PARIS : Protection des équipements connectés et des réseaux industriels

Les cybercriminels ont profité du télétravail pendant l'épidémie de coronavirus pour intensifier leurs attaques contre les équipements médicaux, d'entreprise et industriels connectés, et les infrastructures critiques.

Étant donné que 63 % des entreprises, 92 % des entreprises industrielles et 82 % des organismes de soins de santé utilisent des équipements connectés, presque toutes les entreprises y sont exposées. Tout est connecté : caméras IP, ascenseurs intelligents, moniteurs patients, machines d'IRM et systèmes de contrôle industriels. Malheureusement, la connexion de ces équipements à votre réseau informatique étend la surface d'attaque et ajoute des points d'entrée que les pirates informatiques peuvent cibler. Le risque est réel puisque 67 % des entreprises et 82 % des organismes de soins de santé ont connu des incidents de sécurité liés aux équipements connectés.

Les solutions de cybersécurité de Check Point pour les équipements connectés protègent des milliers d'appareils dans les bureaux, les bâtiments intelligents, les environnements industriels et les environnements de santé contre les attaques au niveau du réseau et des appareils.

Cet article présente les solutions de sécurité pour les réseaux industriels et les systèmes de contrôle industriel (ICS) qui gèrent nos infrastructures critiques, dans les secteurs du pétrole et du gaz, de la fabrication, du transport et des services publics.

Les systèmes de contrôle industriel au cœur des

infrastructures critiques

Les infrastructures critiques comprennent l'eau que nous buvons, l'électricité qui alimente nos foyers et le transport de cargaisons dans le monde entier par mer, terre et air. Elles aiguillent les services d'urgence et veillent à ce que notre circulation se déroule sans encombre. Elles automatisent la fabrication des produits que nous utilisons quotidiennement et alimentent notre industrie en pétrole, en gaz et en énergies renouvelables. Elles contrôlent même les systèmes de gestion des bâtiments dans les hôpitaux, les Datacenters et les bureaux. Comme vous pouvez le voir, une attaque contre les infrastructures critiques peut avoir des répercussions sur presque tout le monde.

Le risque pour la sécurité est considérablement amplifié par le coronavirus

Les cyberattaques contre les infrastructures critiques ont augmenté de 2 000 % en 2019, perturbant souvent des activités essentielles. Le télétravail, rendu obligatoire par le coronavirus, a amplifié le risque pour la sécurité. Il y a actuellement une pénurie de travailleurs dans les infrastructures critiques et, en raison d'arrêts-maladie et des mesures de quarantaine, davantage d'employés travaillent à distance avec moins de contrôles de sécurité sur leurs réseaux personnels que sur les réseaux de leurs lieux de travail.

Ces connexions à distance ont estompé les frontières entre les réseaux informatiques et les réseaux industriels, et ont élargi la surface d'attaque, offrant de nouveaux points d'entrée que les pirates peuvent exploiter. Si l'ordinateur portable d'un collaborateur est compromis, cela peut avoir des conséquences sur l'accès aux réseaux informatiques et industriels, car les pirates peuvent utiliser les privilèges de ce collaborateur pour se déplacer latéralement, et passer du réseau informatique au réseau industriel et aux systèmes de contrôle des usines. Une fois parvenus aux systèmes de

contrôle, les pirates peuvent superviser et manipuler les composants opérationnels, notamment en lisant les commandes ou en les modifiant pour perturber les activités.

Élargissement de la surface d'attaque des systèmes de contrôle et accélération de la fréquence des attaques

La surface d'attaque des systèmes de contrôle et la fréquence des attaques augmentent, avec 61 % des incidents perturbant les réseaux industriels des entreprises et touchant les processus de production. Sécuriser les infrastructures critiques d'aujourd'hui contre les cyberattaques est plus difficile que jamais pour plusieurs raisons.

Premièrement, les ressources des systèmes de contrôle sont plus vulnérables aux attaques car beaucoup d'entre elles n'ont jamais été prévues pour être connectées à un réseau. Deuxièmement, les systèmes de contrôle industriel sont de plus en plus connectés à mesure que les entreprises se dirigent vers le principe d'Industrie 4.0. Industrie 4.0 est la combinaison des méthodes de fabrication traditionnelle avec les toutes dernières technologies, y compris les communications M2M et les équipements connectés, pour permettre des processus automatisés et intelligents.

Cela présente de grands avantages, et a permis d'étendre les réseaux industriels et les systèmes de contrôle pour connecter des dizaines de milliers de nouveaux appareils intelligents, ce qui signifie des milliers de nouveaux points de vulnérabilité. Cela a continué d'estomper les frontières entre les réseaux informatiques et industriels, et permettre aux pirates de se déplacer plus facilement dans les réseaux.

Les ressources des systèmes de contrôle sont intrinsèquement vulnérables

Les systèmes de contrôle utilisent des logiciels propriétaires et anciens qui n'intègrent pas de protection. Ces dispositifs n'ont pas été conçus à l'origine pour la connectivité en

réseau et encore moins pour la sécurité. Ils ne disposent pas de capacités suffisantes d'authentification des utilisateurs, des données et des systèmes. Leurs logiciels ne peuvent être mis à jour ou corrigés fréquemment, en raison des difficultés d'accès, des temps d'arrêt probables, ou de la nécessité de les certifier à nouveau.

Windows XP est le principal système sous-jacent de ces technologies industrielles. Les pirates savent que le système d'exploitation est un talon d'Achille car il n'est plus activement pris en charge par Microsoft, et qu'il est extrêmement difficile et coûteux pour les entreprises de mettre à jour les appareils critiques qui fonctionnent sous XP. Elles utilisent par ailleurs des mots de passe faibles ou codés en dur qui sont faciles à pirater.

Cela en a fait une cible de choix pour les attaques sur mesure, les logiciels malveillants traditionnels, le phishing et les attaques de logiciels rançonneurs qui commencent généralement par cibler le réseau informatique. Les systèmes de contrôle sont une cible particulièrement attractive pour les pirates qui utilisent des logiciels rançonneurs parce qu'ils savent que les entreprises préfèrent payer la rançon plutôt que d'être confrontées à des temps d'arrêt ou, pire encore, à l'arrêt complet de leurs activités. Quel type de système de sécurité peut répondre à tous ces défis ?

On ne peut pas protéger ce que l'on ne voit pas

Les environnements industriels sont devenus de plus en plus complexes, mais les solutions de sécurité informatique traditionnelles sont restées loin derrière. Le point de départ est de gagner en visibilité sur les risques. Les entreprises ont besoin d'un moyen facile de déterminer les appareils dont elles disposent, leurs vulnérabilités et les risques qu'ils présentent. La seconde étape consiste à pouvoir surveiller les protocoles et les commandes ICS et SCADA, afin de pouvoir déterminer si leurs systèmes se connectent et communiquent

correctement. La troisième est de vous permettre de créer des politiques de sécurité pour les réseaux industriels et les systèmes de contrôle, capables d'empêcher les failles de sécurité et de se tenir au fait des toutes dernières menaces. Tout cela doit être fait sans nuire aux opérations de sécurité. La sécurité doit être facile à déployer pour les entreprises, avec une protection automatisée qui n'a pas d'incidence sur les activités quotidiennes.

Solution de sécurité de Check Point pour les systèmes de contrôle industriel : Nouvelle passerelle de sécurité 1570R
La solution de sécurité de Check Point pour les systèmes de contrôle industriel minimise l'exposition aux risques dans les environnements informatiques et industriels, et bloque les attaques avant qu'elles n'atteignent les ressources critiques. Le tout d'une manière facilement évolutive qui ne perturbe pas les processus critiques.

Découvrir et évaluer les risques des appareils

Check Point vous permet de découvrir toutes les ressources présentes sur les réseaux industriels et les systèmes de contrôle afin de de déterminer les risques et les vulnérabilités en matière de sécurité. À partir d'une console unique, vous pouvez visualiser toutes vos ressources, qui sont classées selon leur niveau de risque, et effectuer une analyse des risques pour chaque ressource.

Politiques de sécurité recommandées pour une approche Zero Trust

Une fois que vous avez compris vos risques, Check Point vous propose des politiques de sécurité Zero Trust personnalisées pour chaque appareil afin de minimiser instantanément votre exposition aux risques. Cela vous évite de passer des mois à configurer manuellement les politiques de sécurité, et garantit la protection de vos ressources industrielles dès leur première connexion à votre réseau. Vous pouvez facilement

mettre en œuvre des politiques qui garantissent que les systèmes n'utilisent que les protocoles de communication qu'ils sont autorisés à utiliser, et bloquer les accès non autorisés à vos équipements industriels.

La prévention des menaces commence par la segmentation des réseaux informatiques et industriels

La clé de la conception des réseaux consiste à segmenter vos réseaux informatiques et industriels afin que les pirates ne puissent se déplacer de votre infrastructure informatique vers l'usine de fabrication. Les pare-feux Check Point de nouvelle génération, y compris la nouvelle Appliance 1570R, assurent la protection du périmètre entre le réseau industriel et le réseau informatique, ainsi que la micro-segmentation entre les départements et les lignes de production dans l'usine. Le module Purdue dans le diagramme à votre droite est la méthode préférée de segmentation des réseaux informatiques et industriels. Avec une visibilité granulaire sur les protocoles et les commandes SCADA, ces pare-feux permettent de contrôler l'accès à la totalité de l'environnement industriel.

Prévention des menaces avec protection contre les toutes dernières menaces

Comme nous l'avons appris précédemment, la sécurité doit être facile à mettre en œuvre sans avoir d'incidence sur les opérations. La solution de Check Point vous permet de protéger tous les appareils contre les attaques connues et inconnues de type zero-day grâce au cheminement virtuel. Check Point dispose de plus de 300 signatures de prévention des intrusions contre les attaques ciblant les réseaux industriels, qui sont constamment mises à jour grâce à ThreatCloud, notre base de données d'intelligence sur les menaces. Check Point ThreatCloud est le plus grand réseau d'intelligence sur les menaces au niveau mondial. Sa visibilité sur les tous derniers logiciels malveillants et les attaques de phishing est sans pareil.

1570R : Passerelle de sécurité robuste conçue pour les réseaux industriels et les systèmes de contrôle industriel
L'un des éléments clés de notre solution de sécurité pour systèmes de contrôle industriel est notre nouvelle passerelle de sécurité 1570R. L'Appliance 1570R est sécurisée et robuste, conçue pour les réseaux industriels afin de fournir une prévention des menaces de haut niveau, et protéger les systèmes de contrôle industriel des secteurs de la fabrication, de l'énergie, des services publics et du transport. Caractéristiques de la nouvelle passerelle 1570R :

Sécurité des réseaux informatiques et industriels sans compromis

La sécurité de la passerelle 1570R commence par des performances de 400 Mbps pour le débit de la prévention des menaces. Les performances sont multipliées par 10 par rapport à la passerelle 1200R de la génération précédente. La passerelle 1570R comporte 60 services de sécurité pour empêcher les toutes dernières attaques zero-day de perturber les activités. La segmentation permet une ségrégation totale entre les réseaux informatiques et industriels, avec un contrôle granulaire de l'environnement opérationnel.

Conçue pour les réseaux industriels

Non seulement la passerelle 1570R est en tête en termes de performances, mais elle offre la visibilité la plus complète sur 1 500 commandes et protocoles SCADA utilisés dans les systèmes de contrôle industriel. Cela permet de voir comment chaque appareil est connecté, et quels sont les protocoles et les commandes qu'ils utilisent pour communiquer. Vous disposez de la visibilité nécessaire pour stopper les activités malveillantes avant qu'elles ne se propagent dans votre réseau et ne perturbent vos opérations.

L'Appliance 1570R est fiable, robuste et sans fil

Son format robuste sans aucun élément mécanique permet à la

passerelle 1570R de fonctionner dans une plage de température allant de -40 à +75°C, ce qui la rend idéale pour un déploiement dans des environnements difficiles. Elle est certifiée conforme aux normes industrielles IEEE 1613 et CEI 61850-3 régissant les contraintes de chaleur, de vibration et d'immunité aux interférences électromagnétiques. Elle est également certifiée pour les opérations maritimes avec sa conformité à la norme CEI 60945.

La passerelle 1570R prend en charge les connexions réseau câblées, les connexions Wifi ou modem LTE, pour une protection facile et flexible des applications de ville intelligente (parcmètres intelligents, arrêts de bus, éclairage intelligent, capteurs environnementaux) et les réseaux intelligents (compteurs intelligents, automatisation des sous-stations).

À propos de Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) est l'un des principaux fournisseurs de solutions de cybersécurité pour les gouvernements et les entreprises dans le monde. Ses solutions protègent les clients contre les cyberattaques de 5e génération grâce à un taux de blocage inégalé des logiciels malveillants, des logiciels rançonneurs et autres types d'attaques. Check Point propose Infinity Total Protection avec prévention avancée des menaces de 5e génération, une architecture de sécurité à plusieurs niveaux, qui défend les données des entreprises dans le Cloud, les réseaux et les appareils mobiles. Check Point fournit le système d'administration unifiée de la sécurité le plus complet et le plus intuitif. Check Point protège plus de 100 000 entreprises de toute taille.