

Au royaume des hackers, comment sécuriser une usine connectée ?

Par Erik Halthen, directeur des systèmes pour solutions industrielles, Analog Devices

À choisir, préférez-vous payer une rançon de 30 millions d'euros, ou transformer en profondeur la structure de votre entreprise ?

Imaginez que vous occupez le poste de DSI d'un fabricant. Votre chaîne de production tourne de façon parfaitement fluide quand soudain, les lumières s'éteignent. Les groupes électrogènes se mettent en marche et l'atelier est faiblement éclairé par les signalisations de secours. Que s'est-il passé ? Un appel du responsable informatique vous informe rapidement qu'un hacker a piraté votre usine et qu'il exige une rançon. Plusieurs activités de votre entreprise sont paralysées et vous devez prendre une décision relativement simple : verser la rançon, ou tenter de restaurer le système avec vos fichiers de sauvegarde. Vous optez pour la seconde solution, ce qui, au final, vous coûtera 30 millions d'euros en manque à gagner et immobilisation de votre outil de production.

Êtes-vous prêt à payer des centaines de milliers, voire des millions d'euros à des pirates informatiques pour récupérer vos fichiers ?

Selon l'étude publiée en janvier 2019 par Malwarebytes Labs sous le titre State of Malware, « *dans la seconde partie de l'année 2018, les créateurs de logiciels malveillants ont décidé de cibler les entreprises plutôt que les consommateurs, conscients qu'il était plus rentable de s'attaquer à des sociétés qu'à des particuliers. Dans l'ensemble, la détection de malwares par les entreprises a crû de manière significative au cours de l'année écoulée (+79 % pour être exact), et ce, principalement en raison de l'augmentation du nombre de portes dérobées (backdoors), logiciels de cryptominage (miners), logiciels espions (spyware) et autres applications de vol de données (infostealers).* »

Comment un tel scénario s'est-il produit ? L'ère numérique ouvre en permanence de nouvelles opportunités. Les chefs d'entreprise cherchent des possibilités d'innover, mais cette course à l'innovation n'est pas sans danger. Gérer les risques liés à la cybersécurité est l'un des défis majeurs qu'ils doivent relever, ce qui implique des transformations non conventionnelles de la structure de leur organisation. Ces changements sont indispensables pour influencer efficacement la culture de l'entreprise et favoriser la mise en place de processus opérationnels mieux adaptés à la complexité des systèmes et des cycles de vie.

L'adoption rapide de nouveaux systèmes intelligents installés en périphérie de réseau pour créer et interpréter les données est responsable de cette complexité croissante. Ces données revêtent de la valeur parce qu'elles sont utilisées à des fins décisionnelles ; plus les données sont précises et exactes, plus leur valeur sera élevée. Mais exploiter cette valeur n'est pas une chose aisée. Il est nécessaire de déployer une infrastructure capable d'accéder aux données et de les interpréter de manière opportune pour que les décisions soient prises dans un délai approprié. Cette exigence constitue le véritable moteur du monde connecté et, en matière d'automatisation industrielle, de l'usine connectée. Pour créer de la valeur en permettant d'accéder aux données et de les interpréter au moment opportun, les appareils doivent être interconnectés *via* un réseau distribué.

La tendance actuelle connue sous l'appellation « Industrie 4.0 » ouvre de nouvelles possibilités d'innovation à mesure que les systèmes de contrôle industriel gagnent en flexibilité, en précision et en efficacité. Pour que l'usine connectée apporte les résultats attendus, il est essentiel de s'attaquer aux risques de cyberattaques, et garantir la validité des données et des décisions qui en découlent. Étant donné que l'intérêt des cyberattaques continue d'augmenter proportionnellement à la valeur des actifs, maîtriser ce risque n'est pas chose aisée. Et compte tenu de la complexité inhérente à la cybersécurité et de la nécessité de gérer les risques de cybersécurité au niveau système, les chefs d'entreprise ont besoin d'être guidés.



Cet accompagnement s'appuie sur les nouvelles normes de sécurité publiées par des organismes de standardisation tels que l'International Society of Automation (ISA) ou, aux États-Unis, le National Institute of Standards and Technology (NIST). Si les normes appliquées peuvent varier en fonction des régions, leur contenu est relativement proche. Toutefois, ces documents ne représentent qu'une partie de la solution requise pour résoudre ce problème complexe. Certes, ils fournissent des instructions quant à la manière d'évaluer les risques et aux méthodes à utiliser pour se protéger. Mais pour réussir la mise en œuvre d'une usine connectée sécurisée, l'organisation doit être revue et transformée selon une approche « descendante » (*top-down*).

La mise en œuvre d'une usine connectée sécurisée doit s'appuyer sur une organisation capable à la fois d'interpréter les normes et de créer une infrastructure de sécurité. L'interprétation des normes de sécurité en vue de gérer les cyberrisques de façon appropriée implique certaines exigences en matière de sécurité. Dans un environnement où les menaces sont en constante évolution, il est nécessaire de développer une infrastructure de sécurité critique pour gérer les actifs d'un bout à l'autre du cycle de vie des produits. L'entrée dans la nouvelle ère de la connectivité débute par la mise en place d'une organisation qui pilote les processus métier du sommet jusqu'à la base. Cette approche *top-down* permettra aux équipes de développement de produits d'évaluer les compromis en matière de sécurité, puis de formuler des exigences de sécurité pour les produits en tenant compte de la complexité des systèmes et du cycle de vie.

Sécuriser l'usine connectée : un défi invisible

La sécurisation d'un environnement reposant sur des technologies opérationnelles (OT) d'une grande complexité soulève des défis qu'il est impossible de résoudre à l'aide de solutions basées sur les technologies de l'information (IT) classiques. Les systèmes OT fonctionnent dans des environnements où la valeur des actifs, les priorités et les contraintes en concurrence ne sont pas comparables à celles qui caractérisent l'environnement IT. Dans un environnement informatique, le respect de la confidentialité est primordial ; dans les usines au contraire, la priorité est généralement accordée à la disponibilité des données. De plus, la solution de sécurité sera déployée dans un système hébergeant des produits soumis à des contraintes élevées et où les cycles de vie s'étendent sur plus de 20 ans. Gérer les actifs, les priorités et les contraintes d'un environnement industriel requiert un ensemble unique de compétences et de processus pour élaborer les exigences de sécurité adaptées aux produits. Or, ces compétences et ces processus dépassent souvent les capacités des services informatiques traditionnels.



Figure 1. Processus de modélisation des menaces

La sécurisation d'un environnement OT représente une approche système qui nécessite d'identifier les actifs de grande valeur, d'évaluer les risques qu'ils encourent, et de faire les compromis de sécurité correspondant à son concept d'opérations (CONOPS). En raison des contraintes élevées qui caractérisent les environnements et de la spécificité des designs opérationnels, les risques liés à la sécurité ne seront pas tous traités au niveau des appareils. Une approche définie au niveau système aidera les experts à faire les compromis de sécurité appropriés. Il existe plusieurs façons de modéliser les menaces, mais les entreprises doivent adopter un processus pour tout nouveau développement.

L'objectif premier de la modélisation des menaces est de susciter une discussion concernant les compromis de sécurité dans le but de finaliser les exigences et les spécifications idoines. Pour ce faire, un concept d'opérations sera utilisé pour identifier les actifs critiques et décomposer le système. L'équipe pourra ensuite commencer à identifier les menaces et les vulnérabilités en s'appuyant sur les méthodologies existantes, établissant ainsi un modèle de menaces préliminaire. Ce modèle permet de définir des mesures de réduction des risques de sécurité et d'engager des discussions concernant les compromis qu'il convient de consentir. Étant donné que le concept d'opérations doit prendre en compte la conception du système de A à Z, il est essentiel de vérifier que tous les intervenants concernés prennent part aux discussions relatives aux compromis. À terme, toute menace de sécurité qui n'est pas prise en compte au niveau des composants devra être contrée à un niveau supérieur, ou acceptée comme un risque tolérable. L'adoption d'un processus standardisé pour favoriser l'engagement en faveur de la modélisation des menaces et de l'analyse des risques permettra de s'assurer que les exigences de sécurité ont été définies de façon appropriée.

La transformation organisationnelle, moteur de l'usine connectée

Les cybermenaces auxquelles sont exposés les environnements OT obligent les entreprises à élaborer une approche stratégique pour assurer le succès de l'usine connectée. Remédier à la complexité inhérente aux cybermenaces passe souvent par des changements organisationnels. La présence d'un expert en sécurité au sein d'une équipe Produit marque une avancée dans la bonne direction, mais c'est insuffisant pour qu'une entreprise bénéficie pleinement des avantages de la quatrième révolution industrielle. Dans cette optique, le changement doit intervenir aux plus hauts niveaux d'une entreprise disposant des moyens d'initier et d'appliquer un changement culturel qui s'étendra à l'ensemble de ses activités. En d'autres termes, cette organisation centralisée dédiée à la cybersécurité aura pour mission de déployer de nouveaux processus et de nouvelles procédures afin d'évaluer les cybermenaces, de répondre aux exigences de cybersécurité, de surveiller les incidents de cybersécurité et d'y faire face, ainsi que de procéder à l'évaluation et à la validation des produits.

La mise en œuvre d'un programme d'assurance de la sécurité des produits est essentielle pour faire face aux futurs risques de cybersécurité. Un tel programme permet de vérifier que les équipes de développement sont conscientes des risques de cybersécurité, des actifs majeurs qu'elles doivent protéger et des fonctionnalités de sécurité nécessaires pour améliorer les performances opérationnelles. Les personnes et les processus indispensables à la réussite de ce programme doivent être en place pour vérifier que la cybersécurité est prise en charge tout au long du cycle de vie des produits, mais également pour créer une infrastructure résiliente apte à réagir rapidement face aux nouvelles menaces et anomalies de cybersécurité.

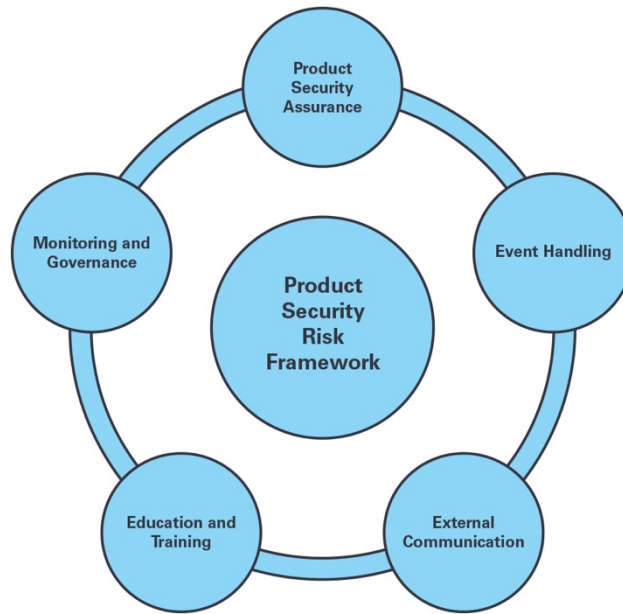


Figure 2. Cycle de gestion des risques liés à la sécurité des produits

Les entreprises devront répondre à de nouvelles exigences de cybersécurité en affichant une connaissance et une approche distillées dans la culture organisationnelle et guidées par des processus et des procédures standard. En ce qui concerne la gestion des risques de cybersécurité, l'aspect organisationnel représente la partie la plus complexe de la transition vers l'usine connectée. Toutes les entreprises devront relever ce défi, mais celles qui favorisent le changement culturel seront les mieux armées pour capitaliser sur les avantages de cette tendance incontournable de notre époque.

Analog Devices a réagi face à l'évolution de l'environnement de cybersécurité en créant un groupe de sécurité centralisé dont la mission est de promouvoir une culture de la sécurité d'un bout à l'autre de l'organisation. Le déploiement de processus de sécurité intégrés aux processus de développement de nouveaux produits marque une étape cruciale dans la mise en œuvre d'une culture de sécurité à tous les niveaux de l'entreprise. Cette solution permet de vérifier que tous les nouveaux produits sont évalués en fonction des besoins de sécurité, un responsable de la sécurité étant affecté au développement. Ce responsable s'assure que les exigences de sécurité protègent efficacement les actifs critiques tels qu'ils existent au sein d'un système entièrement intégré. La sécurité étant toujours une affaire de compromis, les implémentations de sécurité d'Analog Devices sont validées avec les clients en charge de la sécurité de l'usine connectée. Le fait de valider notre approche de la sécurité avec les représentants des clients garantit que les compromis sont adaptés à l'environnement opérationnel.

Dans le cadre d'une institutionnalisation de la culture de sécurité, Analog Devices prône la création d'une équipe d'intervention en cas d'incident de cybersécurité. Son rôle est d'évaluer les nouvelles menaces de sécurité, de réagir lors d'un incident de cybersécurité chez les clients, d'évaluer la conséquence sur les produits et de gérer la mise à jour de sécurité des produits. L'impact à long terme

sur la gestion d'un vaste portefeuille de produits peut être considérable. Une planification appropriée permet de promouvoir la durabilité et la gestion de nos solutions de sécurité dans l'ensemble de la gamme de produits. Alors que les intégrateurs de systèmes s'adressent à leurs fournisseurs pour relever des défis de sécurité particulièrement complexes et abaisser le coût total du cycle de vie, les critères de sélection de nouveaux produits aboutiront à la formation de solides partenariats pour gérer le coût total de l'usine connectée. Analog Devices s'engage à offrir la solution qui, à long terme, apportera une valeur maximale au design de systèmes novateurs.

Si vous devez choisir entre transformer en profondeur la structure de votre entreprise ou prendre un risque, la première option est préférable au versement d'une rançon, quelle qu'elle soit.

Références

Kujawa, Adam, Wendy Zamora, Jovi Umawing, Jérôme Segura, William Tsing, Pieter Arntz et Chris Boyd. [2019 State of Malware](#). Malwarebytes, janvier 2019.