PASSION AFFAIRES et technologies

Présentés ce mois-ci :

Entreprise TI classée #1 à Québec en 2021 par **ThreeBest Rated®**

« La sécurité est importante chez Amisco…

On doit respecter certaines normes, dont C-TPAT. La compétence et la collaboration d'ARS sont indispensables à ce niveau. **Nous sommes à mettre en place une culture de cybersécurité qui protège concrètement notre organisation des cyberattaques.**

Avec les rapports de gouvernance, on est en mesure de prendre les bonnes décisions pour garder un niveau de sécurité adéquat. Cette vision globale qu'ARS nous donne rassure la direction. »

Gilbert Beaudoin
Directeur TI
Les Industries Amisco Ltée

Les cybercriminels visent les entreprises manufacturières vulnérables

L'Agence pour la cybersécurité et la sécurité des infrastructures (CISA) met en garde contre le fait que l'industrie manufacturière restera une cible très attrayante pour les malfaiteurs en 2022…

Pourquoi s'attaquer au marché manufacturier?
Les installations les plus critiques des entreprises manufacturières ne sont pas suffisamment sécurisées et présentent trop de zones de vulnérabilités que les assaillants pourraient atteindre. De ce fait, ce secteur est particulièrement à risque, sans compter l'insuffisance des effectifs de cybersécurité pour se défendre contre les offensives de piratage. « Ces tendances augmentent la vulnérabilité du secteur manufacturier face au nombre croissant d'attaques par rançongiciel visant les entreprises privées, en augmentant ainsi les surfaces d'attaque et en réduisant les capacités de protection », indique le rapport. « Pour atténuer les menaces futures, le secteur manufacturier devrait donc prioriser la gestion des risques. »

SUITE PAGE 2

Faits saillants du rapport de la CISA

01 Si les tendances actuelles se maintiennent, les attaques contre les infrastructures du secteur manufacturier vont continuer d'augmenter.

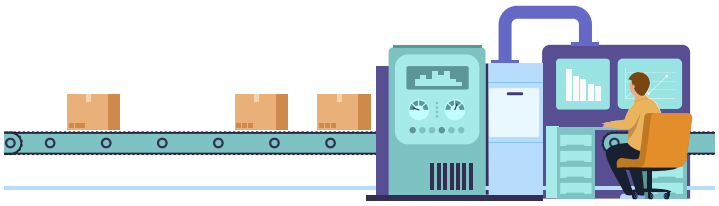
02 Les environnements, auparavant isolés d'Internet, sont davantage connectés aux réseaux d'entreprises, aux clouds publics, aux réseaux des fournisseurs et à d'autres tiers pour la gestion à distance.

03 L'expansion rapide de la surface d'attaque augmente la probabilité d'une cyberattaque suffisamment importante pour compromettre la sécurité du réseau et entraver la production.

04 Les attaques ou les perturbations de la chaîne d'approvisionnement compliquent encore plus la nécessité pour l'industrie manufacturière de fonctionner en toute sécurité. Les attaquants de rançongiciels ont commencé à cibler des systèmes ne disposant pas des contrôles de sécurité nécessaires pour se protéger.

05 Le résultat pourrait être une perte de production catastrophique et des temps d'arrêt, ainsi que des pertes de revenus et des pénalités pour les retards de production.

Un domaine de préoccupation que la CISA a mis en évidence est l'utilisation accrue de la robotique pour automatiser les processus de fabrication critiques et les cybermenaces associées. La surveillance, la validation et le contrôle à distance doivent être adaptés pour soutenir les besoins opérationnels. Bien que l'automatisation des processus par la robotisation



améliore la capacité de production et la sécurité, elle introduit également des risques externes à la chaîne d'approvisionnement.

Les vulnérabilités opérationnelles potentielles dans les systèmes de contrôle qui gèrent les processus industriels (ICS) résultant du travail à distance incluent :

- L'expansion des surfaces d'attaques
- La réduction de la segmentation et de la sécurisation du réseau
- Les accès non autorisés (à la fois physiques et en ligne)

La directrice de la CISA, Jen Easterly, a souligné l'importance pour les entreprises manufacturières de renforcer leur plan de protection en cybersécurité.

Quelques mesures que la CISA recommande aux organisations manufacturières :

- Développer la cybersécurité et les connaissances opérationnelles dans l'environnement de production est essentiel, étant donné la densité réduite des équipes.
- Investir dans la formation des analystes en sécurité pour qu'ils soient capables de surveiller les environnements de fabrication et qu'ils développent davantage de connaissances en sécurité sur les équipements en usine.
- Le partenariat entre les ressources de production et les analystes en cybersécurité doit être développé en fonction de la tolérance au risque de l'organisation.

Sources : CISA, NSA et FBI

Conseils anti-hammeçonnage

Continuez de lutter contre la cybercriminalité! Inscrivez-vous pour recevoir nos **NOUVEAUX "conseils anti-hameçonnage" SANS FRAIS** et gardez vos employés alertes. **Vous recevrez ensuite un conseil à tous les mois par courriel.**

Pour vous inscrire :
www.ars-solutions.ca/conseils-anti-hameconnage-phase-2/
info@ars-solutions.ca • 418 872-4744 #233

8 prédictions de cybersécurité 2022

Les entreprises et les responsables de la sécurité doivent s'aligner sur les menaces potentielles auxquelles ils seront confrontés en 2022. Voici 8 prévisions des dirigeants de LogRhythm en matière de cybersécurité :

1. Le pourcentage de responsables de la sécurité des systèmes d'information va doubler

Le rôle du responsable de la sécurité des systèmes d'information (RSSI) ou Chef Information Security Officer (CISO) va se transformer, car les gestionnaires d'entreprise cherchent à comprendre les risques auxquels leur organisation est confrontée et comment les programmes de cybersécurité peuvent les protéger. Le responsable de la sécurité aura davantage d'influence sur les décisions des membres du comité de direction.

2. Les budgets des équipes de sécurité connaîtront une augmentation à deux chiffres

Les équipes de sécurité gagneront de l'importance en 2022 : l'augmentation des investissements servira principalement à minimiser les risques liés aux fournisseurs dans le cadre de la sécurité des applications et à embaucher des talents pour valider le code source utilisé par les entreprises.

3. Un grand fabricant de vaccins sera stoppé par un rançongiciel

En 2022, des cybercriminels mèneront une attaque par rançongiciel contre l'une des plus grandes entreprises pharmaceutiques produisant le vaccin contre la COVID-19, interrompant ainsi la production de rappels essentiels et empêchant de nombreux autres médicaments vitaux d'être accessibles aux patients.

4. Un pays leader dans la production de puces à semi-conducteurs verra sa chaîne d'approvisionnement compromise

Un pays se fera prendre à utiliser des méthodes frauduleuses pour accéder à la production et à l'approvisionnement des pays producteurs de puces, qu'on retrouve notamment dans les téléphones intelligents, les ordinateurs et les automobiles. Il en résultera des pénuries de fournitures essentielles ainsi qu'une flambée des produits de base.

5. Les cybercriminels vont exploiter les vulnérabilités des interfaces de programmation d'application (API) pour pénétrer dans plusieurs réseaux d'entreprise à la fois

Nous verrons des cybercriminels chercher à exploiter des API mal configurées, qui servent de porte d'entrée pour accéder au réseau d'une entreprise.

6. Une attaque réussie à grande échelle sera lancée par le biais d'un logiciel libre

Les cybercriminels cibleront les entreprises qui ont créé des produits à l'aide de technologies "open source" sans en examiner le code avant de le copier et de le coller dans leurs plateformes. Il est probable que de telles attaques soient déjà présentes aujourd'hui et pourraient être découvertes dans l'année à venir.

7. Les cybercriminels feront chanter les athlètes olympiques pendant les Jeux de Pékin

Les malfaiteurs s'introduiront dans les comptes des athlètes pour trouver des échanges de courriels compromettants concernant l'utilisation de produits dopants ou leur vie privée, afin de les faire chanter pour qu'ils aident les attaquants à mener des cyberattaques contre leur pays d'origine.

8. Les individus, et non les infrastructures, seront les principales menaces de la Coupe du monde de la FIFA 2022 au Qatar

Les cybercriminels s'en prendront aux particuliers, ainsi qu'aux organismes de voyage et d'accueil qui entourent la Coupe du monde. La billetterie, les réservations d'hôtel et les réservations en général peuvent être falsifiées et utilisées pour capturer des données personnelles et compromettre des individus. L'hameçonnage et l'ingénierie sociale seront utilisés pour dérober des informations personnelles et financières.

Comment savoir si des applications vous espionnent via votre Iphone

La dernière mise à jour d'Apple donne aux utilisateurs la possibilité d'identifier les applications qui pourraient les surveiller.

Parmi les nombreux changements apportés par la mise à jour iOS 15.2, disponible depuis décembre dernier, on y retrouve l'introduction du rapport sur la confidentialité des applications. Cet outil **permet aux usagers de voir quelles informations les applications recueillent sur eux et où elles les envoient sur Internet.** Il s'agit d'un moyen de contrôler le suivi des applications et de supprimer celles qui pourraient utiliser ces informations de manière inutile ou dangereuse.

Activez le rapport de confidentialité des applications

La fonctionnalité est disponible sur tous les iPhone qui ont été mis à jour vers iOS 15.2. Elle peut être installée comme d'habitude, via l'application "Paramètres", puis en cliquant sur "Mise à jour du logiciel". **Cette fonction est désactivée par défaut, mais l'activer est très simple.** Il vous suffit d'ouvrir les "Paramètres", de cliquer sur "Confidentialité", puis de faire défiler l'écran jusqu'au "Rapport de confidentialité des apps", au bas de l'écran.

Suivez les informations d'utilisation de vos applications

Ce n'est que lorsque la fonctionnalité est activée que le suivi - ou, plus précisément, le suivi du suivi - commence. Ainsi, lorsque vous l'activez pour la première fois, vous êtes accueilli par un message vous indiquant que "des informations de rapport apparaîtront ici au fur et à mesure de l'utilisation des applications", et **vous devrez attendre un certain temps pour que le système accumule suffisamment d'informations** pour être réellement utile. Une fois ces informations recueillies, il suffit de se rendre dans la même partie de la page des paramètres pour que le rapport s'ouvre et que vous puissiez voir les informations recueillies.

Le rapport est divisé en deux sections : "accès aux données et aux capteurs" et "activités du réseau d'applications". **La première option indique chaque fois qu'une application a demandé l'accès aux informations contenues dans l'iPhone.** Il s'agit de toutes les informations, qu'il s'agisse d'éléments de données, comme les contacts ou les photos, ou d'informations provenant de capteurs, comme les données de localisation ou de santé.

La deuxième option montre comment ces applications se connectent à Internet et où elles envoient les informations. Vous pourrez voir dans quelle mesure elles sont actives, et en cliquant sur une application particulière, vous obtiendrez un ensemble d'URL avec lesquelles ces applications se sont connectées. **Si l'une des applications affichées agit de manière douteuse, son accès peut être restreint dans le menu "Vie privée", voire entièrement supprimé.** N'hésitez pas à nous contacter pour obtenir de l'aide à ce sujet.

Source : Andrew Griffin