industrielle

La gestion de la sécurité dans un environnement ICS nécessite généralement une approche à plusieurs niveaux, comme le recommande le NIST dans le «Guide de Sécurité des Systèmes de Contrôle Industriels;[15] en précisant que les protections USB sont quelques éléments du puzzle de protection complexe. Pour ce qui est de l'utilisation des clés USB, l'ICS-CERT (Centre national d'intégration de la cybersécurité et des communications) a publié des directives spécifiques liées à l'utilisation des clés USB, et conseille aux utilisateurs d'établir des politiques strictes pour les réseaux d'entreprise et ICS.

Le format de ces politiques sera propre aux organisations, mais ils proposent des éléments qui peuvent être mis en place en fonction du scénario envisagé. La disposition physique des installations et des réseaux OT peut, comme nous le savons tous, différer considérablement d'une installation industrielle unique jusqu'au réseau étendu d'un opérateur de réseau électrique.

DataLocker met à votre disposition ses équipes professionnelles afin de vous conseiller sur les options de configuration spécifiques dans ce cas précis.

La solution générale proposée est composée des éléments suivants et répondra à ces critères de politique en:

1. Standardisant l'utilisation de périphériques USB fiables gérés et sécurisés pour le réseau OT
2. Établissant un périmètre strict autour du réseau OT lorsque cela est possible avec des données transitant par une station blanche (kiosque) qui est un type de dispositif de protection des limites
3. Installant un logiciel de contrôle de port USB sur tous les ordinateurs de bureau du réseau OT
4. S'assurant que les périphériques USB sécurisés peuvent être nettoyés entre les cycles d'utilisation ou selon un calendrier défini
5. Analysant tous les fichiers à la recherche de logiciels malveillants et vérification du hachage des charges de données du micrologiciel destinées aux systèmes qui ne peuvent pas vérifier eux-mêmes l'exactitude

13 https://www.cyberscoop.com/trisis-ics-malware-saudi-arabia/
14 https://blog.knowbe4.com/alert-usb-sticks-could-infect-your-network-with-new-spora-ransomware-worm
15 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

«En limitant l'accès au port USB, vous limitez la menace via des dispositifs USB.»

du chargement de données

Nous allons maintenant examiner de plus près chaque élément de la solution proposée.

Périphériques USB standardisés dans le réseau OT

Des contrôles de sécurité physique doivent être mis en place pour garantir que seuls certains périphériques USB fiables, gérés et sécurisés sont autorisés sur le réseau OT. Cette partie de la solution élimine la menace des attaques matérielles malveillantes et l'attaque principale des attaques électriques. Certains réseaux OT seront plus difficiles à contrôler en termes d'accès physique aux dispositifs, de sorte que la mesure a souvent besoin de soutien pour être pleinement efficace.

DataLocker Sentry K300

L'offre DataLocker

La DataLocker Sentry K300 s'est avérée très efficace surtout pour les réseaux OT. Le clavier peut à la fois être entièrement géré et audité lorsqu'il est connecté aux ordinateurs de bureau, mais la Sentry K300 s'utilise également en tant que support amovible pour des déblocages autonomes contrôlés. La capacité de déverrouillage autonome est cruciale pour permettre aux API et aux périphériques IoT de lire et d'écrire des charges de données. La Sentry K300 a également la capacité d'assainir les médias en utilisant l'effacement cryptographique, ceci est indispensable pour assurer la compartimentation dans certains réseaux. L'effacement cryptographique peut également faire partie d'une exigence réglementaire visant à garantir que les données sensibles sont détruites une fois la mission terminée.

Configurer les dispositifs de protection

Le but du dispositif de protection ou de la station blanche est de créer une passerelle entre le réseau informatique et l'OT qui garantira qu'un certain niveau de sécurité est atteint pour toutes les données transmises au réseau OT. La station blanche est le gardien et le seul appareil qui répond aux menaces extérieures. Il existe une multitude de façons de configurer une machine de bureau en fonction des besoins et pour qu'elle agisse telle une station blanche. En général, l'appareil doit avoir un moteur anti-malware à jour et un calendrier de maintenance élevé pour les mises à jour du système d'exploitation. Le matériel standard peut également par exemple être complété par un concentrateur USB protégé contre les décharges électrostatiques (ESD) qui protégera la machine de toute menace électrique USB. Il est également conseillé de n'autoriser qu'un seul clavier HID pour empêcher la majorité des menaces de type BadUSB.

L'offre DataLocker

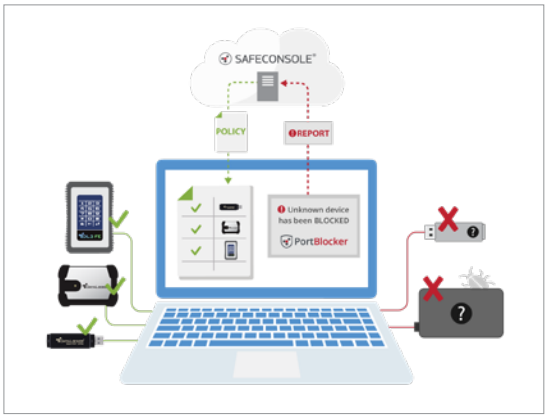
En combinant les technologies DataLocker, il est possible de créer une ou autant de stations blanches que les politiques l'exigent. La DataLocker Sentry K300 peut être configurée pour exécuter l'anti-malware McAfee intégré, ce qui garantit l'arrêt des programmes USB malveillants. Lors de l'utilisation du DataLocker Sentry K300, il est également possible de limiter les types de fichiers qui sont autorisés sur le réseau OT à l'aide d'une politique de restriction de fichiers. En combinant la Sentry K300 avec l'installation de PortBlocker, logiciel de contrôle de ports USB sur un bureau standard fermé, vous obtenez une protection supplémentaire.

«L'amélioration de la sécurité USB renforce la sécurité, la fiabilité et la disponibilité des systèmes de contrôle industriels.»

PortBlocker peut être configuré pour autoriser uniquement les opérations de lecture à partir de périphériques arrivant sur la machine de la station blanche.

Contrôler les ports USB autant que possible

Dans la mesure du possible il faut limiter l'accès aux ports USB sur les API et les périphériques informatiques qui ne peuvent pas être équipés d'un logiciel de contrôle de port, cela peut être réalisé avec des armoires verrouillées ou des prises de verrouillage USB physiques. Pour tout système d'exploitation standard, un logiciel de contrôle de port doit être installé. La logique derrière cette prévention des menaces est simple, en limitant l'accès au port vous limitez la menace que procurent les périphériques USB non approuvés.



DataLocker PortBlocker géré par SafeConsole

L'offre DataLocker

Le logiciel de contrôle de port, PortBlocker, doit être installé sur toutes les machines compatibles du réseau OT et du réseau informatique pour garantir que seuls les périphériques autorisés peuvent se connecter comme stockage de masse USB.

Nettoyage des données des périphériques de stockage

Une mesure raisonnable pour empêcher la propagation de logiciels malveillants est de s'assurer que les données des périphériques de stockage utilisés sont nettoyées régulièrement. Cela garantit des points de contrôle propres dans le mode opératoire et peut également faire partie de la conformité réglementaire pour pouvoir prouver que les données sensibles ne sont pas stockées indéfiniment sur des supports amovibles. Les clés USB ordinaires sont ce que l'on appelle des accumulateurs de données, elles sont conçues pour stocker sur le long terme des données. Ce qui signifie que le périphérique de stockage n'écrasera les secteurs de données que lorsque cela sera absolument nécessaire. Peu importe si la table d'allocation de fichiers (FAT) affiche un périphérique «propre». Cette «thésaurisation des données» a une conséquence malheureuse sur un périphérique USB ordinaire puisque cela expose une grande quantité de données alors qu'elles devraient ne plus exister.

L'offre DataLocker

DataLocker propose tout une gamme de périphériques chiffrés qui va résoudre le compliqué problème de l'assainissement en utilisant une méthode appelée l'effacement cryptographique. En bref il s'agit de détruire la clé de chiffrement actuellement utilisée pour déchiffrer les données stockées et d'en générer une nouvelle, ce processus garantit que votre média est propre et répond aux directives NIST 800-88 pour la désinfection des médias.[16] La plupart des territoires ont des normes similaires à celles du NIST et on peut généralement dire que l'effacement cryptographique complet est l'effacement le plus rapide et le plus efficace possible.

Anti-malware et vérification de chargement de données

Les stations blanches et tous les points de terminaison compatibles du réseau OT doivent

16 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

être équipés d'au moins une couche de protection anti-malware. La mesure combat en général les logiciels malveillants, mais plus particulièrement les logiciels malveillants qui utilisent l'USB comme mécanisme d'amorçage. De plus, les charges de données destinées aux automates ou aux machines qui ne peuvent pas valider les charges de données doivent être pré-vérifiées sur les stations blanches. Cette pré-vérification peut être réalisée en vérifiant les signatures cryptographiques ou les hachages fournis par l'éditeur du logiciel. Cette étape garantit que les données chargées sur les machines sont la copie exacte des données fournies par le développeur du logiciel.

L'offre DataLocker

Le Sentry K300 de DataLocker offre à la fois un anti-malware McAfee intégré et des restrictions de fichiers basées sur les types de fichiers. L'appareil permet à un administrateur de vérifier le hachage MD5 de toutes les données stockées sur le périphérique en s'assurant que seules les charges de données correctes atteignent les automates.

Analyse de rentabilisation pour une meilleure sécurité USB

Grâce à ce document il est démontré que l'amélioration de la sécurité USB renforce la sécurité, la fiabilité et la disponibilité des systèmes de contrôle industriels avec des étapes qui ne

Gestion opérationnelle à distance par batya - stock.adobe.com

sont pas invasives en termes de productivité. Cependant les conséquences dans un environnement industriel sont souvent plus dramatiques que dans un réseau informatique. L'environnement industriel est réel et signifie souvent que les vies, l'équipement et la production peuvent être affectés par des défaillances de sécurité. Nous avons démontré que les risques d'une utilisation USB non gérée peuvent être importants et ne doivent pas être délibérément négligés. L'analyse de rentabilisation exacte devra être ajustée en fonction du scénario en question. Les partenaires, services professionnels et l'équipe commerciale de DataLocker peuvent vous aider à travers des recommandations et des prix à construire votre analyse de rentabilisation avec précision pour arriver à une mise en œuvre de la sécurité opitimisée tout en maîtrisant les coûts.

DataLocker®
Simply Secure

+1-913-310-9088
+31 467 111 205
sales@datalocker.com

Pour trouver votre revendeur local DataLocker veuillez visiter **datalocker.com**

08/2020