A l'ère du piratage informatique, bonnes pratiques de sécurité dans le secteur industriel

by Par Rob Janssens
Responsable Processus et Conformité chez QAD

Livre blanc QAD
pour les Entreprises Industrielles Internationales

SOMMAIRE

A L'ÈRE DU PIRATAGE INFORMATIQUE, BONNES PRATIQUES DE SÉCURITÉ DANS LE SECTEUR INDUSTRIEL

INTRODUCTION : LA SÉCURITÉ DES DONNÉES EST UN ENJEU CRUCIAL POUR LE SECTEUR INDUSTRIEL

Les pirates informatiques et les professionnels de la sécurité des systèmes d'information se livrent une guerre sans merci. Les entreprises sont prises entre les deux et espèrent échapper aux cyberattaques. Toutefois, quels que soient les efforts et les ressources déployées par les experts en sécurité pour lutter contre les attaques et ériger des défenses, les pirates atteignent souvent leur cible, avec parfois des effets dévastateurs.

En principe, les professionnels en sécurité tentent de réduire les failles, les repèrent et les corrigent aussi efficacement que possible pour se protéger et limiter les dommages. L'omniprésence d'internet, des médias sociaux, de l'IoT, des technologies mobiles et la culture du hacking ont considérablement augmenté les risques et le coût de la sécurité informatique. Vous en doutez encore ? Voici ce qui s'est passé en 2017, l'année qui a enregistré le plus grand nombre de cyberattaques à fort impact. Aucun secteur d'activité n'a été épargné (y compris le service public). Les attaques ont ciblé aussi bien les entreprises du secteur industriel que les autres. Voici les principaux piratages ayant touché des entreprises non manufacturières en 2017 :

Plus de 14 millions d'enregistrements client ont été piratés chez Verizon.[1]

- Sabre, une société spécialisée dans les réservations a été victime d'une violation de données qui a impacté les compagnies aériennes, les chaînes d'hôtels et même Google.[1]
- L'agence de crédit Equifax a subi un piratage qui a entraîné la divulgation des données à caractère personnel de 145,5 millions de personnes.[2]
- Deloitte, l'un des plus grands cabinets comptable et de conseil a été visé par un piratage de données personnelles. L'ampleur de l'attaque a discrédité les activités de conseil en cybersécurité de l'entreprise.[3]

Voici quelques attaques ayant touché en 2017 des entreprises manufacturières et de logistique :

- Le ransomware WannaCry a provoqué des arrêts temporaires de production chez Honda, Nissan et Renault.[4]
- WannaCry a aussi contraint LG, le géant de l'électronique, à fermer son centre de service jusqu'à ce que des patchs de sécurité soient appliqués aux systèmes.[5]
- L'entreprise danoise Maersk, leader du transport maritime par conteneurs a subi des pertes atteignant 300 millions de dollars suite à une attaque par le ransomware Petya.[6]
- Quant à la cyberattaque NotPetya, elle a infiltré des fabricants en 2017. On lui impute la responsabilité des pertes réalisées chez le leader pharmaceutique Merck. La multinationale agroalimentaire Mondelez International compte aussi parmi les victimes de l'attaque.[7]

Comment les industriels doivent-ils réagir face aux risques croissants de cyberattaques et à l'augmentation des coûts de sécurité ? Des industriels prudents ont lourdement investi dans des expertises, des pratiques et des outils visant à renforcer la sécurité de leurs systèmes d'information. Toutefois, certains sont dans un tel déni, qu'ils ont même été piratés sans le savoir. Pour les industriels se trouvant dans les deux dernières catégories, il est temps de prendre conscience des problématiques et des risques liés à la sécurité de leurs données.

A L'ÈRE DU PIRATAGE INFORMATIQUE, BONNES PRATIQUES DE SÉCURITÉ DANS LE SECTEUR INDUSTRIEL

REPENSER LA SÉCURITÉ DES DONNÉES DANS LE SECTEUR INDUSTRIEL

Penser sécurité digitale avant sécurité physique pour vos données

Les dirigeants d'entreprise pensent souvent que les applications comme les ERP, notamment celles hébergées sur site, sont protégées. Sans doute, pensent-ils ainsi parce qu'ils n'ont pas encore été piratés, du moins pas à leur connaissance. Ils considèrent à tort que le contrôle physique des data centers sur site est synonyme de sécurité.

Les pirates informatiques ont recours à des technologies numériques, rares sont les attaques à caractère physique. Ces technologies numériques couvrent les sessions web piratées, les hotspots mobiles non sécurisés, le phishing (emails et liens internet), les applications mobiles non sécurisées et leurs données, les malwares et le piratage des médias sociaux. Selon une étude récente d'IBM sur la sécurité dans le secteur industriel, les violations de données d'ordre physique sont une minorité.[8]

Certains industriels continuent d'affirmer que la sécurité physique ne doit pas être négligée, alors que seulement 18 % des attaques sont d'ordre physique.[9]

L'une des méthodes les plus couramment employées pour infiltrer les données est « l'injection SQL » (les bases de données et les systèmes d'exploitation sont compromis par l'envoi de requêtes fallacieuses). Toutefois, nombreuses sont les techniques utilisées par les cybercriminels.[9] Il faut de plus s'attendre à ce que de nouvelles techniques voient le jour, car les pirates innovent constamment.

Qui est en mesure de se tenir au fait des dernières techniques de piratage informatique en termes d'expertise et de coût ?

Les industriels peinent à s'adapter, et les petits fournisseurs de services managés et d'hébergement placent toujours la sécurité physique au centre de leurs préoccupations. Les dirigeants devraient plutôt tenter de résoudre par eux-mêmes leurs problèmes ou avec l'aide de fournisseurs Cloud qualifiés.

Le coût croissant de la sécurité des données

Pour beaucoup d'industriels, il est difficile de conserver une expertise pointue en cybersécurité. ISACA, un groupe industriel de sécurité, anticipe un déficit de compétences en cybersécurité.

En 2019, il y aura une pénurie de deux millions d'experts dans le monde entier. Aux États-Unis, chaque année 40 0000 postes d'analystes en cybersécurité sont vacants.[10] Les entreprises industrielles internationales paient cher l'expertise maison. De plus, le coût des logiciels et des outils de cybersécurité est très élevé voire prohibitif. A tel point que certains industriels s'orientent vers une approche « maison ».

Cette attitude met sérieusement en danger la pérennité de l'entreprise. Quels sont les impacts potentiels d'une violation de données pour une entreprise industrielle ?

- Dans le pire des scénarios, la production est arrêtée. Le coût de la fermeture d'une usine varie selon le type de production mais à titre d'exemple, « la fermeture d'une ligne d'auto-assemblage coûte au moins 1 100 000 € par heure. »[11]
- Le coût moyen pour remédier aux données volées ou compromises est de 124 € par enregistrement.12 Ce qui signifie que le coût estimé pour remédier à 100 000 enregistrements compromis est approximativement de 12,3 millions d'€.

A L'ÈRE DU PIRATAGE INFORMATIQUE, BONNES PRATIQUES DE SÉCURITÉ DANS LE SECTEUR INDUSTRIEL

Le Cloud, un refuge sûr pour les industriels ?

Au début du « Cloud » ou des services SaaS (Software as a Service), terme utilisé pour désigner les applications exécutées dans le Cloud, le principal frein à l'adoption du Cloud était la sécurité. Les entreprises craignaient une perte de contrôle de leur sécurité informatique et pensaient que le Cloud représentait un risque supplémentaire.

Cela fait maintenant presque 20 ans que le Cloud et les services SaaS ont conquis les entreprises. Les fournisseurs Cloud ont eu largement le temps d'améliorer leurs outils, leurs pratiques et leurs processus de sécurité. Ils sont conscients des craintes des entreprises et ont beaucoup investi en cybersécurité. Compte-tenu de la multiplicité de leurs clients, ils savent qu'un Cloud infecté peut avoir des répercussions sur plusieurs, voire tous leurs clients. C'est pourquoi la sécurité est au cœur de la stratégie des fournisseurs Cloud. Ils sont vraisemblablement les plus impliquées dans la lutte contre les cyberattaques. En cas d'attaque, ils veulent avoir les moyens de limiter les impacts.

Face à des attaques toujours plus sophistiquées, le Cloud constitue désormais un environnement plus sécurisé et moins onéreux que les environnements sur site. Les fournisseurs Cloud engagés dans la protection des données ont l'expertise nécessaire et investissent dans des programmes, processus et outils de sécurité.

Les fournisseurs de services managés manquent de connaissances pour assurer la sécurité des applications et n'offrent pas beaucoup plus de protection que les environnements sur site et les solutions « maison ». De même, de nombreux industriels n'ont ni les moyens ni les ressources d'assurer une protection maximale de leurs systèmes d'information.

BONNES PRATIQUES ET OUTILS RECOMMANDÉS

Comment les industriels peuvent-ils se prémunir des piratages ? Quel que soit l'environnement utilisé (On Premise (sur site), dans le Cloud ou en mode hybride), il est important d'adopter les trois méthodes de protection suivantes :

(1) Application régulière et rapide des patchs de sécurité, (2) tests d'intrusion permanents et détection des menaces, et (3) réponse immédiate en cas d'incident. Et de façon plus détaillée :

- Il est essentiel d'**appliquer scrupuleusement les patchs et correctifs**. Au cours des premiers mois de 2017, Microsoft [9] a publié plus de 900 mises à jour de sécurité à destination des serveurs et systèmes d'exploitation.[13]

  Toutefois, quels que soient les efforts de Microsoft pour déployer rapidement ces patchs, des hackers peuvent exploiter une faille de sécurité. Il incombe aux industriels ou à leurs fournisseurs Cloud d'appliquer régulièrement les patchs pour se protéger des attaques.
- Même s'ils font preuve de rigueur, les industriels ne sont pas à l'abri d'une attaque. C'est pourquoi les **tests d'intrusion et la réponse en cas d'incident** sont impératifs. Plus une violation est détectée tôt, moins l'impact sur les coûts, les clients et la marque sera important.[12]

La plupart des industriels s'accordent sur le caractère stratégique des solutions ERP et de la Supply Chain. Quelles sont les meilleures pratiques de sécurité pour les entreprises utilisant des solutions telles que les ERP Cloud ? Pour bien choisir leur solution ERP, les entreprises doivent prendre en compte les critères suivants :

- Un programme de détection des intrusions dédié fonctionnant à temps plein et testé régulièrement.
- Une équipe de **réponse en cas d'incident** dédiée s'appuyant sur des processus de sauvegarde, restauration, et reprise après incident.

A L'ÈRE DU PIRATAGE INFORMATIQUE, BONNES PRATIQUES DE SÉCURITÉ DANS LE SECTEUR INDUSTRIEL

- Une application centralisée des patchs pour tous les éléments de la solution (système d'exploitation, bases de données, serveurs/plates-formes d'application, logiciel d'intégration, logiciel ERP, autres applications connexes). Cela implique l'adoption d'une approche globale de gestion des systèmes 24h/24.
- Une équipe **dédiée** en charge de gérer et d'assurer la sécurité du Cloud, ayant une **excellente connaissance** de l'ERP (un ERP hébergé via des services managés de tierces parties offre une sécurité moindre car l'équipe Cloud et l'équipe ERP ne collaborent pas et ne sont pas familiarisées avec les pratiques des unes et des autres).
- Des pratiques Cloud qui **respectent les certifications en matière de sécurité**. Cela comprend également le partage des résultats des tests et la publication des plannings de conformité. La démarche de certification témoigne de l'engagement de l'entreprise dans la lutte contre le piratage et la prévention des risques.
- Les services Cloud ne doivent pas prendre les clients en otage. Des **fournisseurs Cloud publics** tels qu'IBM Cloud, Amazon Web Services, etc. doivent offrir un niveau de protection élevé et répondre aux exigences de secteurs d'activité tels que le Life Sciences, notamment en ce qui concerne « l'infrastructure qualifiée ».
- Une équipe dédiée pour les services Cloud qui **collabore avec les experts en sécurité de l'entreprise pour garantir que les exigences de conformité de l'entreprise sont comprises et appliquées.**

Cette liste n'est pas exhaustive. Les problématiques de sécurité des industriels constituent un défi majeur dans l'économie numérique. Les récentes évolutions technologiques telles que l'IoT, les nouvelles formes de partage d'informations de la chaîne de valeur comme la blockchain et la gestion des relations clients-fournisseur dans le Cloud sont les futurs challenges du secteur industriel.

EN RÉSUMÉ : LE CLOUD OUVRE LA VOIE A LA SÉCURISATION DES DONNÉES

Ironiquement, la sécurité qui était autrefois un prétexte pour éviter le Cloud, est désormais une excellente raison pour passer au Cloud. Selon Aberdeen, les entreprises ont commencé en 2016 à s'orienter vers des ERP Cloud plutôt que des ERP sur On Premise (sur site).

Toutefois, chaque industriel doit prendre les mesures adéquates pour sécuriser ses données, se protéger des violations de données et prévoir un plan de remédiation en cas d'attaque. La pérennité de son entreprise en dépend. Compte-tenu des coûts de sécurité élevés, de la plus grande collaboration tout au long de la chaîne de valeur et de la nécessité d'intégrer de nouvelles applications, les industriels qui ont uniquement une approche maison de la sécurité doivent anticiper des obstacles.

L'ERP Cloud peut constituer un bon compromis pour trouver la juste mesure entre les risques et le coût. Toutefois, toutes les solutions ERP ne se valent pas en matière de sécurité. L'ERP Cloud peut être considéré comme un moyen d'atteindre un meilleur niveau de sécurité mais il est nécessaire que le ou les Clouds choisis satisfont aux engagements et aux critères permettant de se protéger des cyberattaques et de s'en prémunir.

Et vous où en êtes-vous en matière de sécurité ?
Pour obtenir une évaluation de votre situation actuelle en matière de sécurité Cloud, contactez un conseiller client QAD. Utilisé depuis plus de 10 ans dans le secteur industriel, QAD Cloud ERP a fait ses preuves et offre d'excellents résultats en matière de disponibilité, performances, sécurité et rapidité des implémentations.

A L'ÈRE DU PIRATAGE INFORMATIQUE, BONNES PRATIQUES DE SÉCURITÉ DANS LE SECTEUR INDUSTRIEL

SOURCES

[1]2017's biggest hacks, leaks, and data breaches — so far, ZDNet, September 20, 2017

[2]Equifax data breach affected millions more than first thought, CBS MoneyWatch, October 2, 2017

[3]After hack, security researchers probe Deloitte's security posture, by Zeljka Zorz, HELPNETSECURITY, September 27, 2017

[4]Honda Halts Car Production After WannaCry Infection, by Maritza Santillan, Tripwire: The State of Security, June 21, 2017

[5]LG Shut down due to Wannacry attack on its systems, by Ayobamidele Francis Mo bee, Digital Space Radio, August 23, 2017

[6]Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk by Danny Palmer, ZDNet, August 16, 2017

[7]Cyber 'Worm' Attack Hits Global Corporate Earnings, Reuters, August 2, 2017

[8]Security trends in the manufacturing industry: Intellectual property and operating information are the crown jewels, IBM X-Force® Research, 2017

[9]Countering the Threat of Physical Security Breaches, by Simon Williamson, The Data Center Journal, January 30, 2017

[10]The Fast-Growing Job With A Huge Skills Gap: Cyber Security, by Jeff Kauflin, Forbes, March 16, 2017

[11]Severe Weather and Manufacturing in America, Business Forward Foundation, 2014

[12]2017 Cost of Data Breach Study, Ponemon Institute, June 2017

[13]Microsoft Security Updates first 9 months of 2017 for server software (e.g. SQL Server, BizTalk Server, etc.) and OSes = 985. Source : Microsoft Security Tech Center – Security Update Guide search, January 1, 2017 through September 30, 2017.

QAD Europe
110, rue Auber
75009 Paris
Tél. : 01 1 43 12 95 60
www.qad.com