Internet des objets industriels - Secteur automobile

Implémentation rapide, sécurisation lente

IBM Institute for Business Value

Dans ce rapport

IIoT du secteur automobile : risques de cybersécurité et progression de l'adoption

Trois domaines dans lesquels les entreprises les plus performantes se distinguent en matière de sécurisation de leurs environnements IIoT

Neufs pratiques de cybersécurité incontournables

Fonctionnalités IBM

Plus que de simples moyens de transport, nos voitures deviennent des centres de données mobiles d'un nouveau genre, alimentés par des capteurs et des ordinateurs de bord qui capturent des informations sur leur fonctionnement. Par le biais de ces données en temps réel, IBM donne les moyens aux responsables du secteur automobile de proposer de nouveaux services dont le consommateur connecté a besoin dans le cadre de son expérience de conduite. Notre force de fabrication associée à notre expertise poussée du secteur automobile garantit au consommateur un degré de sécurité et de qualité inégalé. En matière de fonctionnalités d'analyse, les technologies innovantes comme Watson peuvent répondre aux besoins des constructeurs OEM et des fournisseurs, notamment l'obtention de produits et des services plus sûrs et fiables, afin d'accroître la fidélisation et la satisfaction des clients.
Rendez-vous sur **ibm.com**/industries/automotive.

Le secteur automobile aspire à renforcer la cybersécurité

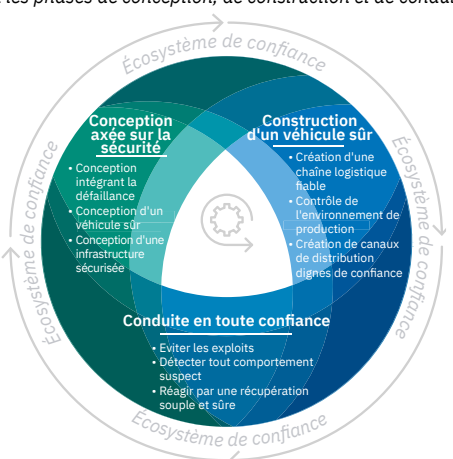
La sécurité des véhicules connectés et autonomes est en point de mire. Mais les entreprises doivent se concentrer sur les fondamentaux : les systèmes industriels utilisés pour la construction des voitures et leurs composants relevant de plus en plus de la haute technologie. La mise en ligne d'"objets industriels intelligents" sans une cybersécurité efficace peut mettre en danger toute une entreprise. Selon une étude de l'IBV (IBM Institute for Business Value), 87 % des constructeurs automobiles implémentent des technologies IIoT (Industrial Internet of Things) dans des usines et des chaînes de montage sans avoir évalué pleinement les risques, ni s'être préparés à réagir efficacement. Ils doivent disposer de fonctionnalités de cybersécurité améliorées à la fois contextuelles, cognitives et évolutives, afin de pouvoir identifier, atténuer et éviter en permanence les risques.

Insécurité générale

À mesure que les équipements et processus de fabrication deviennent plus intelligents et automatisés grâce à la mise en œuvre des technologies IIoT, les entreprises sont de plus en plus exposées aux cyberattaques. Qu'elles soient perpétrées par des pirates informatiques, des concurrents, des pays se livrant à l'espionnage industriel ou même des employés mécontents, les cyber-intrusions peuvent endommager considérablement l'équipement, entraîner la perte de données critiques et nuire à la réputation de l'entreprise, voire même causer des blessures ou des décès.

Dans l'étude de l'IBV "Accelerating security: Winning the race to vehicle integrity and data privacy", nous avons présenté l'approche de sécurité basée sur la conception, la construction et la conduite (voir la Figure 1).[1] La phase "Construction d'un véhicule sûr" de cette approche concerne l'exigence de contrôle de l'environnement de production.

Figure 1
Approche de la sécurité selon les phases de conception, de construction et de conduite



Source : Analyse de l'IBM Institute for Business Value.

87 %
des constructeurs automobiles interrogés déploient des technologies IIoT sans avoir évalué pleinement les risques

86 %
des constructeurs automobiles interrogés ne font pas d'évaluations régulières de la cybersécurité IIoT

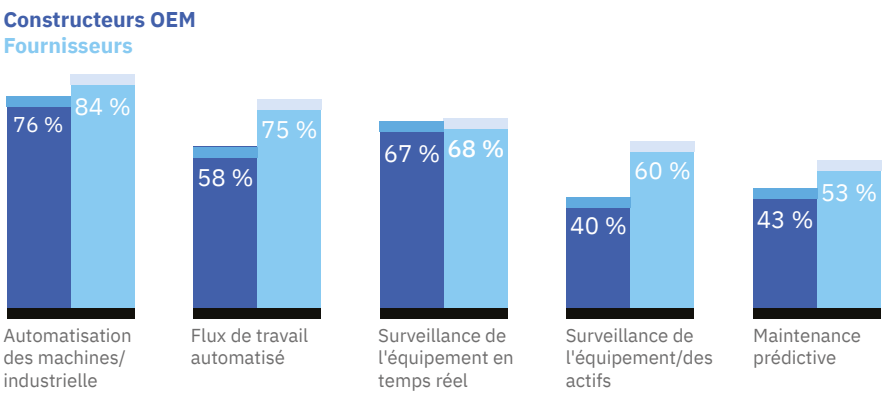
87 %
des constructeurs automobiles interrogés n'ont pas officiellement établi de programme de cybersécurité IIoT

Bien que les technologies IoT augmentent considérablement la productivité, elles offrent aussi un nouvel angle d'attaque et ouvrent une brèche de sécurité si la politique de sécurité n'est pas repensée. La vulnérabilité aux cyberattaques peut aussi bien concerner des actifs ou services à forte valeur ajoutée, des charges de travail critiques dans le cloud, des systèmes de contrôle de processus dans des systèmes cyber-physiques, ou encore des données métier et opérationnelles critiques.

Afin de mieux comprendre les risques et les implications en matière de sécurité de l'IIoT, l'IBV a interrogé 700 cadres en collaboration avec Oxford Economics. Ils représentent 700 entreprises de 18 pays des secteurs énergétiques et industriels (dont 135 du secteur automobile) qui implémentent l'IIoT dans leurs usines.

L'automatisation des machines/industrielle constitue la principale application de l'IIoT pour 76 % des constructeurs OEM et 84 % des fournisseurs (voir la Figure 2). Par ailleurs, 58 % des constructeurs OEM et 75 % des fournisseurs indiquent avoir automatisé les applications de flux de travaux. A noter que les applications de maintenance prédictive n'ont pas été aussi bien placées que l'on aurait pu s'y attendre.

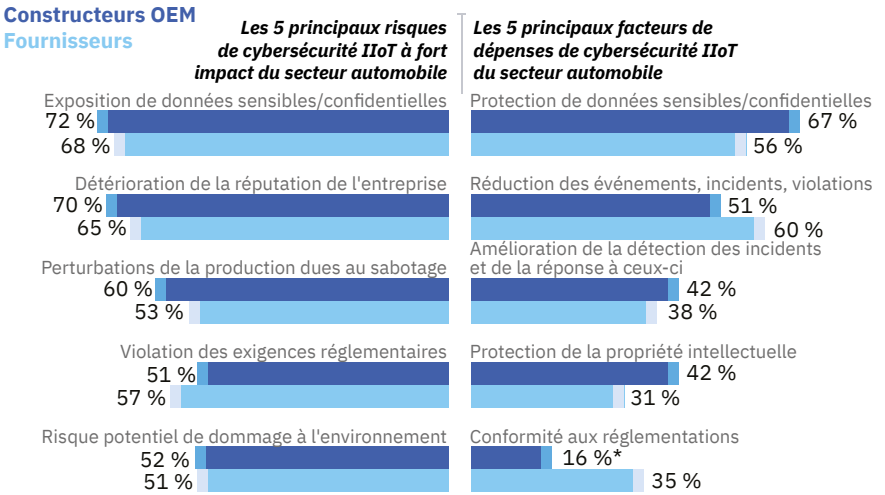
Figure 2
Les cinq principales applications des technologies IIoT dans les usines et chaînes de montage automobiles



n=135.

Les constructeurs automobiles semblent être conscients des risques de cybersécurité et ont, dans une certaine mesure, aligné en conséquence leurs dépenses d'IIoT (voir la Figure 3). Mais ils n'ont pas de vision claire de la combinaison de fonctionnalités de cybersécurité IIoT requises (compétences, contrôles, pratiques et technologies de protection) pour protéger leurs activités actuelles et futures contre les menaces IIoT.

Figure 3
Risques de cybersécurité IIoT comparés aux facteurs de dépense



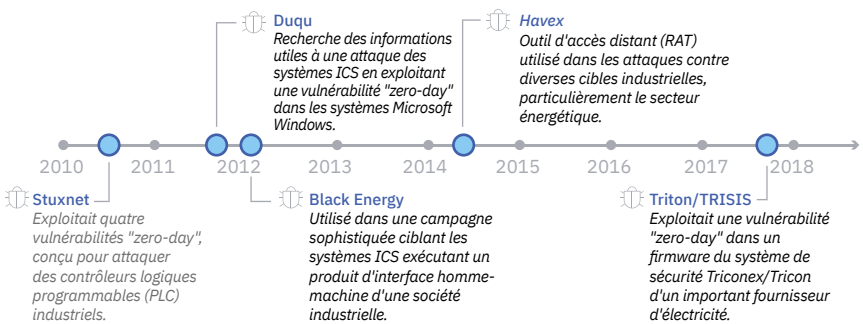
n=135.
**Les comptages n peu élevés (n<20) sont statistiquement non fiables, mais peuvent être considérés comme directionnels quand ils sont comparés aux autres répondants.*

Les constructeurs automobiles qui n'implémentent pas de mesures de protection appropriées, s'exposent à des risques importants, plus particulièrement :

1. *L'exposition de données sensibles/confidentielles*. Les responsables interrogés la considère comme le risque le plus important. 72 % des constructeurs OEM et 68 % des fournisseurs sont parfaitement conscients de l'impact sur leur croissance que pourrait avoir l'exposition des données, comme la propriété intellectuelle des clients et les conceptions techniques avancées.

2. *Détérioration de la réputation d'une entreprise et perte de confiance à son égard.* 70 % des constructeurs OEM et 65 % des fournisseurs considèrent qu'une violation de sécurité peut avoir un impact négatif important sur l'image et la réputation d'un constructeur automobile. La crédibilité d'une marque et la confiance que peuvent lui accorder les clients peuvent aisément être ébranlées, et induire une détérioration irrémédiable des relations métier et clients.
3. *Perturbations de la production résultant du sabotage*. Selon 60 % des constructeurs OEM et 53 % des fournisseurs, ce type de risque est important. Il peut même aboutir à la destruction d'équipement physique et à la production de pièces ou de véhicules défectueux. Les cyberattaquants peuvent accéder aux systèmes industriels d'une entreprise et manipuler l'infrastructure réseau (voir la Figure 4). Ils peuvent modifier les programmes logiciels des machines ou les systèmes de contrôle et d'acquisition de données (SCADA).

Figure 4
Attaques de systèmes de contrôle industriels (ICS) – Vue d'ensemble[2]



4. *Violation des exigences réglementaires*. Le Règlement général sur la protection des données (RGPD) entré en vigueur en mai 2018 et des lois similaires accroissent le risque et l'exposition réglementaires. 51 % des constructeurs OEM et 57 % des fournisseurs interrogés ont indiqué être très inquiets de l'impact potentiel de la non conformité avec les obligations réglementaires ; en effet, de telles infractions peuvent entraîner des amendes importantes.
5. *Risque potentiel de dommage à l'environnement.* 52 % des constructeurs OEM et 51 % des fournisseurs interrogés sont très préoccupés par le risque de rejet de matières dangereuses dans l'environnement en cas de violation de contrôles.

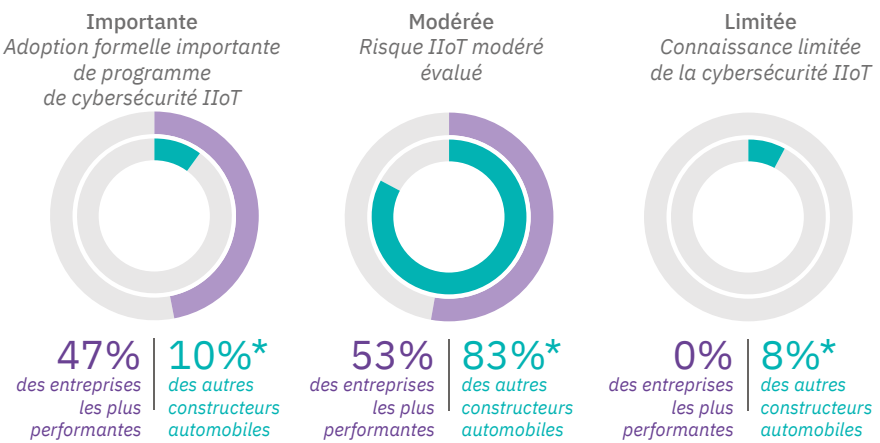
En matière d'investissement, la protection des données sensibles est prioritaire. Pour 67 % des constructeurs OEM et 56 % des fournisseurs, la majeure partie de leurs budgets de cybersécurité IIoT y est consacrée. Plus de 50 % des constructeurs OEM et des fournisseurs indiquent qu'il est hautement prioritaire de réduire les événements, les incidents et les violations.

Les entreprises les plus performantes sont en tête

Nous avons identifié les entreprises les plus performantes en matière de sécurisation de leurs environnements IIoT (voir l'encadré, “Les entreprises les plus performantes en chiffres”).

Si les entreprises les plus performantes ont encore du chemin à faire pour protéger véritablement ces environnements, elles savent beaucoup mieux identifier leurs besoins que leurs pairs. 47 % ont créé des programmes de cybersécurité formels pour établir, gérer et mettre à jour les outils, processus et compétences de cybersécurité IIoT requis, contre seulement 10 % des autres constructeurs automobiles (voir la Figure 5).

Figure 5
Connaissance de la cybersécurité IIoT et adoption de programmes de cybersécurité formels



Entreprises les plus performantes n=76; autres constructeurs automobiles n=115.
**Les comptages n peu élevés (n<20) sont statistiquement non fiables, mais peuvent être considérés comme directionnels quand ils sont comparés aux autres répondants.*
Remarque : Pour plus de détails, voir l'encadré.

Les entreprises les plus performantes en chiffres

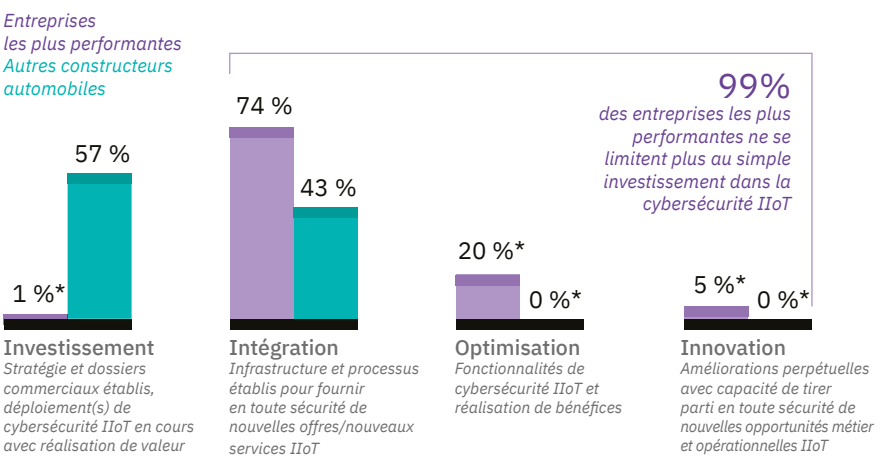
Les entreprises les plus performantes font partie des secteurs étudiés, notamment celui de l'automobile. Sur les 700 entreprises de l'enquête, 76 font partie de ce groupe, dont 20 sont issues du secteur de l'automobile. Ce groupe se situe dans le premier quartile des performances pour les trois indicateurs suivants :

1. Pourcentage de vulnérabilités IIoT connues traitées par des contrôles de sécurité.
2. Temps de cycle d'identification et de détection des incidents de cybersécurité IIoT. La durée d'exposition (délai entre une intrusion et sa découverte) n'est pas incluse.
3. Temps de cycle de réponse aux incidents de cybersécurité IIoT et de restauration.

Dans cette étude, les références aux “entreprises les plus performantes” concernent tous les secteurs étudiés, notamment les 20 entreprises du secteur de l'automobile. L'expression “autres constructeurs automobiles” correspond aux 115 autres constructeurs, à l'exclusion des 20 constructeurs les plus performants.

Les entreprises les plus performantes intègrent aussi beaucoup plus rapidement la cybersécurité IIoT dans leurs processus métier et opérationnels (voir la Figure 6). 20 % des entreprises les plus performantes ont optimisé les fonctionnalités de cybersécurité IIoT et en ont tiré des avantages, ce qui n'est le cas d'aucun des autres constructeurs automobiles. En outre, 5 % des premières se lancent dans des innovations selon leur intégration de la cybersécurité IIoT.

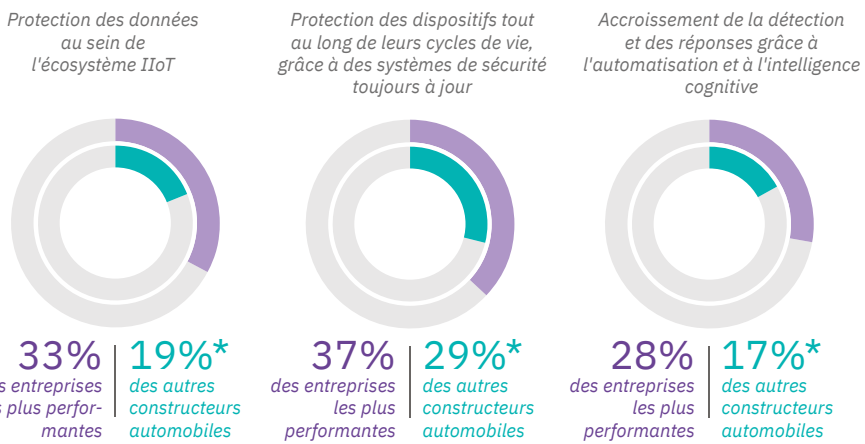
Figure 6
Niveau de maturité de l'intégration de la cybersécurité IIoT



Entreprises les plus performantes n=76; autres constructeurs automobiles n=115.
**Les comptages n peu élevés (n<20) sont statistiquement non fiables, mais peuvent être considérés comme directionnels quand ils sont comparés aux autres répondants.*

Les entreprises les plus performantes se distinguent dans trois domaines, en matière d'utilisation des solutions de cybersécurité pour protéger les données et les dispositifs, et des technologies automatisées et cognitives pour détecter les menaces de sécurité et y répondre (voir la Figure 7).

Figure 7
Les entreprises les plus performantes se distinguent



Entreprises les plus performantes n=76; autres constructeurs automobiles n=115.
**Les comptages n peu élevés (n<20) sont statistiquement non fiables, mais peuvent être considérés comme directionnels quand ils sont comparés aux autres répondants.*

Protection des données au sein de l'écosystème IIoT. De nombreuses données sensibles et relatives à la propriété intellectuelle sont partagées au niveau des chaînes logistiques automobiles. Si elles sont exposées ou volées, elles risquent de mettre en péril les activités futures d'une entreprise. Il n'est donc pas étonnant que 33 % des entreprises les plus performantes, (contre 19 % des autres constructeurs automobiles) aient pris de l'avance dans l'implémentation de solutions de cybersécurité spécifiques.

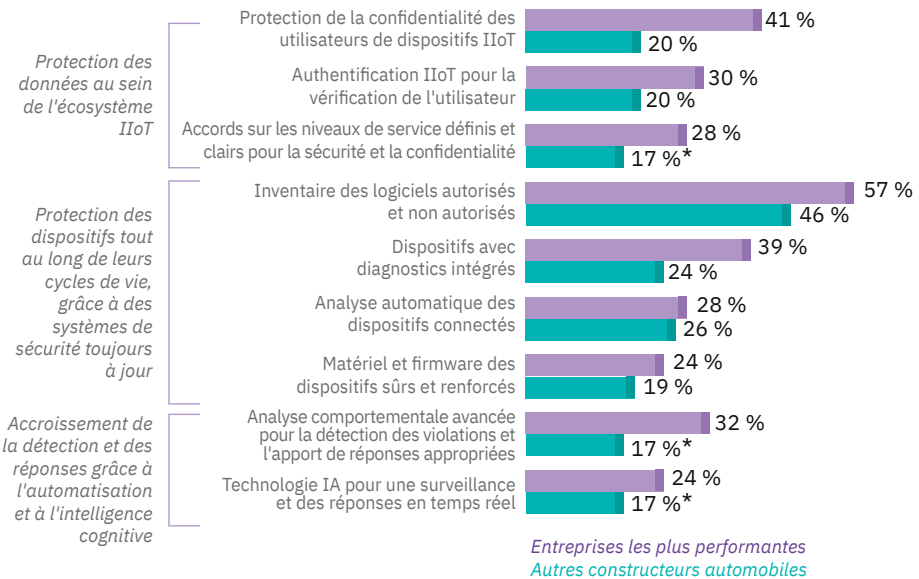
Protection des dispositifs IIoT tout au long de leurs cycles de vie, grâce à des systèmes de sécurité toujours à jour Des capteurs et dispositifs non protégés exposent les réseaux de technologies opérationnelles (OT)/IIoT à des cyberattaques pouvant avoir des conséquences physiques et financières catastrophiques. 37 % des entreprises les plus performantes sécurisent de façon adéquate leurs dispositifs IIoT, contre 29 % des autres constructeurs automobiles.

Accroissement de la détection et des réponses grâce à l'automatisation et à l'intelligence cognitive. La protection et la prévention ne permettent pas de régler tous les problèmes. Des systèmes doivent être mis en place afin de détecter les violations et d'atténuer les dommages. Les systèmes de détection classiques sont conçus pour gérer les attaques, les vecteurs de menaces et les vulnérabilités connus. Les fonctionnalités cognitives comme l'intelligence artificielle (AI), le machine learning et l'analyse comportementale avancée, permettent de gérer les "impondérables" pouvant émerger et être exploités à l'avenir. 28 % des entreprises les plus performantes ont pris de l'avance dans l'implémentation d'une combinaison de ces pratiques, ce qui n'est le cas que de 17 % des autres constructeurs automobiles.

Pratiques fondamentales

Les entreprises les plus performantes appliquent une approche de la sécurité basée sur le risque et la conformité, en s'axant sur 9 pratiques (voir Figure 8).

Figure 8
Les neuf pratiques de sécurité différenciatrices déployées par les entreprises les plus performantes



Entreprises les plus performantes n=76; autres constructeurs automobiles n=115.
**Les comptages n peu élevés (n<20) sont statistiquement non fiables, mais peuvent être considérés comme directionnels quand ils sont comparés aux autres répondants.*

Protection des données au sein de l'écosystème IIoT

L'exposition des données sensibles constitue un risque IIoT critique pour les constructeurs automobiles. Le principal type d'incident est la fuite de données. Il constitue plus d'un quart des incidents de cybersécurité IIoT dans le secteur (32 % pour les constructeurs OEM et 28 % pour les fournisseurs). Ces pratiques permettent :

1. *d'implémenter la protection de la confidentialité des utilisateurs de dispositifs IIoT*. Si des données d'utilisation peuvent être liées à un dispositif, des utilisateurs peuvent en déduire des éléments confidentiels relatifs à la production et aux processus d'une entreprise.[3] 41 % des entreprises les plus performantes, contre 20 % des autres constructeurs automobiles, ont implémenté des contrôles permettant aux utilisateurs de spécifier le mode de stockage des données sur leurs dispositifs et leur mode d'utilisation et de partage avec des tiers. Des stratégies similaires sont aussi importantes dans d'autres situations, comme le changement de propriété.[4]
2. *d'implémenter une authentification IIoT pour la vérification de l'utilisateur.* 30 % des entreprises les plus performantes, contre 20 % des autres, sont à un stade avancé d'adoption de cette pratique. La capacité d'authentification de l'identité d'un dispositif IIoT est essentielle, particulièrement pour les scénarios de communication de machine à machine (M2M) IIoT dans lesquels les dispositifs fonctionnent souvent sans intervention humaine.[5]
3. *de définir des accords de niveau de service clairs pour la sécurité et la confidentialité.* 28 % des entreprises les plus performantes contre 17 % des autres constructeurs automobiles surveillent et appliquent ainsi les exigences de sécurité. Pour combattre les attaques internes et éviter le vol ou la compromission d'informations, un accès contrôlé aux données doit être implémenté. Il est ainsi possible d'identifier qui s'est vu octroyer des droits d'accès à des fonctions ou des données sensibles. Les actions de ces utilisateurs privilégiés doivent être étroitement surveillées et auditées.

Protection des dispositifs tout au long de leurs cycles de vie, grâce à des systèmes de sécurité toujours à jour

Un peu plus d'un tiers des responsables du secteur de l'automobile indiquent que les dispositifs et les capteurs sont les éléments les plus vulnérables de leurs déploiements IIoT. Pour presque la moitié d'entre-eux, le principal obstacle à surmonter est de parvenir à appliquer des correctifs logiciels aux objets connectés. Les quatre pratiques de protection des dispositifs sont les suivantes :

1. *Inventaire des logiciels autorisés et non autorisés.* 57 % des entreprises les plus performantes, contre 46 % des autres constructeurs automobiles, y ont procédé activement. Il est crucial de contrôler les versions des logiciels pilotant les composants IIoT, d'étudier les menaces associées à la gestion des versions et d'établir des bases de référence sûres. Ces initiatives doivent être associées à une connaissance poussée des terminaux, à savoir leur rôle et avec quoi ils communiquent. Chaque terminal doit être profilé, ajouté à un inventaire d'actifs et surveillé.[6]
2. *Déploiement de dispositifs IIoT avec diagnostics intégrés.* 39 % des entreprises les plus performantes ont implémenté des dispositifs qui détectent les dysfonctionnements dûs à des composants défaillants ou à des tentatives de contrefaçon, contre 24 % des autres constructeurs automobiles. Les terminaux IIoT fonctionnent souvent dans des environnements hostiles sans intervention humaine sur de longues périodes. Si la sécurité et la protection de ces terminaux est primordiale, les possibilités d'ajout de fonctions de sécurité cryptographiques au matériel et aux logiciels sont souvent limitées.[7]

L'exposition des données sensibles constitue un risque IIoT critique pour les constructeurs automobiles.

3. *Automatisation de l'analyse des dispositifs connectés*. Il est crucial de procéder à l'évaluation et à la correction continues des vulnérabilités. Les entreprises les plus performantes et les autres constructeurs ont implémenté des stratégies relatives à l'analyse et à la correction à un degré à peu près identique. Il convient toutefois de noter que procéder à des analyses de vulnérabilités actives peut avoir des conséquences défavorables sur les communications réseau des systèmes de contrôle, puis sur la disponibilité des produits et des systèmes. Si l'analyse automatique n'est pas faisable, les entreprises doivent avoir recours à des outils de surveillance passive.[8]
4. *Déploiement de matériel et de firmware de dispositifs sûrs et renforcés.* Remplacer des dispositifs est souvent coûteux. D'autant que les nouveaux dispositifs ne bénéficient pas forcément d'une sécurité accrue. Les entreprises doivent procéder constamment à l'application de correctifs et de mises à jour, malgré les difficultés inhérentes à la mise à jour de dispositifs qui s'exécutent souvent 24h/24. Cela s'avère particulièrement important pour les dispositifs existants, car un grand nombre d'entre-eux n'ont pas été dotés d'un degré de sécurité adéquat.[9] Les responsables de toutes les entreprises étudiées sont conscients de ce problème et s'y consacrent à des degrés divers. Toutefois, les entreprises les plus performantes (24 %) sont légèrement en avance dans leurs implémentations par rapport aux autres constructeurs automobiles (19 %).

Accroissement des capacités de détection et de réponse

La protection et la prévention ne permettent pas de régler tous les problèmes. En outre, un système développé et déployé en toute sécurité ne garantit pas une protection absolue. Les attaquants recherchent constamment de nouveaux moyens d'infiltrer les systèmes ; des mécanismes automatiques doivent donc être mis en place pour détecter les violations et y remédier.

Les ressources de cybersécurité étant inévitablement limitées, les constructeurs automobiles doivent réduire la détection manuelle des menaces en implémentant des processus d'investigation faisant appel à l'IA et à l'automatisation (voir l'encadré "Atténuer les pertes par le biais de l'automatisation"). Les menaces peuvent être hiérarchisées au niveau du système afin de créer des alertes personnalisées, en définissant les données et les actifs sensibles, les segments réseau et les services cloud. Les deux pratiques d'adoption de la détection et de la correction des menaces IA sont les suivantes :

1. *Application de l'analyse comportementale avancée pour la détection des violations et l'apport de réponses appropriées*. 32 % des entreprises les plus performantes utilisent déjà une analyse du comportement des utilisateurs qui tire parti du machine learning, contre 17 % des autres constructeurs. La détection des menaces IA peut être appliquée au niveau d' une entreprise pour révéler des activités utilisateur anormales et hiérarchiser les risques. Les entreprises les plus performantes sont aussi en avance par rapport aux autres constructeurs automobiles en matière d'application du machine learning pour automatiser des modèles adaptatifs de ce qui est considéré comme normal. Cette approche permet de suivre ces modèles de comportement normal et de signaler des activités anormales pouvant indiquer de nouvelles menaces.
2. *Implémentation de technologie IA pour une surveillance de la sécurité et des réponses en temps réel.* Les entreprises les plus performantes sont légèrement en avance par rapport aux autres constructeurs automobiles dans ce domaine (24 % et 17 % respectivement). L'application de techniques pilotées par les données pour créer des flux en temps réel d'informations sur les menaces issues de sources externes et internes va permettre d'accroître encore davantage la vitesse de détection et de résolution.

Atténuer les pertes par le biais de l'automatisation[10]

Ponemon a récemment dévoilé que le coût moyen d'une violation de données pour les entreprises ayant totalement automatisé la sécurité de leurs systèmes est inférieur de 35 % à celui des entreprises qui n'ont pas mis en place d'automatisation.

L'automatisation de la sécurité consiste à faire appel à des technologies de sécurité qui supplémentent ou remplacent l'intervention humaine dans l'identification et le blocage des cyber-exploits ou des atteintes à la sécurité. De telles technologies reposent sur l'intelligence artificielle, le machine learning, l'analyse et l'orchestration.

L'IIoT requiert la convergence des technologies de l'information et des technologies opérationnelles. Or, il en résulte davantage de complexité et des risques particuliers. Il est crucial de sécuriser correctement les technologies IIoT. Dans le cas contraire, les bénéfices opérationnels et financiers immédiats qui y sont associés risquent d'être obtenus au détriment du futur de l'entreprise.

L'entreprise doit avoir une stratégie de sécurité IIoT claire. Elle doit aligner les pratiques de sécurité avec ses structures de risques étendues et intégrer les technologies de sécurité à des processus opérationnels. Elle doit être proactive, équilibrer prévention et détection. En outre, les fonctionnalités de sécurité doivent être "intelligentes" afin qu'elles puissent gérer les menaces avancées d'aujourd'hui et les menaces inconnues actuelles et à venir. Elle doit être préparée à récupérer rapidement en cas de violation, et disposer de plans de réponse et de communication avant qu'ils ne soient requis.

Êtes-vous prêt à hiérarchiser la cybersécurité ?

Quelle gestion du risque et de la conformité sont proposés dans votre programme de cybersécurité IIoT ?

Comment avez-vous intégré la cybersécurité IIoT dans vos processus métier et opérationnels ?

Comment vos employés ont-ils connaissance des opérations de cybersécurité IIoT ?

Quels types de simulations de violations de cybersécurité effectuez-vous pour préparer votre entreprise ?

Comment assurez-vous la visibilité des actifs les plus précieux de l'entreprise et des vulnérabilités pour effectuer une hiérarchisation intelligente et efficace du risque ?

Publications IBV connexes

Serio, Guiseppe et Ben Stanley. “Accelerating security: Winning the race to vehicle integrity and data privacy." IBM Institute for Business Value. Janvier 2017 https://www-935.ibm.com/services/us/gbs/thoughtleadership/acceleratesecurity/

Hahn, Tom, Marcel Kirsch et James Murrhine. “Internet of threats: Securing the Internet of Things for industrial and utility companies.” IBM Institute for Business Value. Mars 2018 https://www-935.ibm.com/services/us/gbs/thoughtleadership/iotthreats/

“Intelligent Connections – Reinventing enterprises with intelligent IoT.” Etude internationale sur les hauts dirigeants, 19ème édition. IBM Institute for Business Value. Janvier 2018 https://www.ibm.com/services/insights/c-suite-study/iot

Pour en savoir plus

Pour en savoir plus sur cette étude de l'IBM Institute for Business Value, écrivez-nous à l'adresse iibv@us.ibm.com. Suivez @IBMIBV sur Twitter. Pour obtenir un catalogue complet de nos recherches ou pour vous abonner à notre newsletter, rendez-vous sur : **ibm.com/**iibv.

Vous pouvez accéder aux rapports de synthèse de l'IBM Institute for Business Value sur votre dispositif mobile en téléchargeant les applis gratuites “IBM IBV” pour smartphone ou tablette depuis votre magasin d'applis.

Le partenaire idéal dans un environnement en pleine mutation

IBM collabore avec ses clients, en leur faisant bénéficier d'éclairages métier, de recherches et de technologies avancées afin qu'ils se différencient clairement dans l'environnement actuel en rapide mutation.

IBM Institute for Business Value

L'IBM Institute for Business Value (IBV), qui fait partie d'IBM Services, élabore des analyses stratégiques factuelles destinées aux cadres supérieurs sur des sujets sensibles des secteurs public et privé.

Rédacteurs

Giuseppe Serio est le responsable solution à l'international IBM pour la cybersécurité, dans les secteurs de l'automobile, de l'aérospatiale et de la défense. Il a plus de 20 ans d' expérience. Il discute avec des clients du monde entier à propos des programmes et des défis liés à la sécurité, notamment la sécurité des véhicules connectés. Il collabore avec d'autres départements IBM, comme la recherche et la sécurité, ainsi qu'avec les unités commerciales IoT, pour développer et adapter des solutions de sécurité visant à répondre aux besoins de secteurs spécifiques. Vous pouvez contacter Giuseppe par e-mail : giuseppe.serio@de.ibm.com et sur LinkedIn : linkedin.com/in/giuseppe-serio-183582

Ben Stanley est le responsable en recherche automobile pour l'IBM Institute for Business Value. Il est chargé du développement de contenu de leadership éclairé et d'éclairages métier stratégiques destinés aux solutions IBM pour le secteur automobile. Ben a plus de 40 ans d'expérience dans le secteur de l'automobile et a collaboré avec des clients majeurs de ce secteur dans le monde entier dans les domaines de la stratégie métier et de l'innovation concernant les modèles métier. Vous pouvez contacter Ben par e-mail : ben.stanley@us.ibm.com et sur LinkedIn : linkedin.com/in/benjamintstanley

Lisa-Giane Fisher est responsable Benchmarking pour l'IBM Institute for Business Value dans la zone Moyen-Orient et Afrique. Elle est chargée du benchmarking relatif aux garanties et à la sécurité IoT ; elle collabore en outre avec des experts sectoriels IBM et avec l'APQC (American Productivity & Quality Center) pour développer et maintenir des structures pour les processus sectoriels. Lisa a plus de 10 ans d'expérience dans le consulting et la gestion d'équipes multidisciplinaires pour l'implémentation de projets IT complexes intersectoriels. Vous pouvez contacter Lisa par e-mail : lfisher@za.ibm.com et sur LinkedIn : linkedin.com/in/lisa-giane-fisher

Notes et sources

1. Serio, Guiseppe et Ben Stanley. “Accelerating security: Winning the race to vehicle integrity and data privacy." IBM Institute for Business Value. Janvier 2017 https://www-935.ibm.com/services/us/gbs/thoughtleadership/acceleratesecurity/
2. “Attacks on Industrial Control Systems.” IBM Security. 2015. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEL03046USEN&attachment=SEL03046USEN.PDF; “TRISIS/TRITON.” New Jersey Cybersecurity & Communications Integration Cell. 14 décembre 2017. https:www.cyber.nj.gov/threat-profiles/ics-malware-variants/triton
3. Hahn, Tim et JR Rao. “IoT Security: An IBM Position Paper.” Watson IoT. IBM. Octobre 2016. https://www.ibm.com/internet-of-things/spotlight/iot-security. Pour accéder directement à ce document, accédez à https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WWW12379USEN
4. Maxim, Merritt. “TechRadar™: Internet Of Things Security, Q1 2017.” Forrester. 19 janvier 2017. https://www.forrester.com/report/TechRadar+Internet+Of+Things+Security+Q1+2017/-/E-RES117394
5. Ibid.
6. Hahn, Tom, Marcel Kirsch et James Murrhine. “Internet of threats: Securing the Internet of Things for industrial and utility companies.” IBM Institute for Business Value. Mars 2018 https://www-935.ibm.com/services/us/gbs/thoughtleadership/iotthreats/

7. Hahn, Tim et JR Rao. “IoT Security: An IBM Position Paper.” Watson IoT. IBM. Octobre 2016. https://www.ibm.com/internet-of-things/spotlight/iot-security. Pour accéder directement à ce document, accédez à https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WWW12379USEN
8. “CIS Controls Version 7 Implementation Guide for Industrial Control Systems.” Center for Internet Security. 2018. https://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial-control-systems/
9. Grau, Alan. “What's the Difference Between Device Hardening and Security Appliances?” Electronic Design. Jeudi 3 août 2017. https://www.electronicdesign.com/industrial-automation/what-s-difference-between-device-hardening-and-security-appliances
10. “2018 Cost of a Data Breach Study: Global Overview.” Etude de référence financée par IBM Security. Menée de façon indépendante par Ponemon Institute LLC. Juillet 2018. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produit aux États-Unis d'Amérique
Septembre 2018

93018893FRFR-03