Rockwell Automation

COMPRENDRE LA CYBERSÉCURITÉ AUTOMOBILE :

les menaces courantes et la prévention proactive

Résumé

Les acteurs malveillants ciblent les constructeurs automobiles avec des cyberattaques réussies. De récents incidents très médiatisés indiquent que les cyberprotections actuelles dans l'industrie automobile ne sont clairement pas suffisamment robustes :

- Février 2021. Un grand constructeur sud-coréen subit une attaque par rançonlogiciel qui paralyse ses services de paiement, ses applications mobiles et les systèmes internes des concessions.
- Juin 2020. Un constructeur japonais de premier plan est victime d'une cyberattaque qui provoque des interruptions de la production dans des usines au Royaume-Uni, en Amérique du Nord et en Italie.
- Avril 2020. Une enquête réalisée par une publication automobile trouve des failles de sécurité majeures dans deux modèles d'automobile phares.

Les facteurs suivants contribuent à étendre la surface d'attaque chez les constructeurs automobiles :

- Augmentation des flux de données, des communications, de la connectivité et de l'intégration de l'infrastructure des technologies de la production (OT) et des technologies de l'information (IT).
- Manque de ressources qualifiées pour gérer les risques liés aux systèmes de commande, aux système d'acquisition et de contrôle des données (SCADA) et à d'autres systèmes OT.
- Visibilité médiocre du nombre et des types d'actifs connectés aux réseaux automobiles.
- La pandémie actuelle a mis les chaînes logistiques sous tension, d'où un risque et un coût encore plus élevés concernant les arrêts de fabrication, à un moment où l'inventaire est très réduit. Malheureusement, il est peu probable que cette situation se résorbe de si tôt.
- L'avènement de l'infrastructure pour les véhicules électriques est porteuse de nouvelles menaces pour les véhicules connectés, les bornes de recharge publiques, voire le réseau électrique. Et le manque de normes de sécurité pour la protection des bornes de recharge ne fait que compliquer davantage leur protection.

Les adversaires ciblent les vulnérabilités du parc d'actifs du réseau, y compris les machines et dispositifs dans les ateliers. Comme près de la moitié des actuels 100 premiers constructeurs automobiles sont considérés comme fortement susceptibles de subir des attaques par rançonlogiciel[1], une chose est claire : la gestion des risques dans l'industrie automobile demeure trop réactive pour faire face à la rapidité et à la sophistication croissantes des attaques.

[1] Black Kite

Coûts et conséquences

Les vulnérabilités exploitées par des acteurs malveillants peuvent avoir de multiples conséquences négatives sur les opérations, notamment des problèmes informatiques classiques tels que des violations des données, mais elles peuvent aller bien plus loin.

TEMPS D'ARRÊT DE PRODUCTION

Les temps d'arrêt non planifiés constituent l'un des risques majeurs pour les constructeurs automobiles en raison de leur coût très élevé au niveau de l'usine. Selon une estimation, une minute d'arrêt coûte 22 000 dollars et une heure, 1,3 million de dollars. Certaines estimations indiquent un coût de 50 000 dollars par minute.[2] Bien souvent, les cyberattaques provoquent des temps d'arrêt dans les environnements de production (OT). Les adversaires connaissent ces coûts très élevés des interruptions de la production de véhicules, ce qui fait de l'industrie automobile une cible privilégiée.

D'autres coûts, distincts de ceux liés aux temps d'arrêt, vont des dommages matériels et sur la production aux coûts de la réponse, de la résolution et de la reprise après la cyberattaque, lesquels sont généralement estimés entre 1 million à 13 millions de dollars ou plus par incident.

COMPROMISSIONS DE DONNÉES SENSIBLES

Le potentiel de compromission de données sensibles s'étend des technologies de l'information aux technologies de la production. Toutefois, les données confidentielles dans l'atelier se présentent sous une autre forme. Les secrets de fabrication, y compris les formules, techniques et logiciels, ou les données de machines et de recettes constituent une propriété intellectuelle de très haute valeur et des actifs d'entreprise hautement concurrentiels. Les constructeurs automobiles accordent une grande valeur à ces informations, car elles peuvent leur offrir un avantage concurrentiel en matière d'efficacité opérationnelle ou de caractéristiques de produits, en particulier dans le cadre de l'évolution vers les véhicules électriques et les bornes de recharge.

Les attaquants qui parviennent à infiltrer les environnements de production et de systèmes de commande peuvent compromettre et exfiltrer des informations vitales et/ou des données clients sensibles.

PÉNURIES AU NIVEAU DE LA CHAÎNE LOGISTIQUE

Les constructeurs automobiles ne sont pas les seules cibles des attaquants. Les risques s'étendent aux sous-traitants, lesquels fournissent aux constructeurs des composants critiques tels que les systèmes de climatisation et de chauffage. Des cyberattaques majeures contre des sous-traitants peuvent avoir un effet de domino pouvant provoquer des pénuries étendues au niveau de la chaîne logistique.

Les cybercriminels ciblent les vulnérabilités à tous les échelons de la chaîne logistique automobile. En octobre 2021, par exemple, le fournisseur allemand de pièces automobiles Eberspächer Group[3], qui exploite 50 usines, a subi une attaque par rançonlogiciel qui a crypté les données sur ses réseaux et serveurs dans le monde entier. L'entreprise a arrêté ses systèmes informatiques par mesure de précaution, mais a dû faire face à une interruption majeure. Elle a renvoyé les employés chez eux, en les rémunérant, et a subi d'autres pertes.

MENACES POUR LA SÛRETÉ PHYSIQUE

Les cyberattaques infiltrant les environnements de production automobile peuvent devenir des menaces potentielles pour la sûreté physique. Les logiciels malveillants, vers et virus peuvent saboter des dispositifs industriels tels que des automates programmables (API), et donner à des adversaires le contrôle de machines de la chaîne de montage. Des ajustements inattendus des processus de chaîne de montage ou du comportement d'équipements peuvent aussi présenter des menaces pour la sûreté du personnel des ateliers. Par ailleurs, des dommages intentionnels aux technologies de la production peuvent porter atteinte à l'intégrité des produits et mettre les clients en danger.

[2] TPC, [3] Eberspaecher

Acteurs malveillants et cyberattaques courantes dans l'automobile

Pour obtenir une vue complète du paysage de la cybersécurité automobile, il est important de mieux comprendre les acteurs malveillants qui ciblent les constructeurs automobiles, ainsi que les méthodes employées fréquemment au cours des attaques. Il est aussi important de noter que, même si la sophistication des attaques connaît une croissance exponentielle, la majorité des cyberattaques réussies exploitent des vulnérabilités bien connues, qui peuvent être corrigées avec les outils et les meilleures pratiques disponibles.

ACTEURS MALVEILLANTS

Les acteurs malveillants dans le domaine de la cybersécurité, notamment les gangs spécialisés dans les rançonlogiciels, cherchent à infiltrer les réseaux afin d'en tirer un profit pécunier. D'autres acteurs malveillants peuvent attaquer des entreprises automobiles avec l'intention de provoquer des dommages matériels ou de dérober une propriété intellectuelle de valeur, des informations d'identification personnelles ou d'autres informations précieuses.

Par ailleurs, l'industrie automobile fait partie du secteur de la fabrication critique, identifié par la CISA (Cybersecurity and Infrastructure Security Agency)[4] comme crucial pour la prospérité et la continuité de l'économie américaine.

La nature économique critique de la fabrication automobile expose les entreprises de ce secteur aussi à des cyberattaques étatiques. Afin d'essayer de favoriser leurs propres intérêts nationaux, certains pays peuvent louer les services d'acteurs malveillants, afin de collecter des renseignements ou de saboter des cibles industrielles clés.

Des chercheurs en sécurité découvrent aussi et publient des vulnérabilités concernant les postures de cybersécurité des entreprises automobiles. Suite à un incident récent[5], des chercheurs en sécurité ont analysé les systèmes informatiques d'un modèle phare d'un grand constructeur automobile américain et ont découvert un ensemble d'informations d'identification Wi-Fi d'une usine d'assemblage.

Même si les chercheurs ne cherchent généralement pas à exploiter les vulnérabilités à des fins malveillantes, ils peuvent découvrir des lacunes susceptibles de créer des cauchemars en termes de relations publiques et d'impacter la crédibilité auprès des clients.

Examinons maintenant les attaques courantes auxquelles les constructeurs automobiles et leurs sous-traitants sont confrontés fréquemment.

RANÇONGICIELS

Les rançonlogiciels sont un type d'attaque en plein essor et touchent tous les secteurs. Selon le Third Party Breach Report 2021 de Black Kite[6], les rançonlogiciels sont désormais la cause numéro un des violations de données tierce partie et ont représenté 27 % des attaques en 2021. 53 % des CISO ont déclaré avoir subi une attaque par rançonlogiciel au moins une fois l'an passé.

Dans ce type d'attaque, les adversaires infiltrent le réseau et délivrent une charge utile malveillante, qui crypte de multiples fichiers et dispositifs. De nombreux incidents avec rançonlogiciel incluent l'exfiltration et le cryptage de données. En effet, les acteurs malveillants pensent que l'extorsion a plus de chances de réussir s'ils peuvent menacer de publier des informations sensibles dérobées. À mesure que les frontières entre les technologies de l'information et celles de la production s'estompent, les attaques par rançonlogiciel peuvent entraîner des perturbations redoutées des ateliers de production.

[4] CISA, [5] Which.co, [6] Black Kite

ATTAQUES DES SYSTÈMES DE COMMANDE (ICS)

La connectivité intégrée et les communications de plus en plus ouvertes entre les dispositifs informatiques, de production et de l'Internet des objets (IoT) ont aussi élargi la surface d'attaque dans les environnements de systèmes de commande, exposant pour la première fois à Internet et aux applications de cloud des technologies souvent vieilles de plusieurs décennies. Les entreprises qui considèrent avoir une zone tampon suffisante découvrent souvent que c'est tout l'inverse.

Les attaques fréquentes incluent l'exploitation de protocoles de communications non sécurisés, des logiciels non corrigés, une sécurité IoT insuffisante, ou encore des logiciels malveillants utilisés contre la chaîne logistique et impactant les équipements de fabrication. Et les attaques de systèmes de commande sont en hausse, comme l'atteste la divulgation de 41 % de vulnérabilités d'ICS en plus[7] au premier semestre 2021 par rapport à la même période de 2020.

PIRATAGES DE VÉHICULES CONNECTÉS

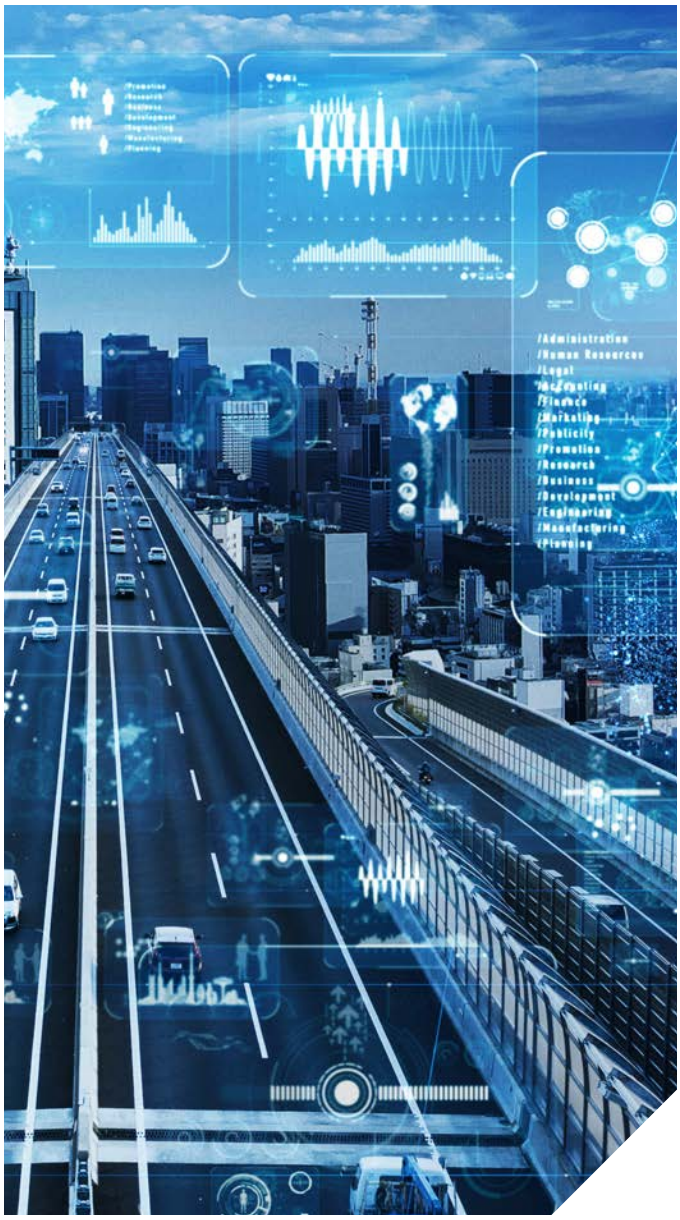
Les véhicules à moteur connectés modernes ont plusieurs systèmes informatiques embarqués, que les acteurs malveillants peuvent cibler à travers des attaques à distance et physiques. Aujourd'hui, les véhicules deviennent interactifs et connectés avant de quitter la chaîne de montage, et ils sont équipés de systèmes potentiellement exploitables.

- Le boîtier télématique ou TCU (Telematic Control Unit) peut faire l'objet de piratages. Dans le cadre d'un incident[8], des chercheurs ont retiré un boîtier télématique d'un véhicule, ont extrait sa carte SIM (Subscriber Identity Module) et, avec des informations d'identification d'administrateur, ont réussi à utiliser l'accès de la carte pour prendre le contrôle complet du réseau d'entreprise de l'équipementier (OEM).
- Le bus CAN (Controller Area Network) permet les communications entre différents microcontrôleurs et capteurs sur les véhicules à moteur. Des recherches[9] montrent qu'un bus CAN type est largement exposé à des attaques qui exploitent des vulnérabilités telles qu'un manque d'authentification ou de cryptage, d'où la possibilité d'une prise de contrôle du véhicule ou de violations de données sensibles.

APPLICATIONS MOBILES

Dans notre monde toujours plus mobile, de nombreux OEM proposent des applications mobiles qui permettent aux clients de se connecter à leurs véhicules. Certaines de ces applications permettent aux clients de localiser leur véhicule, d'ouvrir les portes et de démarrer le moteur. Les pirates peuvent exploiter les vulnérabilités du code applicatif, les modes de communication de l'application ou le mode de stockage utilisé par cette dernière pour les données.

Les répercussions d'attaques d'applications mobiles vont de la violation d'informations sensibles aux menaces potentielles pour la sûreté. En 2018, par exemple, un constructeur automobile[10] a exposé accidentellement les données personnelles de plus de 50 000 utilisateurs de l'application dans une zone non sécurisée de stockage dans le cloud.



[7] CPO Magazine, [8] Pen Test Partners, [9] University of Washington, [10] Bleeping Computer

Cybersécurité proactive dans la fabrication automobile

Les entreprises automobiles ont besoin d'une approche plus proactive face à l'avalanche de menaces auxquelles elles sont désormais confrontées. Nos recommandations couvrent les aspects critiques de la défense en profondeur et s'alignent sur le cadre de cybersécurité (CSF, Cybersecurity Framework) du NIST.

INVENTAIRE DES ACTIFS ET ÉVALUATION DES RISQUES

La sécurité proactive commence par le comblement des lacunes en matière de visibilité. Quels actifs d'atelier sont présents sur le réseau ? Quels logiciels sont utilisés dans les environnements de production (OT) et quels sont les risques particuliers associés à ces actifs et logiciels ? Les entreprises automobiles ne peuvent pas protéger ce dont elles n'ont pas connaissance.

Une évaluation des risques et un inventaire complets peuvent vous guider vers les correctifs les plus importants, avant que des acteurs malveillants exploitent une quelconque vulnérabilité flagrante. Les mesures initiales que vous pouvez adopter s'alignent avec la catégorie Identifier du NIST CSF. Cette catégorie vise à vous aider à cibler en premier lieu les protections concernant les vulnérabilités hautement prioritaires. L'objectif est de sécuriser d'abord les actifs d'entreprise à plus forte valeur, sur la base des menaces et risques identifiés pour votre entreprise.

GESTION DES CORRECTIFS

La gestion des correctifs dans les environnements de production est complexe car n'importe quel temps d'arrêt est coûteux et doit être évité. Par ailleurs, l'application de correctifs à des logiciels obsolètes requiert souvent la mise hors service d'une machine.

Dans la majorité des cas, un inventaire des actifs et une évaluation des risques permettront d'identifier de nombreux équipements d'atelier exécutant des systèmes d'exploitation obsolètes. Ces étapes identifieront aussi des actifs non autorisés dissimulés sur le réseau et exposant l'entreprise à des vulnérabilités critiques.

Une approche de sécurité proactive doit inclure la gestion méthodique des correctifs pour traiter les vulnérabilités en phase avec la fonction Protéger du NIST CSF. Les entreprises automobiles ont besoin de processus pour gérer les correctifs avec un minimum d'interruption opérationnelle. Certaines entreprises optent pour une approche du type « infrastructure en tant que service », laquelle simplifie considérablement l'application des correctifs et d'autres processus de gestion des opérations et de la cybersécurité.

Les équipes de sécurité doivent prendre en compte les facteurs suivants pour prioriser l'application des correctifs :

- Le risque potentiel pour les actifs si une vulnérabilité est exploitée.
- L'importance de tout équipement ou système vulnérable dans le processus de fabrication global.
- Les contributions de chaque correctif à la sécurité.

ZONAGE LOGIQUE DU RÉSEAU ET ARCHITECTURE CPWE

L'architecture réseau joue un rôle vital dans la sécurité des environnements informatiques et de production connectés. Les attaques peuvent se propager des machines individuelles aux switchs et à d'autres composants d'atelier vers le réseau informatique, et aussi dans le sens inverse, autrement dit des réseaux de production aux réseaux informatique. Cela conduit souvent à placer les systèmes de production hors ligne pendant les incidents de sécurité touchant l'informatique.

Dans l'exemple d'exploit précédent, à savoir une violation du TCU d'un véhicule, l'OEM n'avait pas de segmentation du réseau appropriée en place. Le zonage logique du réseau contribue à créer les stratégies de zonage appropriées pour une sécurité plus globale de l'usine et une protection des opérations contre un large éventail d'attaques.

Une architecture de référence éprouvée telle que l'architecture CPwE (Converged Plantwide Ethernet) fournit aussi un socle solide pour une segmentation appropriée du réseau, afin que les acteurs malveillants ne puissent pas exploiter des vulnérabilités et se déplacer entre les environnements informatiques et de production.

Souvent, les architectures OT émergent à partir de conceptions fonctionnelles et d'efficacité de la production, au lieu d'intégrer la sécurité dès le départ. Les systèmes OT sont conçus pour être déployés et fonctionner sans incident. L'attention se porte peu, ou pas du tout, sur les conséquences que peut avoir une décision concernant une conception particulière sur la sécurité du réseau.

Les constructeurs automobiles ont besoin de systèmes OT stables, disposant des mécanismes de cybersécurité appropriés pour leur protection. Alors même que le nombre et la gravité des attaques sont en hausse, il demeure important de maintenir un flux d'informations harmonieux et sécurisé pour maximiser les durées de fonctionnement fiables.

L'architecture CPwE utilise une zone démilitarisée industrielle (IDMZ) pour le partage sécurisé des informations entre les systèmes informatiques et de production, tout en protégeant les systèmes de production du trafic malveillant provenant des systèmes informatiques et d'Internet. Des pare-feux en première ligne et à l'arrière assurent une protection robuste et l'application des politiques de sécurité, par une inspection du trafic sur l'ensemble des réseaux.

DES MENACES FAISANT L'OBJET D'UNE DÉTECTION ET D'UNE RÉPONSE CONTINUES

La détection des menaces et la réponse à celles-ci fournissent des armes critiques dans l'arsenal de défense de toute entreprise.

Alors qu'une approche proactive de la cybersécurité automobile commence par des étapes de prévention qui améliorent la cyberrésilience, la mise en œuvre de contrôles de détection des menaces et de réponse aux incidents peut aider les entreprises à détecter rapidement des attaques, à répondre aux menaces, à éviter leur propagation et à rétablir les systèmes affectés plus rapidement en cas d'intrusion.

Les solutions de détection doivent identifier continuellement les signatures des menaces, notamment la présence d'équipements et d'une activité anormaux sur le réseau. Des références en matière d'activités normales des utilisateurs et de flux de trafic normaux peuvent être utiles lors de l'analyse et peuvent raccourcir les délais de détection d'incidents, en particulier sur les réseaux complexes à haut niveau de convergence IT/OT.

La détection des attaques en temps réel permet aussi une réponse rapide aux incidents, notamment la mise en quarantaine d'équipements ou la suppression des accès, afin d'éviter une escalade des dommages pour les constructeurs automobiles.

L'expertise de Rockwell Automation dans la cybersécurité pour l'industrie automobile

Les services de cybersécurité industrielle de Rockwell Automation protègent les processus de fabrication automobile sur lesquels vous et vos clients vous appuyez au quotidien. Notre approche proactive couvre l'intégralité du cycle de vie de la cybersécurité, de l'évaluation à la reprise, afin que votre entreprise soit parée avant, pendant et après une attaque.

Nous proposons une compréhension approfondie des opérations de production, laquelle repose sur plus de 100 ans au service de l'automatisation industrielle. En commençant par une évaluation des risques et un inventaire complets, nous pouvons vous aider à avoir une bonne visibilité de l'architecture en place, de l'infrastructure réseau et des vulnérabilités présentes dans votre environnement.

Notre expérience de l'architecture CPwE garantit une défense en profondeur globale, capable de bloquer la propagation des menaces de l'informatique à la production. Une solution de détection et de réponse de qualité industrielle, qui utilise un centre des opérations de sécurité (SOC) opérationnel 24 h/24, 7 jours/7, peut contribuer à stopper les attaques avant que les acteurs malveillants perturbent les opérations.

Pour découvrir plus avant comment les stratégies de sécurité automobile proactive peuvent vous protéger contre les cyberattaques, contactez-nous dès aujourd'hui.

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

Allen-Bradley et expanding human possibility sont des marques commerciales de Rockwell Automation, Inc.
Les marques commerciales n'appartenant pas à Rockwell Automation sont la propriété de leurs sociétés respectives.

Publication GMSN-WP004A-FR-P – Mai 2022

Copyright © 2022 Rockwell Automation, Inc. Tous droits réservés. Imprimé aux États-Unis.