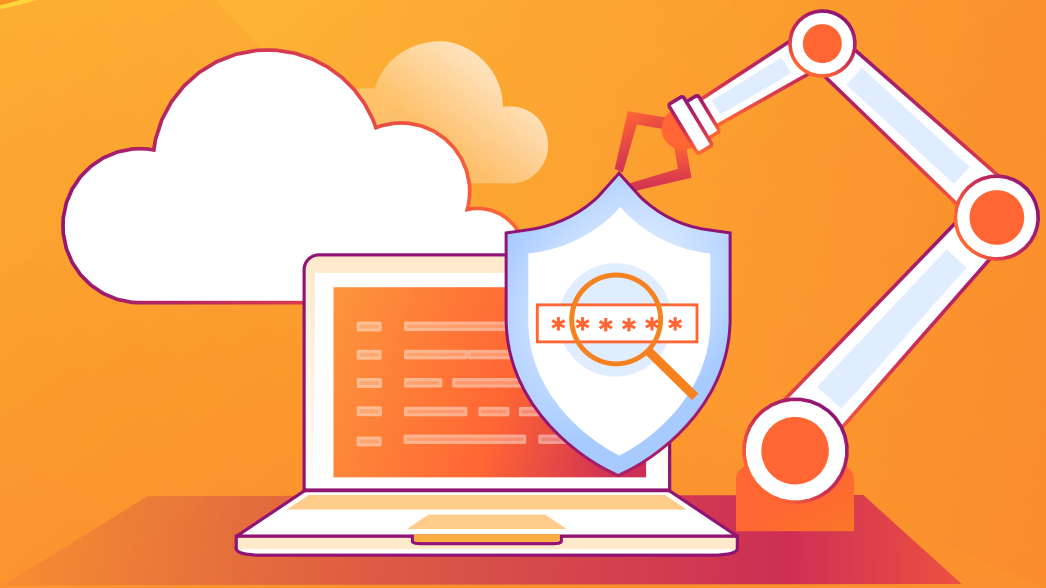
CLOUDFLARE

LIVRE BLANC

Défendre le secteur manufacturier : les meilleures pratiques de sécurité pour arrêter les cyberattaques



Vue d'ensemble

Des rançongiciels jusqu'aux bots et aux attaques lancées contre les applications et les appareils IdO, les fabricants constituent une cible de choix pour les cybercriminels. En 2022, selon un rapport d'IBM, les attaques par rançongiciel ont ciblé le secteur manufacturier plus que tout autre secteur de l'industrie.

Ces tendances alertent les DSI et leurs équipes responsables de la sécurité. En dégradant les performances des systèmes informatiques et des technologies opérationnelles, ces attaques peuvent entraîner une diminution de la production, voire des fermetures d'usines. Si un acteur malveillant dérobe des données sensibles ou de la propriété intellectuelle, le fabricant court le risque de commettre des infractions à la réglementation, voire de perdre un avantage concurrentiel.

Compte tenu de ces risques, les fabricants doivent examiner leurs stratégies et leurs tactiques de sécurité afin d'identifier les vulnérabilités et se défendre contre les cybermenaces. Dans ce livre blanc, nous présentons les défis courants auxquels sont confrontés les fabricants et recommandons des pratiques exemplaires permettant d'élaborer une stratégie de sécurité solide, afin d'éviter que des incidents ne provoquent des pertes de données et ne perturbent les opérations, avec des conséquences préjudiciables sur le chiffre d'affaires et les relations avec les parties prenantes.

Des problématiques de sécurité difficiles à résoudre avec des ressources limitées

Les entreprises qui luttent contre la cybercriminalité sont confrontées à un manque de ressources dans le domaine de la sécurité informatique. La protection du personnel sur site et hybride (ainsi que la protection des données, des applications, de l'infrastructure et des équipements) est une tâche difficile pour n'importe quelle entreprise. Cependant, en raison des contraintes budgétaires, les DSI ont encore plus de mal à doter leurs équipes de sécurité d'un personnel suffisant, possédant la disponibilité et la compétence indispensables pour mettre un terme aux attaques sophistiquées. Un cas illustrant les conséquences est celui de l'entreprise MKS Instruments, qui a annoncé en 2023 qu'un incident lié à un rançongiciel affecterait ses résultats au premier trimestre.

Les écosystèmes des fournisseurs des fabricants constituent un autre domaine qu'il est difficile de prioriser en l'absence de ressources suffisantes dédiées à la sécurité. Des attaques sophistiquées utilisent des logiciels malveillants conçus pour exploiter les vulnérabilités des chaînes d'approvisionnement, et ainsi, obtenir des informations confidentielles ou perturber les opérations. Le groupe auteur de menaces Chernovite, qui se concentre sur les systèmes de contrôle industriel, a ciblé des technologies dépendantes de fournisseurs tiers, qui assurent l'approvisionnement en composants des fabricants.

Les réseaux de l'Internet industriel des objets (IIoT) présentent également des menaces. Trois fournisseurs de routeurs cellulaires industriels ont découvert que leur plateforme de gestion cloud exposait leurs réseaux de technologies opérationnelles à des risques. Ces vulnérabilités étaient suffisamment graves pour que des analystes de la sécurité déterminent qu'elles pouvaient affecter des milliers d'appareils IIoT soutenant les activités de clients.

Les budgets limités contraignent les équipes responsables de la sécurité à prioriser certaines vulnérabilités et menaces de ce type, sans disposer des technologies de sécurité adéquates. Il est pratiquement impossible de traiter l'immense volume de données indispensables à l'identification, la hiérarchisation et l'atténuation du large éventail de menaces :

- **Les rançongiciels** ciblent à la fois les systèmes technologiques opérationnels et les systèmes informatiques, contraignant souvent les fabricants à arrêter des lignes de production.
- **Les attaques contre la chaîne d'approvisionnement** menacent les fabricants qui dépendent d'un écosystème complexe de fournisseurs tiers.
- **Les attaques par ingénierie sociale** dupent les collaborateurs, les incitant à divulguer des informations vitales ou à télécharger des logiciels malveillants.
- **Les vulnérabilités affectant les appareils Industrial IoT** apparaissent lorsque des équipements connectés aux systèmes de contrôle industriels n'ont pas bénéficié de correctifs ou utilisent un système d'exploitation obsolète.
- **Les attaques contre la couche application** incluent les injections SQL permettant de manipuler le code afin d'accéder à des données sensibles ou d'exécuter des requêtes malveillantes.
- **Les attaques de bots** utilisent des scripts automatisés pour perturber les performances des serveurs et des points de terminaison, dérober des données ou effectuer des achats frauduleux.
- **Les attaques DDoS (Distributed Denial of Service)** inondent les serveurs et les sites web de trafic frauduleux, rendant l'accès impossible pour les utilisateurs légitimes.

Les fabricants sont également confrontés à des risques internes. Un employé peut accidentellement permettre à des données sensibles de quitter le réseau, ou un employé mécontent peut endommager des systèmes par malveillance ou dérober des données.

Meilleures pratiques de consolidation de la stratégie de sécurité

Pour élaborer une stratégie de sécurité solide, permettant de protéger les utilisateurs, les applications et les ressources du réseau, les fabricants doivent mettre en œuvre une série de bonnes pratiques en matière de sécurité :

- **Mettez en œuvre un modèle de sécurité Zero Trust**, afin de fournir à tous les utilisateurs un accès sécurisé, tout en réduisant la latence des applications. Cette démarche consiste à mettre en œuvre une stratégie consistant à « ne jamais faire confiance, toujours vérifier » à l'égard des utilisateurs et des appareils, chaque fois qu'ils se connectent à un réseau d'entreprise.

  L'adoption de cette approche est particulièrement cruciale pour les effectifs comptant des sous-traitants et des fournisseurs. Chaque groupe d'utilisateurs doit disposer d'un accès sécurisé à des applications et outils internes spécifiques, quel que soit l'endroit depuis lequel les utilisateurs travaillent. Le modèle Zero Trust permet un accès aux applications fondé sur l'identité et le contexte, ainsi que la mise en œuvre d'une sécurité définie par logiciel, aidant ainsi les fabricants à sécuriser les utilisateurs, les appareils et les données à distance sans sacrifier les performances ou l'expérience utilisateur.

  En complétant le modèle de sécurité Zero Trust avec des outils de protection des utilisateurs et des appareils (par exemple, un CASB (Cloud Access Security Broker), une passerelle web et une solution cloud de sécurité des e-mails), les fabricants peuvent défendre les applications web, SaaS et auto-hébergées contre les menaces. L'association de ces outils permet l'application de politiques de sécurité (telles que la limitation du débit) et la surveillance des requêtes et des activités des utilisateurs lorsqu'ils interagissent avec les applications. Les administrateurs de système sont également notifiés en cas de menaces liées à des logiciels malveillants, et peuvent analyser la manière dont les réseaux de technologies opérationnelles et les réseaux informatiques appliquent les politiques de sécurité. Pour les utilisateurs, ces outils empêchent l'accès aux applications malveillantes et offrent une protection contre les menaces véhiculées par e-mail, telles que le phishing.

- **Déployez une défense en profondeur** afin de contraindre les cybercriminels à franchir plusieurs couches de protection, au cas où ils parviendraient à en franchir une ou même deux. Cette mesure peut inclure le déploiement de pare-feu pour les réseaux et les sites web, ainsi que de dispositifs de protection des API et d'outils de sécurité exécutant des analyses afin d'identifier les logiciels malveillants.

- **Déployez une protection contre les vulnérabilités de l'IdO** en mettant en œuvre des politiques de gestion des appareils, en vérifiant régulièrement si les systèmes présentent des vulnérabilités et en installant des mises à jour de sécurité.

- **Mettez en œuvre des restrictions d'accès strictes** pour les collaborateurs et surveillez les comportements qui indiquent qu'ils pourraient être en train de fouiner. Vérifiez également les antécédents des nouveaux collaborateurs, afin d'avoir connaissance de tout acte répréhensible commis chez un précédent employeur.

Parmi les autres pratiques exemplaires que les fabricants peuvent mettre en œuvre pour garantir la solidité de leurs mesures de sécurité figure la formation, qui aidera le personnel de direction et les collaborateurs à comprendre leur rôle dans la sécurité et à éviter d'être victimes d'une attaque. Enfin, il convient d'examiner les stratégies de sécurité des fournisseurs, en vous assurant qu'ils déploient les contrôles d'accès indispensables et qu'ils surveillent les systèmes compromis afin d'empêcher le lancement d'attaques contre la chaîne d'approvisionnement par le biais de portes dérobées.

Les pratiques de sécurité exemplaires en action : scénarios d'utilisation dans le secteur manufacturier

Les pratiques de sécurité exemplaires fournissent un cadre sur la base duquel les fabricants peuvent déployer des technologies spécifiques permettant de faire face aux menaces en matière de sécurité. Dans un scénario d'utilisation particulier, un fabricant de produits d'éclairage faisait face à un volume croissant d'attaques contre la couche application empêchant les clients d'accéder à son site web.

Les problèmes de performances avaient un impact préjudiciable sur l'image de la marque et empêchaient les clients potentiels de contacter l'entreprise. Il s'avérait également difficile d'analyser et d'atténuer les attaques ; les processus manuels contraignaient l'équipe responsable de la sécurité à consacrer beaucoup de temps à remédier aux menaces, et prolongeaient durablement la dégradation des performances des applications.

Après avoir déployé un pare-feu d'applications web, le fabricant a constaté une amélioration spectaculaire de sa capacité à détecter et atténuer les attaques contre les applications web. L'équipe responsable de la sécurité observe désormais un nombre plus important d'attaques, car le pare-feu détecte les attaques de bas niveau et la neutralisation des menaces demande moins de temps, car la collecte et l'analyse des données des journaux et des flux de trafic sont automatisées.

Une autre pratique exemplaire, la protection du réseau, a permis d'accélérer la réponse aux incidents pour ce fabricant de solutions d'éclairage. Les attaques altéraient auparavant la réactivité des serveurs, ce qui compliquait la collecte des données et la mise en œuvre des changements nécessaires. Désormais, les attaques sont arrêtées avant d'atteindre les systèmes de l'entreprise, ce qui améliore les performances des serveurs et rend inutiles les opérations manuelles de collecte de données et de neutralisation des attaques.

Dans un deuxième scénario d'utilisation, un fabricant mondial de pièces automobiles souhaitait améliorer sa capacité à gérer les surfaces d'attaque. Plus précisément, l'équipe informatique ne pouvait pas déterminer combien d'attaques DDoS et d'attaques liées à des bots se produisaient, ni combien d'attaques étaient évitées. En raison d'un service d'application web exécutant plusieurs instances cloisonnées, la consolidation de l'ensemble des informations et leur gestion centralisée s'avéraient difficiles.

Le déploiement d'une solution de limitation du débit permet désormais à l'équipe informatique de se défendre contre les bots et les attaques DDoS. Dans le même temps, un pare-feu d'applications web offre à l'équipe une visibilité considérablement améliorée des types d'attaques, des vulnérabilités et des niveaux de risque. Cette visibilité permet aux membres de l'équipe de visualiser rapidement quelles attaques représentent une menace sérieuse, afin de pouvoir organiser aussi efficacement que possible les ressources défensives.

Un réseau mondial permettant la connexion sécurisée des utilisateurs aux applications

D'éminents fabricants ont résolu leurs problèmes de sécurité en s'adressant à Cloudflare.

Cloudflare s'exécute sur un réseau mondial couvrant plus de 300 villes, connectant en toute sécurité les utilisateurs aux applications pour entreprises avec des contrôles basés sur l'identité, tout en garantissant la mise en œuvre sécurisée des applications web. Le réseau mondial offre une protection sans compromettre l'expérience utilisateur. Il offre également d'autres avantages, notamment :

- Il sécurise l'accès de tous les utilisateurs à toutes les applications, sur tous les appareils et sur tous les sites
- Il garantit la sécurité, les performances et la fiabilité des réseaux dans le monde entier
- Il accélère le développement et le déploiement d'applications dans le cloud
- Il se connecte facilement à l’infrastructure sur site

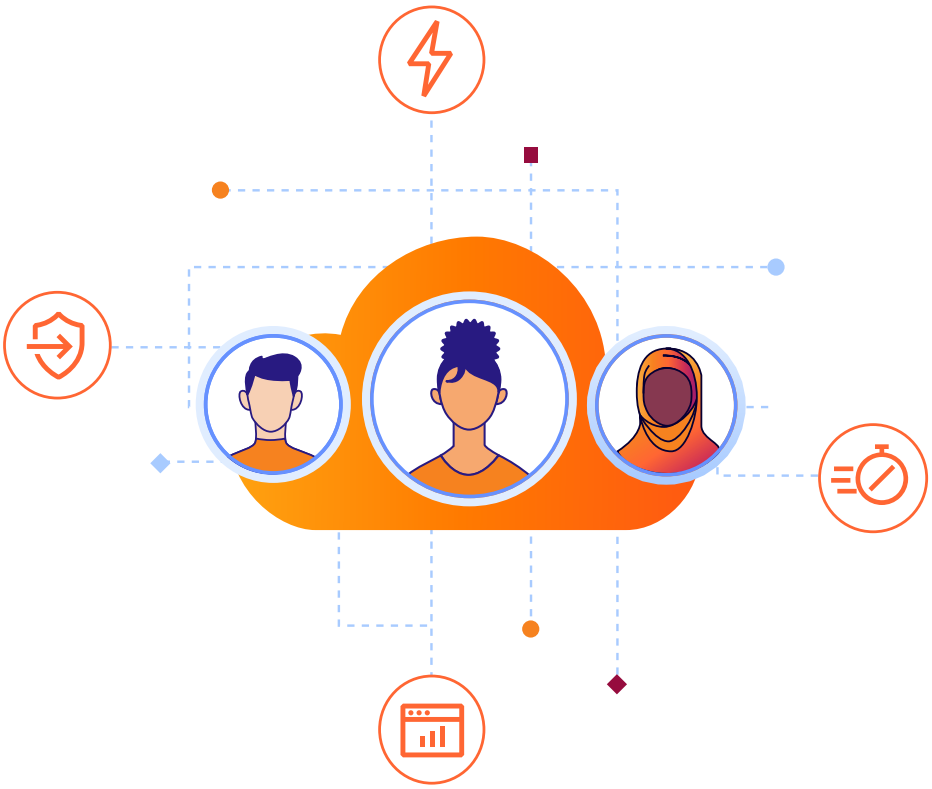
La plateforme unifiée de Cloudflare est également facile à utiliser ; chaque service s'exécute sur chaque serveur dans chaque datacenter du réseau. En servant un pourcentage important de l'ensemble du trafic Internet et en arrêtant 140 milliards de menaces chaque jour en moyenne. Cloudflare applique les informations sur les menaces afin de protéger automatiquement toutes les ressources connectées à notre réseau.

Une protection contre les cyberattaques – sans compromettre l'expérience utilisateur

Les fabricants sont confrontés à de nombreux défis en matière de sécurité, qui s'étendent des rançongiciels jusqu'aux menaces affectant la chaîne d'approvisionnement et incluent également l'ingénierie sociale, les vulnérabilités de l'IIoT, les bots et les attaques DDoS, ainsi que les menaces internes intentionnelles et non intentionnelles dues aux collaborateurs. Il est d'autant plus difficile de relever ces défis que les budgets restreints ne permettent pas aux DSI et aux équipes responsables de la sécurité d'embaucher suffisamment de personnel possédant les compétences requises, ni de lui fournir les outils nécessaires pour bien effectuer son travail.

Le déploiement de Cloudflare vous permet de relever ces défis. La plateforme facilite la mise en œuvre des pratiques exemplaires, notamment du modèle de sécurité Zero Trust, ainsi que d'une approche de défense en profondeur reposant sur plusieurs couches de protection. Ces technologies vous permettent de connecter en toute sécurité les utilisateurs aux applications pour entreprises avec des contrôles basés sur l'identité, tout en accélérant les déploiements – et sans compromettre l'expérience des utilisateurs.

Si vous avez besoin d'aide pour relever vos défis en matière de sécurité ou si vous souhaitez en savoir plus sur la plateforme Cloudflare, contactez Cloudflare dès aujourd'hui.



CLOUDFLARE

+33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV. : BDES-5102.2023SEP13