Reconstruction suite à une atteinte à la cybersécurité.

modis

L'horizon de la menace:
D'une complexité sans précédent

Le coût total de la cybercriminalité passera des trois mille milliards de dollars qu'il était en 2015 à six mille milliards de dollars d'ici 2021.[1] En fait, le rapport 2017 du Forum économique mondial sur les risques mondiaux établissait comme l'une des cinq principales tendances la cyberdépendance croissante menant inexorablement au risque d'une attaque massive. [2]

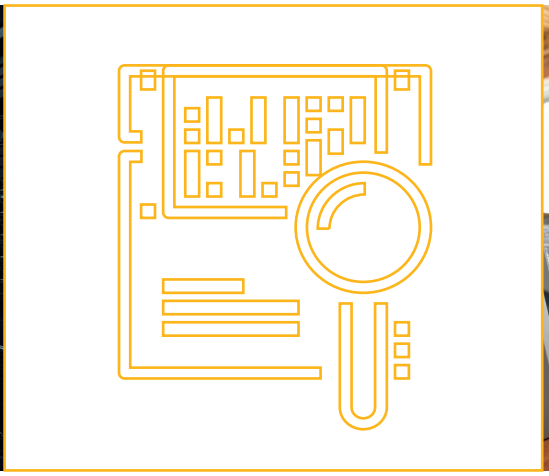
Dès maintenant, les criminels n'ont même plus à posséder quelque expertise en cybernétique pour lancer des attaques : les outils que sont les rançongiciels et les services de demande de rançon sont accessibles aux criminels, et peuvent facilement être adaptés à la demande. « Les entreprises se doivent d'investir de façon importante pour contrer efficacement la menace que constitue la cybercriminalité, dans chaque technologie, en personnel de sécurité à l'interne et en formation de l'ensemble du personnel dans le but de reconnaître, de cerner et d'éviter les menaces » selon la firme d'analystes Frost & Sullivan. [3]

En mai 2017, les nouvelles traitant de sécurité n'en avaient que pour WannaCry. L'attaque, qui selon ce qui en a été rapporté comme estimation, interdisait l'accès aux utilisateurs de 250 000 entreprises dans 70 pays, était particulièrement pernicieuse du fait qu'elle comportait à la fois un rançongiciel et un ver informatique, ce dernier lui permettant de se disséminer dans les réseaux plutôt que d'infecter un seul ordinateur. Les ordinateurs de Telefonica, de FedEx, de Deutsche Bahn et des Services de santé nationaux de Grande-Bretagne ont été entre autres atteints.

WannaCry a été presque immédiatement suivi par des rapports indiquant qu'un autre virus, Adylkuzz, s'emparait des ordinateurs personnels et tentait de s'en prendre à l'écosystème de Bitcoin. [4]

Puis, en juin 2017, une autre attaque mondiale entravait les opérations commerciales dans 64 pays. [5]

La firme de cybersécurité eSentire prédit que « Shadow Brokers », l'organisation criminelle qui s'est emparée d'une vulnérabilité de l'Agence de sécurité nationale qui a permis l'activation de WannaCry, sera de retour, dotée cette fois d'autres armes de cybercriminalité, alors que de plus en plus de criminels, inspirés par les succès de WannaCry et renforcés par l'efficacité de ses méthodes, tenteront d'accéder aux données critiques mondiales. [6]



Changements des attaques et des réactions – Vulnérabilités intrinsèques

Un monde connecté offre une surface d'attaque en constante expansion. Concurremment, des brèches existantes bien documentées demeurent béantes. WannaCry s'avère un exemple criant, lequel a exploité Windows XP. Même la NSA, l'origine même des outils de rançonnage de ces cyberattaques utilise XP, cette version de Windows qui ne bénéficie plus de mises à jour de sécurité.

Le Government Accountability Office des États-Unis inscrivait le recensement de 2020 sur sa liste des risques élevés en raison de sa dépendance à la technologie et de la dépendance du gouvernement aux systèmes en place. [7]

En mai 2017, la Maison-Blanche émettait un décret présidentiel portant sur le renforcement de la cybersécurité des réseaux fédéraux et de l'infrastructure essentielle. Cependant, il pourrait falloir plusieurs années avant que les systèmes du gouvernement soient totalement sécuritaires. [8]

La situation au sein des entreprises est quelque peu meilleure, mais n'atteint pas l'excellence. Un sondage effectué par le regroupement des professionnels de la sécurité des TI, « Spiceworks » montre que 14 % des ordinateurs personnels des entreprises dans plus de la moitié de toutes les entreprises commerciales opèrent encore sous la plateforme Windows XP. [9]

Les automobiles connectées sous attaque

Les voitures particulières sont devenues de plus en plus complexes et informatisées. En 2014, des chercheurs en sécurité rapportaient que les automobiles connectées étaient vulnérables en raison de leurs fonctions de connectivité, de leurs sondes et de leurs systèmes informatisés. [10]

De plus, les modèles les plus récents peuvent être déverrouillés et même démarrés à distance au moyen d'applications de téléphonie mobile – des applications qui peuvent facilement être attaquées, selon la firme de cybersécurité Kaspersky. [11] Le RSA insistait auprès des professionnels pour qu'ils tiennent à l'œil non seulement les cibles prisées que constituent les infrastructures, mais qu'ils n'ignorent pas ces cibles plus facilement accessibles que sont les automobiles [12] ou encore les lecteurs d'empreintes digitales des téléphones intelligents. [13]

Menace aux appareils et aux systèmes intégrés

Les pirates informatiques centrent leurs efforts tant sur les appareils que sur les logiciels. Scott Borg, directeur de U.S. Cyber Consequences Unit, disait récemment à un groupe d'ingénieurs en appareils d'informatique que les criminels délaissaient les systèmes de contrôle des opérations et centraient dorénavant leurs efforts sur les contrôleurs et les dispositifs intégrés de logique programmable.

« Vous, messieurs-dames, êtes maintenant dans la ligne de mire ; les décisions que vous prendrez en design auront des implications percutantes en sécurité. » — Scott Borg, U.S. Cyber Consequences Unit

« Au début, ils centraient leurs efforts sur le contrôle des opérations, surveillant diverses installations à partir d'un site central. Puis, ils ont ciblé le contrôle des processus, y compris les contrôleurs de logique programmable et les réseaux locaux. Ils ont ensuite migré vers les dispositifs intégrés et la possibilité de contrôle de pièces d'équipement individuel. Ils migrent maintenant vers les sondes elles-mêmes, les dispositifs à systèmes mécaniques microélectriques (MEMS). »

L'Internet des objets demeure hautement vulnérable. Alors que les villes deviennent de plus en plus « intelligentes », elles s'exposent de plus en plus aux manipulations malveillantes. 14 Les réseaux intelligents, les systèmes de transport connectés, les feux de circulation, l'éclairage intelligent des rues et les caméras de sécurité peuvent être l'objet d'attaques informatiques.

Manipulation du marché

Les cybercriminels peuvent faire beaucoup d'argent en manipulant le marché boursier. En 2015, un cercle criminalisé s'est emparé de plus de 100 000 communiqués de presse avant qu'ils ne soient publiés et s'est servi de cette information pour faire plus de 100 millions de dollars. [15]

Dans d'autres cas, les pirates informatiques se sont introduits dans les systèmes d'institutions financières et de firmes de courtage pour voler les données des clients et manipuler les prix des actions en bourse. [16]

Pratiques exemplaires pour la reprise après une intrusion

Les experts en sécurité s'entendent pour dire que les entreprises devraient se comporter comme si les intrusions en cybersécurité étaient inévitables. En 2016, Rob McMillan, directeur chez Gartner Research alertait en ces termes : « Votre entreprise doit être prête – une intrusion est inévitable pour nombre d'entreprises et les mesures de sécurité préventive s'avéreront éventuellement inefficaces. La question que vous devez vous poser n'est pas si des incidents de sécurité surviendront, mais plutôt à quelle vitesse vous pourrez les détecter et y remédier. » 17

Une entreprise bien préparée possède un plan de réaction aux incidents pour de telles situations. Le plan doit être conçu par une équipe interfonctionnelle qui comprend non seulement les TI, mais aussi la haute direction, le service juridique, des administrateurs de la sécurité des renseignements personnels (le cas échéant), ainsi que du personnel des relations publiques et des communications.

Le plan de réaction aux incidents décrit les procédures applicables en cas d'intrusion ainsi que les répercussions. Il sert de modèle d'approche sur mesure pour chaque incident.

Un rapport de mesure de 2012 produit par Ponemon Institute a démontré que les entreprises pouvaient réduire sensiblement le coût des intrusions touchant les données en ayant en place un plan de réaction aux incidents, un positionnement solide quant à la sécurité des TI, et un officier principal de la sécurité de l'information. 18

Voici les six étapes que devrait respecter toute entreprise lorsque survient une intrusion :

1. Évaluer et isoler les dommages.

Isoler les lieux physiques des appareils compromis et des logiciels ou systèmes qui ont été endommagés. Le fournisseur en protection de données Digital Guardian recommande de déconnecter tous les appareils affectés, mais en les laissant opérationnels. Attendre que l'équipe des sciences judiciaires ait entamé son enquête plutôt que de laisser le personnel permanent des TI examiner les fichiers. 19

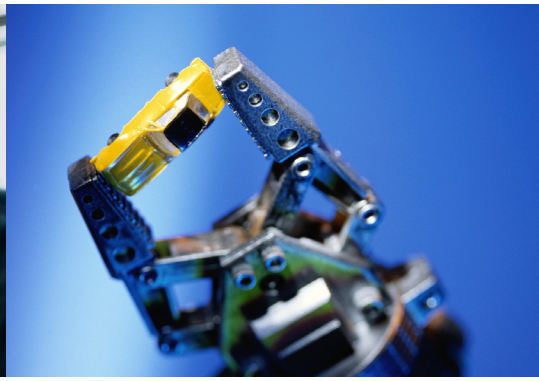
Il est important de documenter tout au sujet de l'intrusion et de la perte potentielle de données ou des systèmes compromis aussitôt que l'intrusion est découverte. Procéder à la réalisation de sauvegardes images en lecture seule des appareils affectés. Il devrait y avoir une ou des personnes de l'équipe de réaction qui soient responsables de la documentation. Sinon, désigner un membre du personnel pour cette responsabilité.

Les données numériques d'analyse judiciaire peuvent être fournies par une équipe interne d'experts ou par un fournisseur externe. L'équipe devrait être familiarisée avec les outils d'analyse judiciaire, et centrée sur l'enquête d'intrusion et le vol de données ; et en cette ère de dispositifs multiples, alors que plusieurs intrusions résultent de l'insertion d'une clé USB infectée, il serait bien avisé d'analyser les appareils mobiles et les dispositifs intégrés. Les informations judiciaires d'informatique peuvent aussi déterminer si un membre du personnel est responsable du vol des données.

Évaluer si les fonctions commerciales de l'entreprise ont été affectées, quelles sont les données hébergées dans les appareils ou les réseaux qui ont été compromises, si les données ont été compromises ou volées, et si des preuves numériques ont été détruites ou modifiées.

L'analyse judiciaire devrait s'appliquer à tous les dispositifs clients, tels que les disques durs, la mémoire, le trafic réseau et les applications.

Toutes les données du trafic réseau devraient être capturées et tous les paquets sauvegardés aux fins d'analyse judiciaire, de l'avis de Digital Guardian. L'équipe d'analyse judiciaire devrait évaluer les données de trafic archivées afin de rechercher les anomalies ou les signaux d'alerte.



Les solutions d'analyse judiciaire capturent automatiquement les données et les analysent en temps réel, donnant ainsi l'accès immédiat aux données nécessaires pour comprendre l'intrusion. Si l'entreprise ne fait pas appel à une telle solution, les registres et les fichiers doivent être vérifiés et analysés manuellement.

Prendre note de la façon dont l'intrusion a été découverte, et de tout le personnel impliqué, de même que si quelque appareil est manquant. Alors que plus d'information devient disponible, continuer la rédaction de la documentation. Établir une chaîne de mise sous garde des appareils et des données au cas où une action au criminel puisse être intentée.

2. Réparer le réseau.

Il s'agit sans conteste de la plus évidente et contraignante des étapes à suivre, mais elle ne devrait pas débuter avant que l'intrusion n'ait été complètement documentée.

Préciser l'origine de l'intrusion permettra non seulement à l'entreprise la maîtrise totale et la réparation complète du réseau, mais déterminera les mesures à prendre pour prévenir d'autres intrusions.

En plus de la réparation du réseau, d'autres réparations et d'autres actions peuvent s'avérer nécessaires. Par exemple, si l'intrusion provient d'un appareil ou d'une application fournie par l'entreprise, les appareils peuvent devoir être mis à niveau ou remplacés. Si l'intrus a volé les mots de passe ou l'information d'un client, tous devraient être avisés de modifier leurs mots de passe. Dans le cas de vol de données de cartes de crédit, de nouvelles cartes devraient être émises à tous les clients touchés.

3. Communiquer l'intrusion.

En réalité, il ne s'agit pas de la troisième étape ; ceci devrait se faire concurremment avec les deux premières étapes, au même moment où les équipes de sécurité sont affectées et procèdent à l'évaluation et à la réparation des dommages.

- Les équipes internes et les membres de la haute direction devraient être informés immédiatement.
- Informer le service juridique pour qu'il décide si les services policiers doivent être demandés et si les clients doivent être informés.
- Si les clients et les usagers sont touchés, ils devraient en être informés promptement. Il y a exigence de notification en vertu des lois fédérales et provinciales dans certains cas.
- Il est probable que l'incident puisse faire les manchettes. Il est préférable alors de contacter les médias sélectionnés de façon proactive.

Plusieurs entreprises sont réticentes à admettre une intrusion. Cependant, si les données de clients ont été volées, il est important d'être transparent à cet égard. Bien que l'événement comporte un effet négatif, si et lorsque l'intrusion est finalement révélée, l'effet devient alors doublement négatif : non seulement y a-t-il eu intrusion, mais l'entreprise a tenté de la camoufler.

Selon le fournisseur de protection des données Digital Guardian, vous devriez faire appel aux tactiques suivantes pour divulguer publiquement l'information :

- Si cela convient, admettez l'erreur. Dans tous les cas, assumez la responsabilité de sécuriser votre réseau et les données. Promettez de faire tout ce qui est possible pour atténuer les dommages pour les personnes et clients touchés.
- Précisez les détails sur ce qui s'est passé et, si possible, la raison et la façon dont s'est produite l'intrusion.
- Décrivez explicitement les solutions possibles et les mesures d'atténuation aux personnes et entreprises touchées. Si possible, offrez du soutien ou des services spéciaux. Par exemple, lorsque des données de clients sont volées, les entreprises offrent parfois une année de services de protection d'identité sans frais. Préparez les réponses aux questions fréquemment posées par les personnes ou entreprises touchées ; affectez une équipe pour répondre aux préoccupations dans les meilleurs délais via les canaux de communication.
- Dirigez les discussions. Impliquez des clients ou des utilisateurs, des experts du secteur, des analystes et les médias relativement à des sujets d'une portée plus étendue, traitant de l'horizon des menaces et de la manière dont les entreprises devraient faire face aux défis. [20]

Assurez-vous de vous conformer aux lois fédérales et provinciales, particulièrement en informant les personnes appropriées en cas d'intrusion.

Une fois que la vulnérabilité aura été réparée et que les systèmes redeviendront opérationnels, voici les autres étapes à suivre au cours de la période de calme après la tempête.

4. Procéder à une analyse rétrospective.

Trois éléments doivent être analysés :

- La cause de l'intrusion
- Le plan de réaction à l'incident
- Le plan de communication

La cause de l'intrusion. L'analyse judiciaire devrait avoir permis de découvrir la mécanique de l'attaque, la vulnérabilité exploitée et les dommages subis.

Le plan de réaction à l'incident. Le plan a-t-il été efficace ? Y a-t-il eu des circonstances imprévues qui n'ont pas été prises en compte ? Les responsabilités et les rôles avaient-ils été clairement définis ? Les résultats attendus du plan étaient-ils atteignables ? Le plan peut être modifié en fonction de ce qu'aura appris l'entreprise suite à l'intrusion. S'il n'y avait pas de plan de réaction en place, l'incident peut servir à générer un cadre de travail pour sa rédaction, tout en convenant qu'il devra être modifié régulièrement.

Le plan de communication. Toutes les entreprises et tous les organismes devraient avoir un plan de communication en place pour s'assurer que l'information puisse être diffusée rapidement, efficacement et dans sa totalité. Si vous possédez un tel plan, évaluez à quel point il a été suivi et, le cas échéant, s'il s'est avéré efficace. Procédez à des ajustements au besoin. Si vous n'aviez pas de plan de communication avant l'intrusion, cette analyse rétrospective peut vous aider à en rédiger un. Si l'intrusion a été dévoilée au public, les réactions des médias et du public devraient être analysées.

Le service de surveillance en sécurité Threat Stack conseille de faire en sorte que les analyses rétrospectives de sécurité soient exemptes de « blâmes », en s'assurant qu'il soit clairement compris que des individus ne sont jamais pointés comme étant à l'origine d'une intrusion. Si un membre du personnel est blâmé pour un incident, tout le monde au sein de l'entreprise deviendra moins enclin à faire rapport d'incidents suspects ou de possibilités que la sécurité soit compromise. L'analyse rétrospective devrait être axée sur la raison pour laquelle quelque chose s'est produit, et sur la façon d'éviter toute récidive à l'avenir. 21

5. Préciser les futures mesures de prévention.

L'analyse rétrospective peut révéler des failles de la sécurité, des processus ou au sein du personnel, failles qui devraient être prises en compte. Accordez-leur la priorité selon le degré de risque qu'elles constituent pour votre entreprise.

Qualys, un fournisseur de services de sécurité en infonuagique, affirme que les facteurs suivants devraient servir à l'établissement des priorités en ce qui concerne les risques liés aux biens des TI :

- L'importance du rôle qu'ils ont en ce qui a trait aux opérations essentielles de l'entreprise.
- Leur niveau d'interconnectivité avec d'autres biens propres à votre environnement des TI.
- Le niveau d'exposition à Internet par le truchement du web et des applications mobiles.
- L'ampleur et la nature de la base de leurs utilisateurs. 22

Déterminez l'atténuation la meilleure pour chaque mesure. Rédigez un plan ainsi qu'un échéancier de travail pour l'établissement de cette liste de priorités. Ceci peut impliquer des prévisions budgétaires pour des appareils, des logiciels et des services. Désignez une personne responsable de la gestion de ce processus ou faites appel à un fournisseur.

6. Compléter le protocole de rapport.

Les résultats de l'enquête devraient être rapportés à toutes les parties prenantes au sein de l'entreprise. Les vulnérabilités du réseau devraient être examinées, de même que le plan et l'échéancier pour atténuer ces vulnérabilités. Si l'intrusion ou l'entreprise est assujettie aux règlements régissant les rapports d'incident, révisez ces exigences pour voir si elles ont été respectées.

Lorsque l'intrusion est d'origine interne.

Bien que nous croyions que les cyberattaques proviennent de l'extérieur, il y a une autre forme d'attaque qui s'avère tout aussi pernicieuse : le vol de données par un membre du personnel. Un membre du personnel n'a pas à s'introduire par effraction sur le réseau ou dans les systèmes ; il lui suffit d'insérer une clé USB dans un des ordinateurs de l'entreprise et de copier les fichiers.

Il est fréquent qu'un membre du personnel s'empare de matériel de propriété intellectuelle alors qu'il est embauché par une entreprise concurrente ou qu'il démarre sa propre entreprise. Dans un tel cas, les analyses judiciaires peuvent découvrir le vol et fournir des preuves solides qui peuvent servir en cour.

Selon D4, la solution du Groupe Adecco Special Counsel's eDiscovery destinée aux entreprises, l'entreprise devrait impliquer un large échantillonnage de membres du personnel interne, qu'une entreprise d'analyse judiciaire prenne ou non en charge l'enquête.

Gestionnaires

Le gestionnaire du membre du personnel est souvent la première personne à constater le vol allégué de données ou de renseignements ; il se doit alors d'en faire rapport immédiatement en respectant le protocole en place. Selon D4, le gestionnaire devrait décrire les tâches et responsabilités du membre du personnel concerné, et préciser le déroulement des événements. 23

Ressources humaines

Dans certaines entreprises, le service des ressources humaines assume la responsabilité de la conduite des enquêtes internes, ou ce service peut agir comme principal point de contact pour les enquêteurs judiciaires externes. Ce service doit agir de façon à éventuellement faire face à une contestation judiciaire de la part du membre du personnel concerné tout en respectant la confidentialité de ses renseignements personnels et de l'enquête elle-même.

Consultation interne ou externe

Les représentants juridiques de l'entreprise doivent être informés de façon à ce qu'ils puissent décider, en s'appuyant sur les preuves découvertes, s'il y a lieu de procéder à une poursuite en justice ou déterminer la façon de procéder. Par exemple, la preuve du vol de matériel de propriété intellectuelle ou de secrets commerciaux peut être à ce point solide qu'elle justifie une ordonnance d'injonction temporaire.

IT

Le personnel du groupe des technologies de l'information fournit aux enquêteurs une description claire des systèmes d'information de l'entreprise, incluant les services de courriels, les réseaux, les appareils mobiles, les données d'infonuagique, l'utilisation de médias externes et les appareils fournis par l'entreprise et leur utilisation. L'équipe des TI doit s'assurer de la sauvegarde protégée des preuves numériques, incluant les mégadonnées.

Tous ces groupes doivent collaborer les uns avec les autres, de même qu'avec les analystes judiciaires, de façon à assurer une enquête menée de façon rigoureuse et exhaustive qui puisse tenir en cour tout en protégeant les intérêts de l'entreprise. [23]

Renforcement du réseau

Comme on a pu le constater par le haut niveau des cyberattaques de l'année dernière, pratiquement n'importe quoi peut permettre l'accès par des criminels ambitieux. Une entreprise ne peut pas sécuriser tous les magnétoscopes numériques, les clés USB ou les systèmes de chauffage, de ventilation et de climatisation du monde entier. Ce qu'elle peut cependant faire, c'est d'adhérer à des normes et à des pratiques exemplaires de sécurité.

Au moment de la reprise suite à une intrusion de sécurité et avant même de procéder à toute mise à niveau importante de cybersécurité, examinez les mesures en place de sécurité réseau et procédez aux modifications qui s'imposent.

Antivirus

Des applications d'antivirus devraient être installées pour protéger le réseau, et ce, au niveau de ses trois couches : au niveau des périphériques, du serveur et des clients, ce qui peut inclure non seulement les ordinateurs de bureau, mais aussi les appareils mobiles fournis par l'entreprise, ainsi que les appareils personnels.

Au niveau des périphériques, tous les points d'accès possibles devraient être précisés et sécurisés. Ceci peut inclure une infrastructure connectée, ou des appareils ou dispositifs tels que des thermostats intelligents. Tout le trafic accédant au réseau par ces points d'accès devrait être acheminé au moyen d'une application de passerelle munie d'un antivirus.

Au niveau du serveur, une pratique exemplaire consiste en l'installation d'un logiciel antivirus sur chaque serveur, et à l'interne, tant au niveau client (ordinateur de bureau) qu'au niveau du serveur.

Pour s'assurer que la protection antivirus est active et qu'elle demeure à jour, un serveur central antivirus devrait être utilisé pour configurer et procéder au balayage des serveurs et des postes clients. Lorsque possible, installez des produits antivirus propres à chaque application.

Les programmes d'antivirus devraient continuellement être mis à jour par le fournisseur du logiciel ou le fournisseur de service. Les serveurs et les postes de travail devraient être l'objet d'un balayage quotidien, au moment le moins susceptible d'interférer avec les opérations ou l'utilisation.

Appareils et logiciels

Si un appareil ou un logiciel de l'entreprise a atteint la fin de son cycle de vie ou s'il n'est plus l'objet d'un soutien technique, il devrait être mis à niveau.

Un logiciel devrait être mis à jour et tout correctif devrait y être appliqué régulièrement ; idéalement, les correctifs devraient être appliqués dès qu'ils deviennent disponibles. Pour vous assurer de mises à jour efficaces d'un logiciel, vous devez avoir les trois possibilités suivantes :

1. Procéder au balayage du réseau pour y déceler tous les appareils connectés et vérifier l'état de leurs systèmes d'exploitation et de leurs logiciels.
2. Détecter l'état actuel des correctifs de toutes les applications.
3. Obtenir, configurer et appliquer les correctifs logiciels en évitant tout conflit.

Profitez des mises à jour automatiques offertes par les fournisseurs des logiciels. Un service ou une solution de gestion des correctifs peut assurer le maintien à jour des logiciels.

Application de liste blanche

Cette pratique aide à prémunir les systèmes informatiques contre les logiciels malveillants en interdisant l'accès à toute application qui n'a pas été préalablement spécialement approuvée par son inscription à la liste blanche. Le logiciel de liste blanche vérifie automatiquement si les nouvelles applications qui accèdent au système figurent à la liste blanche ; si elles n'y figurent pas, l'accès est refusé. Cette approche est plus sécuritaire que celle des applications de liste noire. Cependant, ceci exige de la part de l'utilisateur une étape additionnelle qui consiste à demander que l'application soit ajoutée à la liste blanche.

Renforcement de l'entreprise

L'analyse rétrospective peut déceler des failles dans les politiques et les processus de l'entreprise, de même qu'au sein du personnel.

Deborah Hurley, professeure agrégée et directrice de la cybersécurité, est d'avis que la diversité des disciplines en cybersécurité est un facteur tout aussi important que la diversité des genres et de l'ethnicité. La gestion, le service juridique, le service de la conformité, le service des ressources humaines et le service des communications doivent contribuer et collaborer en ce qui concerne la sécurité. La sécurité affecte toutes les composantes de l'entreprise et devrait être partie intégrante de toutes les composantes. [24]

« Le but devrait être de créer une culture de sécurité », selon Andrea M. Matwyshyn, professeur de droit et des sciences de l'informatique à l'Université Northeastern. *« La sécurité devrait être diffusée du sommet à la base comme étant une partie fondamentale de l'entreprise »* selon cette dernière. [25]

Selon Mme Matwyshyn, « la réaction de sécurité n'exige rien de moins qu'un effort du sommet vers la base de la part de la haute direction ; la sécurité étant traitée comme pièce fondamentale des structures internes de l'entreprise, parce que la sécurité de l'information n'a de force que celle de son plus faible maillon. » Elle est d'avis que les entreprises doivent avoir un chef de la sécurité investi de suffisamment de pouvoirs et de capital social pour lui permettre d'articuler les besoins en matière de personnel, de formation et d'autres types d'investissement.

Cette culture de sécurité devrait s'étendre à l'ensemble de la main d'œuvre. Tous les membres du personnel devraient être informés des risques encourus par l'entreprise, des raisons de la mise en place de fonctions individuelles de sécurité, des pratiques exemplaires et des exploitations communes telles que l'hameçonnage.

Officier principal de la sécurité de l'information (OPSI) : Toutes les entreprises n'ont pas nécessairement un officier principal de la sécurité de l'information désigné. Chez plusieurs d'entre elles, le directeur de l'informatique (DI) ou le dirigeant principal de la Technologie (DPT) assume la responsabilité de la cybersécurité. Un OPSI assume la responsabilité de la conception et de la mise en œuvre d'un programme infosec. Membre de l'équipe de la haute direction, l'OPSI est un pair en mesure d'informer et de persuader d'autres membres de la haute direction de l'importance de la cybersécurité et des meilleures manières de l'assurer.

Directeur ou gestionnaire de la sécurité : Dans des entreprises sans OPSI, le directeur ou gestionnaire de la sécurité est la personne qui dirige le développement et la mise en œuvre de la sécurité. Cette personne devrait posséder la même expérience technique qu'un OPSI. De plus, il est important que le directeur ou le gestionnaire de la sécurité ait un accès direct à tous les membres de la haute direction.

Architecte en sécurité : L'architecte conçoit les systèmes définis par l'OPSI ou par le directeur ou gestionnaire de la sécurité.

Ingénieur en sécurité : Les ingénieurs en sécurité mettent en œuvre les systèmes et les concepts de sécurité de l'architecte en sécurité. Leurs tâches incluent les mises à niveau, les tests et l'application des correctifs des systèmes de sécurité. Ils assument de plus la responsabilité de la maintenance et des tests à intervalles réguliers. Ces membres du personnel sont les acteurs de première ligne de la sécurité quotidienne d'une entreprise.

Analyste de la sécurité : Un analyste de la sécurité rédige les politiques pour l'entreprise qui sauront le mieux la protéger contre les menaces et les risques, puis évalue si les mesures en place sont conformes aux politiques de sécurité. L'analyste doit déceler les nouvelles menaces au fur et à mesure qu'elles se présentent, tout en évaluant si les mesures de sécurité demeurent adéquates. L'analyste fait régulièrement rapport du rendement des systèmes de sécurité. L'analyste peut aussi formuler des recommandations relativement aux méthodologies et aux produits de sécurité.

Gestionnaire des systèmes : La gestion des comptes, des mots de passe et de l'accès aux ressources des TI fait partie des responsabilités des gestionnaires des systèmes, faisant de ces derniers d'importants collaborateurs au sein de l'équipe de sécurité. Ils assurent aussi la maintenance de la protection antivirus, des coupe-feu et des applications des listes blanches et des listes noires.

Comment l'innovation modifiera la formation et le rôle des professionnels de la sécurité

Cybersecurity Ventures prédit une pénurie estimée à 1,5 million de professionnels de la sécurité d'ici 2021, alors qu'un million de postes étaient à pourvoir en 2016. 26 Pendant ce temps, le travail des professionnels de la cybersécurité a changé et continuera à changer au cours des quatre prochaines années et des autres années à venir.

La National Initiative for Cybersecurity Careers and Studies du Département de la Sécurité intérieure des États-Unis repère de nouveaux types d'emplois et offre de la formation et une certification pour pourvoir ces postes. Par exemple, un chercheur en renseignements sur les menaces en cybersécurité qui met en place des « trous noirs » et des « pots de miel » ; il fait appel à une variété d'outils pour tester et évaluer les logiciels malveillants, et pourchasse les responsables des attaques. 27

L'intelligence artificielle et l'apprentissage machine sont peut-être les technologies les plus transformatrices de la prochaine décennie. L'IA s'imposera comme principal différentiateur pour les entreprises, offrant des améliorations des processus ou effectuant des tâches jusque-là impossibles à réaliser. 28

L'efficacité et la puissance de calcul considérable de l'intelligence artificielle seront inévitablement harnachées par les criminels. Selon Harvard Business Review, les cyberattaques propulsées par l'intelligence artificielle porteront le piratage à un niveau désespérant. 29 En fait, les systèmes d'intelligence artificielle eux-mêmes seront susceptibles d'être piratés, voyant leur raison d'être initiale corrompue et servant à réaliser des prouesses encore plus sophistiquées.

Les entreprises qui visent à utiliser l'intelligence artificielle de façon concurrentielle devront embaucher des experts capables de développer des façons d'assurer que l'intelligence artificielle agisse dans les intérêts supérieurs de leur propriétaire et qu'elle soit protégée contre les intrusions ou l'exploitation malveillante. 30

Or, l'intelligence peut aussi servir à améliorer la cybersécurité. Par exemple, un système d'intelligence artificielle peut vérifier de façon ininterrompue tous les systèmes d'une entreprise à la recherche d'intrusions, déceler les signes d'alerte de menaces internes et surveiller constamment les manquements aux politiques de sécurité. Des experts devront concevoir, mettre en œuvre et gérer ces systèmes de sécurité super-intelligents.

Préparez-vous aujourd'hui en vue de la cybersécurité de demain

En raison de l'explosion des appareils connectés et de l'expansion constante de l'Internet des objets, la surface d'attaque pour toute entreprise continuera elle aussi son expansion. Concurremment, de nouvelles technologies telles que l'intelligence artificielle exigeront de nouvelles capacités de la part de l'entreprise – ainsi qu'une nouvelle expertise.

Les entreprises doivent convenir qu'il n'est plus possible de mettre en place des mesures de sécurité, puis de simplement en assurer la maintenance. Les pratiques et les produits de sécurité doivent constamment être mis à jour, évalués et améliorés sous la direction d'experts du domaine.

Chez Modis, nous pouvons être votre partenaire pour cerner les écarts de compétences au sein du personnel de cybersécurité en place, préciser de nouvelles responsabilités et de nouveaux rôles, et procéder à l'embauche de talents exceptionnels et expérimentés en TI pour vous permettre de réaliser votre stratégie des TI. Pour en savoir davantage ou pour obtenir de l'information plus détaillée concernant les échelles de salaires, les descriptions de postes et la demande du marché, n'hésitez pas à communiquer dès aujourd'hui avec le représentant Modis de votre localité.

Sources

1. http://cybersecurityventures.com/cybersecurity-market-report/
2. http://opim.wharton.upenn.edu/risk/downloads/WEF_Global-Risks_2017.pdf
3. https://ww2.frost.com/news/frost-commentary/cybersecurity-aftermath-ransomware-attack-what-lies-ahead/
4. http://www.pandasecurity.com/mediacenter/malware/adylkuzz-new-virus-wannacry/
5. http://www.bbc.com/news/technology-40428967
6. https://www.globalsecuritymag.com/WannaCry-What-s-Next-expert,20170518,71206.html
7. http://www.gao.gov/highrisk/overview
8. https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal
9. http://www.eweek.com/enterprise-apps/businesses-keep-clinging-to-windows-7-and-xp
10. http://analysis.tu-auto.com/telematics/can-you-hack-it-securing-connected-car
11. https://www.wired.com/2017/02/hacked-android-phones-unlock-millions-cars/
12. http://www.techrepublic.com/article/4-questions-businesses-should-be-asking-about-cybersecurity-attacks/
13. http://www.cnbc.com/2017/05/19/new-hacking-threats-fingerprint-vulnerabilities-and-sophisticated-ransomware.html
14. https://ioactive.com/pdfs/IOActive_HackingCitiesPaper_cyber-security_CesarCerrudo.pdf
15. https://blog.surfwatchlabs.com/2016/09/08/short-selling-vulnerabilities-latest-in-string-of-stock-market-manipulation/
16. https://medium.com/@RPublicService/feds-at-work-bringing-cybercriminals-to-justice-7dfe5d7a5920
17. https://www.gartner.com/smarterwithgartner/prepare-for-the-inevitable-security-incident/
18. https://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf
19. https://digitalguardian.com/blog/data-breach-experts-share-most-important-next-step-you-should-take-after-data-breach-2014-2015
20. https://digitalguardian.com/blog/data-breach-experts-share-most-important-next-step-you-should-take-after-data-breach-2014-2015
21. https://blog.threatstack.com/how-to-conduct-a-blameless-security-post-mortem
22. https://blog.qualys.com/news/2017/01/17/overwhelmed-by-security-vulnerabilities-heres-how-to-prioritize
23. http://d4discovery.com/discover-more/involved-with-conducting-corporate-investigations
24. https://www.forbes.com/sites/ciocentral/2017/05/07/improving-cybersecurity-the-diversity-imperative/#639ce3571e30
25. http://knowledge.wharton.upenn.edu/article/massive-global-cyberattack/?
26. http://cybersecurityventures.com/jobs/
27. https://niccs.us-cert.gov/training/search/cybertraining-365/certified-cyber-threat-intelligence-analyst
28. Menalto Advisors, Menalto Advisors Thought Report: Artificial Intelligence and Machine Learning.
29. https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse
30. http://www.businessinsider.com/deepmind-has-hired-a-group-of-ai-safety-experts-2016-11