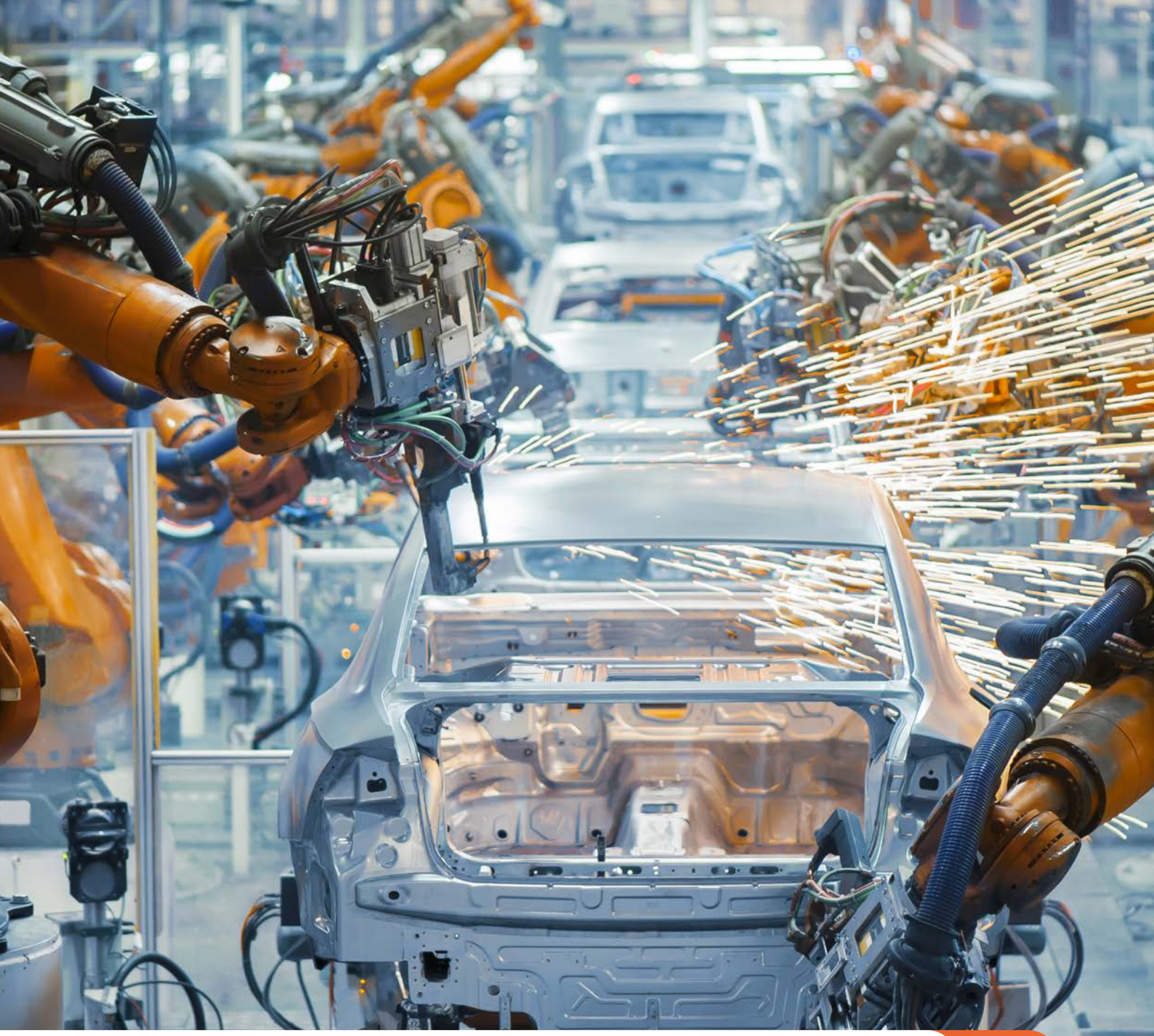


Rockwell Automation

La nouvelle intelligence de la fabrication automobile exige une cybersécurité proactive

Table des matières

Introduction

De l'adoption des automobiles autonomes aux opinions qui s'expriment en faveur des véhicules électriques, l'industrie automobile connaît les mutations les plus rapides et les plus disruptives de son histoire. Les leaders du secteur innovent afin d'améliorer l'agrément de conduite des voitures électriques ou hybrides, tandis que les moteurs à combustion internes sont repensés afin de réduire les émissions polluantes et de décupler les performances. Simultanément, les constructeurs automobiles ont une occasion unique d'introduire une nouvelle efficacité dans leurs opérations par plus d'automatisation, de numérique et de connectivité dans les ateliers.

Cette transformation numérique effrénée, de même que le côté très médiatique de l'industrie automobile, font de celle-ci une cible de plus en plus attrayante pour la cybercriminalité. Les acteurs malveillants connaissent pertinemment les coûts élevés des temps d'arrêt dans les usines automobiles et ils savent que ces coûts peuvent inciter les victimes de rançonlogiciels à payer des sommes importantes pour reprendre rapidement la production.

Les cybercriminels savent aussi que le parc installé d'équipements de production automobile, y compris les systèmes de commande (ICS) et les systèmes de gestion de la production (MES) ont tendance à avoir un long cycle de vie et que la gestion des vulnérabilités est un défi perpétuel pour les technologies de la production (OT).

Dans le monde actuel, les constructeurs automobiles font face à des cyberrisques majeurs et significatifs. Le paysage des menaces demeure problématique, avec des dommages annuels provoqués par la cybercriminalité estimés à plus de 10,5 billions de dollars d'ici 2025 et une croissance des coûts de 15 % chaque année.[1] Entre temps, les acteurs malveillants capables de la plus grande sophistication et les mieux financés, autrement dit ceux soutenus par des États, sont encore plus capables et audacieux. Les chercheurs estiment que la fréquence des cyberattaques « significatives » soutenues par des États a doublé entre 2017 et 2021[2] Au moins 53 % des fabricants dans l'industrie ont subi une violation de leur cybersécurité dans un de leurs établissements ces deux dernières années.[3]

[1] *Cybersecurity Ventures*, [2] *States, Cyberconflict and the Web of Profit*, [3] *LNS Research*

Les raisons de l'exposition des constructeurs automobiles aux cyberattaques

Les constructeurs automobiles sont une cible privilégiée des cybercriminels, en partie parce qu'ils ont de nombreux traits en commun avec d'autres fabricants, notamment des infrastructures existantes qui ne font souvent pas l'objet de correctifs et un manque de ressources qualifiées pour la gestion des risques. Des études récentes montrent que, parmi les 100 premiers constructeurs automobiles, 49 % sont « hautement susceptibles » de subir des attaques par rançonlogiciel. Des mots de passe victimes d'une fuite ou des informations d'identification subtilisées de 91 % de ces entreprises ont été retrouvés en vente sur le Dark Web. Par ailleurs, 79 % des constructeurs et des sous-traitants de rang 1 ont reçu de mauvaises notes pour leur gestion des correctifs et 90 % ont été classés comme « hautement susceptibles » de subir des attaques par hameçonnage.[4]

Les constructeurs automobiles sont aussi une cible de choix en raison des risques uniques propres au secteur. Les chaînes logistiques automobiles sont, par nature, complexes, car les OEM s'appuient sur des réseaux mondiaux de sous-traitants pour une multitude de pièces et composants, y compris les logiciels et composants électroniques. Dans la mesure où les véhicules actuels intègrent des nombres croissants de systèmes pilotés par des logiciels et connectés à Internet, la garantie de l'intégrité des chaînes logistiques est critique pour la sécurité fonctionnelle des véhicules et pour la protection de leurs occupants.

La sécurité pendant la transformation numérique rapide

La transformation numérique concerne l'ensemble du paysage industriel. L'automobile est l'un des secteurs qui avance le plus vite en la matière. Le passage des processus de fabrication automobile au numérique améliore la productivité, ainsi que la qualité et l'homogénéité des produits, et optimise les flux qui améliorent la sûreté et l'efficacité des usines. Le partage possible des données entre les systèmes informatiques (IT) et de production (OT) autorise des analyses qui améliorent les opérations et, au final, les résultats opérationnels pour les constructeurs automobiles.

Ces avancées peuvent aussi accroître les cyberrisques, en particulier lorsque les constructeurs automobiles n'ont pas élaboré un programme complet de cybersécurité industrielle pour leur entreprise. L'adoption d'une défense en profondeur calquée sur le cadre de cybersécurité du NIST ou « NIST Cybersecurity Framework » est essentielle pour sécuriser les réseaux et les dispositifs individuels, et ainsi pour défendre les systèmes contre des attaques extérieures.

Les constructeurs automobiles doivent aussi développer des capacités continues de détection et de réponse rapides, afin d'identifier les activités anormales et de bloquer les attaques avant qu'elles provoquent des temps d'arrêt importants ou des pertes financières ou matérielles conséquentes. Et ils doivent être en mesure de restaurer rapidement leur activité après des cyber-incidents. Cela exige une approche multicouches, qui fait appel aux personnes, processus et technologies appropriés, y compris des systèmes de commande à sécurité intrinsèque et des solutions de sécurité robustes conçues spécifiquement pour les environnements industriels.

[4] Black Kite

PRIORITÉ POUR L'AVENIR :

la sécurité des véhicules connectés est essentielle pour gagner la confiance des consommateurs d'aujourd'hui

Les véhicules connectés partagent des données avec des systèmes dans le cloud, des applications embarquées et d'autres systèmes, notamment l'infrastructure routière, d'autres véhicules, des appareils mobiles ou des services de télématique. Depuis l'introduction par GM du premier système d'appel d'urgence embarqué automatique en 1996, la connectivité des véhicules personnels a connu un développement phénoménal. **Selon des estimations, les véhicules connectés représenteront plus de 25 % du marché automobile mondial d'ici à la fin 2023 et plus de 75 % d'ici 2025.**[5]

Aujourd'hui, les véhicules à la pointe de la technologie intègrent des systèmes d'aide à la conduite avancés (ADAS), comportent plus de 150 calculateurs à microprocesseur (ECU) et plus de 150 millions lignes de code.[6] Deloitte estime que les systèmes électroniques à semi-conducteurs représentent pas moins de 40 % du coût d'une voiture neuve[7] et que le bon fonctionnement d'un logiciel est souvent déterminant pour les performances et l'efficacité d'un véhicule, d'où les préférences des consommateurs pour un modèle de voiture ou une marque spécifique.

Selon des estimations, les véhicules connectés représenteront plus de 25 % du marché automobile mondial d'ici à la fin 2023 et plus de 75 % d'ici 2025.

Les voitures sont désormais 'interactives de naissance'

De nombreux conducteurs attendent désormais de leurs voitures qu'elles fonctionnent avec des logiciels et se comportent comme des centres de données mobiles véloces. Ils accordent aussi une plus grande attention à la cybersécurité embarquée. Lorsque des chercheurs en sécurité ont démontré qu'ils pouvaient prendre à distance le contrôle d'une Jeep sur autoroute et pirater ses systèmes embarqués via Internet, l'incident a amené Chrysler à rappeler 1,4 million de véhicules. Cela a aussi attiré l'attention des grands médias.[8]

Au cours d'une autre démonstration de validation de principe, des pirates ont réussi à ouvrir les portes d'une voiture électrique populaire au moyen d'un drone emportant un dongle Wi-Fi, voire à accéder au service de commande-contrôle (C2) servant à communiquer avec toute la flotte de clients du constructeur.[9]

Plus que jamais, une cybersécurité rigoureuse des véhicules connectés est impérative si les marques automobiles souhaitent gagner et conserver la confiance des clients. Selon une étude récente, 80 % des acheteurs n'acquerraient jamais une voiture auprès d'un constructeur ayant déjà subi un piratage de véhicule.[10] Et une autre étude a montré que 84 % des consommateurs ne reviendraient pas acheter une nouvelle voiture chez le même concessionnaire s'ils découvraient que leurs données ont été compromises lors d'une intrusion.[11]

[5]Capgemini, [6]IEEE Future Directions, [7]Deloitte, [8]Wired,
[9]Electrek, [10]After Market News, [11]Total Dealer Compliance

Les plus grandes cybermenaces actuelles pour l'industrie automobile

La transformation numérique concerne l'ensemble du paysage industriel. L'automobile est l'un des secteurs qui avance le plus vite en la matière. Le passage des processus de fabrication automobile au numérique améliore la productivité, ainsi que la qualité et l'homogénéité des produits, et optimise les flux qui améliorent la sûreté et l'efficacité des usines. Le partage possible des données entre les systèmes informatiques (IT) et de production (OT) autorise des analyses qui améliorent les opérations et, au final, les résultats opérationnels pour les constructeurs automobiles.

Ces avancées peuvent aussi accroître les cyberrisques, en particulier lorsque les constructeurs automobiles n'ont pas élaboré un programme complet de cybersécurité industrielle pour leur entreprise. L'adoption d'une défense en profondeur calquée sur le cadre de cybersécurité du NIST ou « NIST Cybersecurity Framework » est essentielle pour sécuriser les réseaux et les dispositifs individuels, et ainsi pour défendre les systèmes contre des attaques extérieures.

Les constructeurs automobiles doivent aussi développer des capacités continues de détection et de réponse rapides, afin d'identifier les activités anormales et de bloquer les attaques avant qu'elles provoquent des temps d'arrêt importants ou des pertes financières ou matérielles conséquentes. Et ils doivent être en mesure de restaurer rapidement leur activité après des cyber-incidents. Cela exige une approche multicouches, qui fait appel aux personnes, processus et technologies appropriés, y compris des systèmes de commande à sécurité intrinsèque et des solutions de sécurité robustes conçues spécifiquement pour les environnements industriels.

Les cyberattaques fréquentes ciblant les constructeurs automobiles

Les trois scénarios d'attaques les plus courants aujourd'hui incluent les attaques par rançonlogiciel, l'hameçonnage (aboutissant au vol d'informations d'identification) et l'exploitation de vulnérabilités non corrigées dans les équipements d'atelier.

LA MENACE DES RANÇONLOGICIELS

Les attaques par rançonlogiciel sont le type de cybercrime qui augmente le plus rapidement à l'échelle mondiale, avec des dommages actuellement estimés à plus de 20 milliards de dollars. Les chercheurs estiment que désormais, toutes les 11 secondes, une entreprise est touchée par une attaque par rançonlogiciel.[12]

La fabrication figure parmi les secteurs les plus ciblés par les opérateurs de rançonlogiciels et le trafic réseau lié aux rançonlogiciels qui impact les entreprises industrielles est pratiquement le double de celui touchant le secteur suivant le plus ciblé.[13] Et, parmi les fabricants, les constructeurs automobiles constituent une cible particulièrement prisée car les coûts associés à un arrêt de la production sont très élevés. En fait, le phénomène qui incite très probablement les constructeurs automobiles à payer des rançons, à savoir l'intolérance aux temps d'arrêt, est le même qui les rend peu prompts à corriger les vulnérabilités.

Les attaques par rançonlogiciel commencent souvent par une tentative d'hameçonnage réussie. Les opérateurs de rançonlogiciels exploitent aussi fréquemment des ports critiques connus publiquement pour charger des logiciels malveillants dans l'environnement ou utilisent des informations d'identification subtilisées pour accéder à distance aux systèmes. Une **segmentation** appropriée des réseaux industriels et d'entreprise est essentielle pour empêcher la propagation du rançonlogiciel à partir du point initial de l'infection. Un isolement logique des zones démilitarisées industrielles (IDMZ) et des zones de sécurité critiques vis-à-vis des réseaux informatiques d'entreprise peut bloquer des tentatives de mouvement latéral à travers les environnements de production (OT), en cas d'accès obtenu au réseau informatique ou de production.

[12] *Cybersecurity Ventures*, [13] *Cisco*

DES ATTAQUES PAR HAMEÇONNAGE CIBLANT LES CONSTRUCTEURS AUTOMOBILES

Les attaques par courriel ciblant les constructeurs automobiles sont généralisées. Des chercheurs en menaces évaluant l'exposition de l'industrie automobile au risque d'hameçonnage ont découvert plus de 18 000 faux domaines ou domaines d'hameçonnage créés explicitement pour cibler les 100 plus grands constructeurs automobiles et OEM.[14] L'hameçonnage est une tactique hautement efficace employée par les cybercriminels car elle peut récupérer des privilèges internes concernant l'informatique ou des systèmes de commande, y compris des informations d'identification d'administrateur.

Dès qu'une tentative d'hameçonnage réussit, il peut être difficile pour les défenseurs de détecter les étapes suivantes de l'attaque, car les activités des acteurs malveillants ressembleront à celles d'une personne de l'entreprise. Leur capacité à provoquer des dommages immédiats sera limitée uniquement par leur connaissance du fonctionnement des systèmes d'usine et de la manipulation des composants de système de commande pour atteindre des objectifs spécifiques. La protection contre ces types de menaces exige des contrôles au niveau réseau, applications et dispositifs, ainsi qu'une surveillance constante de la sécurité IT/OT, afin de détecter rapidement des anomalies comportementales ou des tentatives de connexion inhabituelles.

Un programme complet **de formation de sensibilisation à la sécurité**, lequel apprend aux employés à identifier et éviter des tentatives d'hameçonnage, peut atténuer ces risques, au même titre que la mise en œuvre appropriée de politiques contrôlant les accès administratifs aux systèmes de fabrication et aux systèmes d'exploitation industriels. L'investissement dans l'éducation et la formation, afin d'actualiser les connaissances du personnel sur les menaces pour la sécurité et les meilleures pratiques, est aussi crucial.

VULNÉRABILITÉS DU PARC INSTALLÉ SANS CORRECTIFS

La gestion des correctifs du parc installé est très complexe pour les entreprises automobiles, mais celles qui ne parviennent pas à réduire les vulnérabilités au niveau des systèmes d'ateliers se retrouvent rapidement confrontées à un risque inacceptable.

Un rapport d'étude récent a montré que pas moins de 91 % des constructeurs automobiles comportaient au moins une vulnérabilité extrêmement grave dans leurs logiciels OT ou de systèmes de commande.[15] Certains étaient exposés à l'Internet public et de nombreux ne pouvaient pas être corrigés, car les fabricants ne fournissaient plus de mises à jour pour les matériels ayant dépassé leur fin de vie.

Il est essentiel de développer un processus efficace et parfaitement compris, capable de gérer les vulnérabilités du parc installé et de respecter les exigences en matière de correctifs. **L'identification et l'inventaire de tous les actifs réseau** dans l'ensemble de l'environnement OT, y compris les matériels, équipements, serveurs, capteurs et appareils mobiles, de même que la **surveillance continue des actifs** pour détecter des actifs ou utilisateurs non autorisés sur le réseau, constituent une étape vitale.

Des tests **de pénétration réguliers** sont aussi cruciaux. Des experts essaient de s'introduire sur les systèmes et peuvent fournir une véritable évaluation des points faibles et vulnérabilités, pour ensuite permettre leur correction.

[14] *Intsights*, [15] *Black Kite*

La nature de ce qu'il faut protéger évolue

Par le passé, il fallait protéger et défendre les réseaux informatiques des constructeurs automobiles, tout comme les API et systèmes de commande dans l'atelier.

Aujourd'hui, il faut sécuriser ces systèmes, mais aussi les écosystèmes IT/IoT/IIoT sans cesse plus complexes et interconnectés, tout comme les véhicules connectés qui s'appuient sur des logiciels. Cela amène les constructeurs automobiles à se poser tout un ensemble de nouvelles questions :

- Comment un constructeur peut-il corriger un logiciel dans un véhicule déjà en circulation ?
- Les constructeurs automobiles doivent-il construire de nouveaux centres des opérations de sécurité (SOC) juste pour être capables de surveiller le parc de véhicules qu'ils ont déjà produits ?
- À quels types de nouvelle supervision réglementaire l'industrie automobile sera-t-elle confrontée dans les années à venir ?
- Comment les constructeurs automobiles peuvent-ils acquérir une meilleure visibilité des pratiques de sécurité de leurs fournisseurs d'ECU tierce partie ?

Une approche robuste à bâtir pour la cybersécurité automobile

Alors que les constructeurs automobiles adoptent de plus en plus une connectivité de bout en bout au niveau de leurs installations de production et dans leurs écosystèmes informatiques d'entreprise, il devient progressivement nécessaire d'avoir une approche complète de la cybersécurité, afin de protéger les personnes, la propriété intellectuelle, la productivité et la continuité de l'activité.

Les réseaux OT sont intrinsèquement complexes. Il n'existe pas de solution miracle ou de correctif unique et simple, capable de garantir un environnement sécurisé en permanence.

Il est plutôt essentiel d'adopter une approche continue basée sur les risques, afin d'identifier les risques uniques de l'entreprise concernant les personnes, processus et technologies. Une évaluation claire des vulnérabilités et des risques associés peut aider les entreprises à allouer les ressources appropriées, à mettre en œuvre les politiques et procédures adaptées, et à déployer les technologies pertinentes.

Les constructeurs automobiles doivent commencer par comprendre la posture de sécurité de leur parc installé, en réalisant un inventaire complet des actifs et une évaluation tout aussi complète des risques.

Chronologie des attaques majeures ciblant des constructeurs automobiles

Mars 2019

Lors d'une attaque hautement ciblée, un groupe de cybercriminels spécialiste des menaces persistantes avancées (APT) a réussi à accéder à des serveurs contenant les données des clients et à impacter potentiellement pas moins de 3,1 millions de personnes.[16]

Décembre 2019

Selon des rapports, un groupe spécialiste des APT, appelé APT 32 (Ocean Lotus) et suspecté d'avoir des liens avec le gouvernement vietnamien, aurait infiltré les réseaux de deux grands constructeurs automobiles.[17]

Février 2020

Des chercheurs en sécurité ont trouvé 19 vulnérabilités dans des véhicules, lesquelles leur permettent de communiquer avec les serveurs back-end du constructeur automobile pour ouvrir les portes du véhicule et démarrer leur moteur à distance.[18]

Avril 2020

En réalisant l'ingénierie à rebours du boîtier télématique (TCU) d'un véhicule individuel, des chercheurs en sécurité ont réussi à utiliser la connexion de télématique pour infiltrer le réseau d'entreprise de l'OEM et bénéficier d'un accès avec des privilèges d'administrateur complets.[19]

Mai 2020

Il y a eu une fuite du code source de composants installés dans des vans d'un constructeur automobile, lorsque des référentiels Git contenant des images, du code, de la documentation détaillée et des environnements de développement pour les boîtiers logiques embarqués (OLU) des vans ont été rendus publics.[20]

Juin 2020

Une attaque par rançonlogiciel ciblant un constructeur automobile japonais a infecté les serveurs internes et a amené l'entreprise à suspendre la production dans des usines du monde entier.[21]

Août 2020

Un chercheur en sécurité a réussi, via une automobile, à prendre le contrôle de toute la flotte connectée de l'entreprise en exploitant une vulnérabilité de serveur sur le réseau de l'OEM.[22]

Août 2020

Une concession a été victime du groupe exploitant le rançonlogiciel Ryuk. Les attaquants ont dérobé des données de l'entreprise pendant l'incident et les ont publiées sur leur portail dédié aux fuites.[23]

Février 2021

Un constructeur automobile a subi une supposée attaque par le rançonlogiciel DoppelPaymer. Celle-ci a impacté ses systèmes internes et ceux au contact des clients, et à provoqué une paralysie étendue.[24]

Mai 2021

Une filiale d'un grand constructeur automobile spécialisée dans la fabrication de pièces a subi une attaque ciblée par rançonlogiciel. Des données financières et de clients ont été exfiltrées et exposées, tandis que la société mère de l'entreprise a été confrontée à des arrêts de la production dus à des problèmes de chaîne logistique.[25]

[16] CPO Magazine, [17] ZD Net, [18] Upstream, [19] Pen Test Partners, [20] ZDNet,
[21] Dark Reading, [22] Electrek, [23] TechNadu, [24] CPO Magazine, [25] The Register

Le cadre de cybersécurité du NIST

Le cadre de cybersécurité du NIST (National Institute of Standards and Technology) ou « NIST Cybersecurity Framework » fournit un ensemble de directives et meilleures pratiques qui ont été adoptées en tant que norme dans une multitude de secteurs. Le « NIST Cybersecurity Framework » propose des conseils sur la manière dont les entreprises peuvent gérer et atténuer les cyberrisques, et il inclut un ensemble de recommandations sur la prévention et la détection des événements de cybersécurité, ainsi que la réponse à ceux-ci, l'objectif étant de permettre une reprise rapide. Ce cadre est largement reconnu comme le socle de référence sur lequel une entreprise peut bâtir un programme de sécurité solide.

Le cadre inclut cinq fonctions clés : **Identifier, Protéger, Détecter, Répondre et Reprendre.** Ensemble, ces fonctions englobent le continuum complet d'une attaque et le cycle de vie de gestion de la sécurité. Les cinq fonctions structurent les domaines clés que les constructeurs automobiles doivent prendre en compte pour améliorer leur posture de sécurité globale, pour réduire le nombre de vulnérabilités exploitables et pour limiter au maximum les dommages pouvant résulter d'un cyber-incident ciblant les technologies de la production (OT).

Nous allons explorer ci-après chacun de ces domaines plus en détail, afin de fournir une feuille de route des étapes nécessaires pour élaborer une stratégie de sécurité du type « défense en profondeur » alignée sur le « NIST Cybersecurity Framework ».

IDENTIFIER

La première fonction du cadre de sécurité du NIST invite les entreprises à identifier les processus et actifs stratégiques, ainsi qu'à inventorier les systèmes et logiciels dans leurs environnements informatiques et de production. Cette étape permet de mieux appréhender les sources du cyberrisque en les associant aux systèmes, actifs, données et capacités. À partir de cette compréhension, une entreprise peut cibler et prioriser sa démarche de manière cohérente avec les objectifs de l'entreprise et la stratégie de gestion des risques.

Les environnements de fabrication d'aujourd'hui permettent de placer rapidement en ligne les dispositifs nouvellement connectés. Dans ce contexte, il peut devenir de plus en plus difficile pour les équipes de sécurité de comprendre quel matériel de production est mis en réseau. Il est quasiment impossible de protéger ce que vous ne pouvez pas voir.

La gestion d'un inventaire à jour et précis des actifs (avec les informations sur les spécificités du dispositif, notamment la connectivité et les risques ou vulnérabilités présents dans les actifs) est essentielle. Lorsque les équipes de sécurité savent ce qu'il y a sur le réseau, elles peuvent documenter les architectures de systèmes et les flux de données au moyen de représentations standard qui permettront aux équipes mondiales de comparer les topologies matérielles et les risques sur différents sites.

Un inventaire complet des actifs fournit une référence pour identifier les lacunes, puis pour concevoir et mettre en œuvre un programme de sécurité visant à les corriger. Après un inventaire initial des actifs, les constructeurs automobiles doivent planifier des évaluations de sécurité continues, afin de garantir la réalisation constante des objectifs de sécurité et le respect des normes sectorielles. Les inventaires d'actifs peuvent aussi mettre en lumière des actifs non autorisés ou utilisés à des fins non autorisées.

Les évaluations de sécurité sont aussi essentielles pour identifier des vulnérabilités logicielles (CVE). Elles fournissent un socle pour atténuer les vulnérabilités existantes dès maintenant, tout en permettant aux entreprises de mettre en place une approche proactive pour identifier et corriger des vulnérabilités futures.

PROTÉGER

La fonction Protéger inclut des activités qui améliorent la cyberhygiène et permettent une défense en profondeur. Elle propose un ensemble de protections qui réduisent le cyberrisque et protègent l'intégrité et la confidentialité des données à haute valeur, ainsi que la disponibilité des systèmes stratégiques. De telles protections incluent les contrôles de gestion des identités et des accès, la segmentation du réseau, CIP Security, l'architecture CPwE, les programmes de gestion des vulnérabilités, les solutions de sauvegarde, les formations de sensibilisation du personnel à la sécurité et les contrôles de configuration axés sur les dispositifs.

La segmentation du réseau est un aspect clé pour les constructeurs automobiles et d'autres fabricants dans l'industrie. Les réseaux de production (OT) existants ont tendance à avoir une conception « plate », mais des réseaux informatiques et de production mal segmentés permettent à des attaquants qui accèdent aux systèmes informatiques d'effectuer rapidement un mouvement latéral dans les environnements d'usine, afin potentiellement de diffuser un rançonlogiciel, d'accéder à des informations propriétaires ou de compromettre la production.

Un réseau bien conçu et une segmentation efficace des IDMZ et des zones de sécurité permettent aux équipes de sécurité d'isoler rapidement des systèmes impactés en cas d'attaque. Ainsi, la production peut continuer normalement ailleurs dans l'usine.

Les constructeurs qui déploient de nouvelles solutions automatisées ou connectées peuvent tirer avantage d'une architecture de référence validée, pour avoir l'assurance de concevoir un réseau paré pour l'avenir, lequel a été segmenté correctement et dont les performances, la disponibilité et la sécurité ont été testées. En utilisant une architecture constituée de conceptions validées auparavant, avec la documentation des meilleures pratiques et des paramètres de configuration, les entreprises peuvent mettre en œuvre un réseau de convergence IT/OT robuste, qui satisfait à toutes les exigences de performances, d'évolutivité et de sécurité.

DÉTECTER

Les activités dans le cadre de la fonction Détecter permettent aux équipes de cybersécurité d'identifier rapidement des comportements ou flux de données anormaux sur le réseau, lesquels peuvent être le signe d'une attaque. Ces activités incluent la collecte et la surveillance des journaux, ainsi que la surveillance constante de la sécurité logique et physique des environnements informatiques et de production. Un centre des opérations de sécurité (SOC) opérationnel 24 h/24, 7 jours/7 fournira les capacités requises d'alerte, d'enquêtes sur les événements et de réponse.

Des services tierce partie de détection des menaces peuvent fournir un accès à des technologies de détection des anomalies et intrusions. Leur utilisation permet aux défenseurs d'établir des références opérationnelles normales, et d'identifier et d'examiner des situations qui ne sont pas conformes à ces modèles escomptés.

Pour déterminer l'impact possible d'un événement de sécurité sur le fonctionnement d'une usine, il est vital d'avoir une documentation cohérente et complète de tous les systèmes d'usine, des réseaux OT et des dispositifs IoT/IIoT, y compris de ceux potentiellement non sécurisés. Dans de nombreux environnements de fabrication, une compréhension des architectures de systèmes OT, et des systèmes exposés aux réseaux externes, a été préservée sous forme de « savoir-faire spécifique » au sein du personnel de l'usine. Une documentation formelle permet une collaboration plus forte et plus productive entre les ingénieurs de l'usine et les équipes des opérations de sécurité.

RÉPONDRE

Lorsqu'un cyber-incident est détecté, les entreprises qui ont réalisé les activés liées à la fonction Répondre seront en mesure d'agir rapidement pour contenir l'incident et réduire son impact. La fonction Répondre intègre des capacités techniques, des processus et des flux de communication. Les entreprises doivent identifier proactivement les rôles et responsabilités des intervenants clés qui seront mobilisés en cas de cyber-incident touchant les technologies de la production.

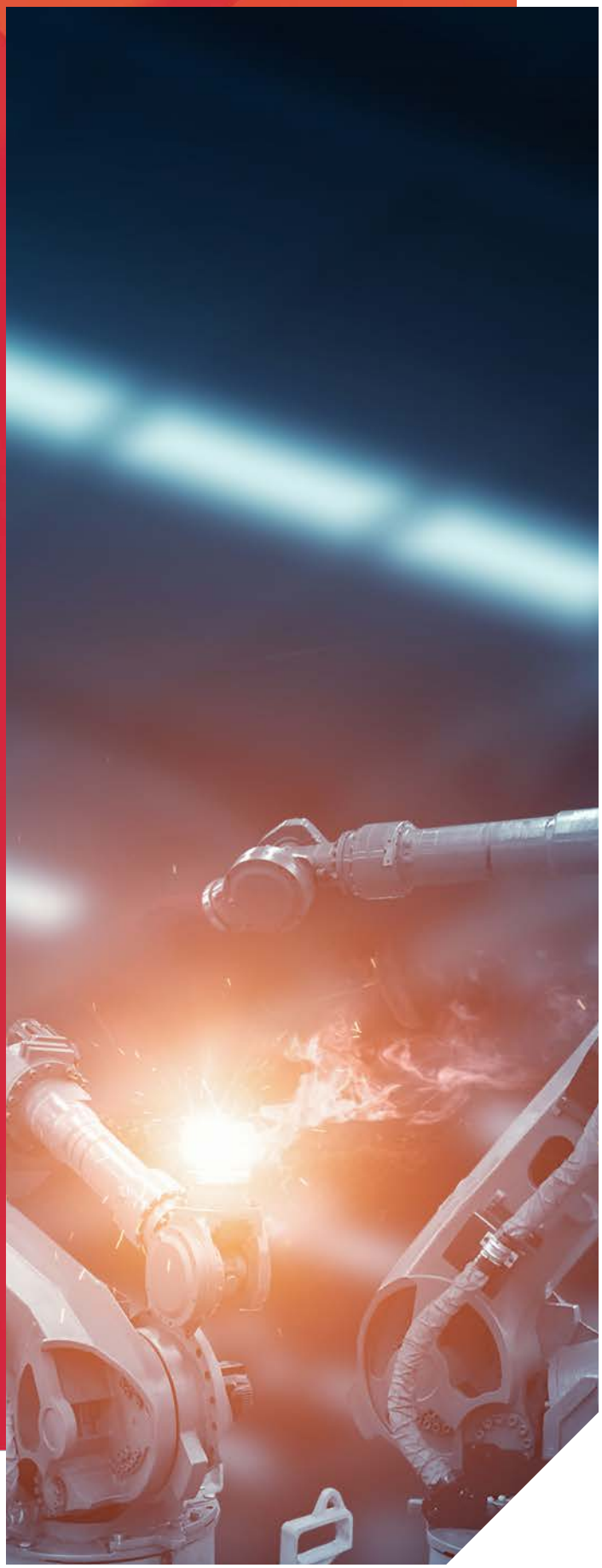
Les équipes du SOC et les ingénieurs d'usine devront se partager les responsabilités concernant l'enquête sur l'événement. Tout le personnel sur site et hors site saisira l'occasion d'exercices de simulation réguliers pour réviser les procédures en place et pour s'assurer qu'il est prêt à prendre des décisions rapides et précises en cas de crise.

REPRENDRE

La fonction Reprendre va au-delà des activités de réponse immédiate et à court terme. Les entreprises doivent élaborer des plans qui leur permettront de restaurer rapidement les capacités ou les services impactés par des cyber-incidents. Cela renforce la résilience et protège la continuité de l'activité.

Tous les fabricants dans l'industrie doivent non seulement gérer des sauvegardes complètes, mais aussi s'assurer qu'une restauration intégrale peut être réalisée dans un laps de temps suffisamment court pour éviter des conséquences graves pour l'activité. Des tests des capacités de sauvegarde sont essentiels, de même que des exercices de simulation réguliers, afin d'identifier et d'éliminer des lacunes dans la résilience des processus métier.

La récupération des systèmes de commande exige des compétences et capacités spécialisées. Non seulement les équipes de sécurité doivent effectuer l'analyse de la cyberattaque, évaluer les dommages et veiller à ce que tous les logiciels malveillants aient été éradiqués, mais elles doivent aussi remettre en service les variateurs et rétablir les processus d'API, afin que tout soit de nouveau opérationnel. Les équipes doivent être expérimentées dans le rétablissement rapide des processus.



Le concept central de l'approche zéro confiance est « ne jamais faire confiance, toujours vérifier ».

L'approche zéro confiance pour les constructeurs automobiles

L'approche zéro confiance concerne la sécurité des réseaux et a été présentée initialement il y a plus de dix ans par John Kindervag, du cabinet d'étude Forrester. Depuis, elle s'est répandue parmi les professionnels de la sécurité informatique, en grande partie parce qu'elle est parfaitement adaptée pour sécuriser les environnements informatiques modernes basés sur le cloud et compatibles avec les accès à distance. Aujourd'hui, elle commence à se généraliser aussi parmi les professionnels de la sécurité des technologies de la production.

Le concept central de l'approche zéro confiance est « ne jamais faire confiance, toujours vérifier ». Le postulat sous-jacent est qu'aucun utilisateur, aucune identité de machine, aucun flux de trafic ou aucune application ne doit bénéficier d'une confiance intrinsèque. Les identités et niveaux de risque doivent plutôt être vérifiés constamment et une politique continue doit être appliquée pour chaque connexion.

Dans un monde actuel où les attaques sont incessantes, l'adoption d'une approche zéro confiance atténuera les risques et abaissera les chances de succès de n'importe quelle attaque. L'approche zéro confiance peut procurer les bénéfices suivants aux constructeurs automobiles :

- Réduction de la taille de la surface d'attaque via des contrôles d'accès à granularité fine pour les actifs critiques.
- Réduction considérable du nombre d'intrusions malveillantes sur le réseau, par des exigences plus draconiennes en matière d'authentification et de validation des identités.
- Élimination de toute confiance excessive des conceptions d'architecture de réseau, afin de rendre la tâche des attaquants nettement plus difficile.

La conception optimale des stratégies zéro confiance actuelles passe par une autre méthodologie fournie par Kindervarg. Celle-ci se focalise sur l'identification des surfaces à protéger de l'entreprise, à savoir les données, actifs, applications et services (DAAS), qui sont les éléments les plus critiques des opérations, et sur leur protection avec des contrôles zéro confiance par ordre de priorité.

L'aide de Rockwell Automation

Rockwell Automation est le leader mondial de l'automatisation industrielle et cumule plus de 100 ans d'expérience dans la conception et la construction de systèmes de production (OT).

L'entreprise met à profit cette expertise poussée pour sécuriser les usines, actifs et réseaux critiques dans le monde entier. Au service de milliers de clients qui utilisent des services de commande et l'automatisation dans le monde, Rockwell Automation sait comment protéger les infrastructures, empêcher les temps d'arrêt et atténuer les dommages des cyberattaques. Rockwell Automation fournit des services de cybersécurité industrielle qui protègent les opérations de production sur lesquelles vous vous appuyez au quotidien, de l'atelier jusqu'au cloud.

Rockwell fournit des services gérés qui englobent les activités dans les cinq fonctions du « NIST Cybersecurity Framework », notamment des services d'identification des actifs, d'évaluation et de tests de pénétration, de surveillance et de correction des vulnérabilités, de conception et de mise en œuvre de programmes de sécurité, de détection des menaces et de sauvegarde, ainsi que de réponse aux incidents et de reprise.

Par ailleurs, Rockwell Automation propose, en complément, un ensemble exhaustif de services spécifiques aux projets, afin d'aider les clients à accélérer la maturité de leur sécurité OT. Rockwell Automation entretient aussi des partenariats étroits avec des leaders industriels dans l'informatique et la sécurité, notamment Cisco, Claroty, Microsoft, Dragos et Crowdstrike. Ils ont codéveloppé l'architecture CPwE (Converged Plantwide Ethernet) avec Cisco pour offrir aux clients un ensemble de plans d'architecture prévalidés et documentés, avec des conseils pratiques pour leur mise en œuvre et leur configuration.

La gamme de produits de Rockwell Automation inclut des solutions de commande industrielle à sécurité intrinsèque, ainsi que des technologies de sécurité créées spécialement pour ajouter des couches de protection supplémentaires aux produits de Rockwell. Ces solutions de sécurité spécifiques fournissent une protection périmétrique, la segmentation du réseau, des communications sécurisées entre les éléments de contrôle, ainsi que la protection des données pour les utilisateurs de leurs dispositifs.

Pour découvrir comment les constructeurs automobiles peuvent passer à l'étape suivante de la création d'installations de production cyberrésilientes, contactez dès aujourd'hui un expert Rockwell Automation.

Suivez-nous.

rockwellautomation.com — expanding **human possibility**®

AMÉRIQUES : Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 États-Unis, Tél. : +(1) 414.382.2000, Fax :+(1) 414.382.4444
EUROPE / MOYEN-ORIENT / AFRIQUE : Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgique, Tél. : +(32) 2 663 0600, Fax : +(32) 2 663 0640
ASIE PACIFIQUE : Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tél. : +(852) 2887 4788, Fax : +(852) 2508 1846
CANADA : Rockwell Automation, 3043 rue Joseph A. Bombardier, Laval, Québec, H7P 6C5, Tél: +1 (450) 781-5100, Fax: +1 (450) 781-5101, www.rockwellautomation.ca
FRANCE : Rockwell Automation SAS – 2, rue René Caudron, Bât. A, F-78960 Voisins-le-Bretonneux, Tél: +33 1 61 08 77 00, Fax : +33 1 30 44 03 09
SUISSE : Rockwell Automation AG, Av. des Baumettes 3, 1020 Renens, Tél: 021 631 32 32, Fax: 021 631 32 31, Customer Service Tél: 0848 000 278

Publication GMSN-BR004A-FR-P-Mai 2022