Stimuler le système cyberimmunitaire de votre organisation

L'heure est venue d'imaginer la cybersécurité différemment

Un livre blanc de Bell

Voilà le programme

Avec les cybermenaces qui évoluent toujours plus rapidement et les pirates devenant de plus en plus sophistiqués, les organisations chercheront continuellement à améliorer leur sécurité. Cependant, on ne peut suivre le rythme des pirates qu'en abordant le problème d'une manière différente. Ce livre blanc décrit à quel point la cybersécurité ressemble à la manière dont le système immunitaire humain anticipe, détecte, s'adapte et se défend contre les menaces — permettant au corps de fonctionner à son meilleur niveau de performance. Tout comme le système immunitaire, dans le monde cybernétique, certains moments requièrent un effort communautaire coordonné pour se protéger contre les « flambées » de menaces massives. Les fournisseurs de services Internet sont idéalement positionnés pour jouer un rôle important dans cette défense communautaire.

Table des matières

Introduction

Menaces croissantes. Flux persistant de nouvelles vulnérabilités. Intensification des impacts sur les affaires. À mesure que les cyberattaques s'empirent et se diversifient, les organisations requièrent non seulement de nouveaux outils et de nouvelles techniques, mais aussi une nouvelle façon de penser à la cybersécurité. S'il existe un modèle à suivre parmi les systèmes bien réglés et très résilients, qui se défendent efficacement sans compromettre les fonctions de base, c'est bien le corps humain.

Sans le système immunitaire, nous pourrions tous devoir vivre dans une bulle en perpétuelle quarantaine pour nous protéger des maladies. Une telle approche nous maintiendrait peut-être en bonne santé, mais elle nous empêcherait sérieusement d'interagir et de profiter du monde. Il en va de même pour les réseaux : dans l'environnement d'exploitation actuel, une approche purement périmétrique de la défense consiste simplement à mettre en place des murs qui empêchent de faire des affaires en ligne et à forte consommation de données.

Le système immunitaire du corps humain adopte une approche différente : une approche dynamique et d'apprentissage. Quand il rencontre des menaces qu'il reconnaît, il réagit de manière connue pour les traiter. Quand il rencontre des menaces qui ne lui sont pas familières, c'est alors qu'il intensifie ses défenses — et du même coup, acquiert une connaissance de la façon dont la menace se comporte afin qu'il puisse prendre des mesures plus efficaces la prochaine fois.

Le corps s'affaire à maintenir sa condition physique aussi optimale que possible. L'activité d'une organisation consiste à effectuer ses opérations quotidiennes avec un maximum d'efficacité. Vue de cette façon, la sécurité est vraiment un problème commercial plutôt que purement technique. La solution consiste à adopter une vision holistique du réseau d'entreprise dans la réalisation de ses objectifs commerciaux et à profiter au mieux des investissements de sécurité existants : deux domaines dans lesquels un fournisseur de services Internet (FAI) peut jouer un rôle de partenaire clé.

Le contexte des menaces évolue

Même si la médecine moderne connaît des améliorations considérables, les virus et les maladies s'adaptent et évoluent constamment. Tel est l'environnement externe. Tout cela oblige le domaine médical à des améliorations continues. Il en va de même dans le paysage des cybermenaces, qui évolue de manière à compliquer de plus en plus le travail des organisations pour assurer leur sécurité (comme la virtualisation et l'infonuagique, accroître leur présence en ligne ou traiter des volumes de données explosives).

Les cinq tendances clés qui ont donné l'avantage aux pirates ces dernières années :

Surface d'attaque étendue

Alors qu'ils continuent à numériser leurs entreprises, les organisations transforment rapidement leurs infrastructures informatiques afin d'accroître leur agilité et leur productivité. Plus de terminaux et d'appareils, dont les anciens systèmes mal équipés pour gérer les menaces modernes, entrent et sortent du réseau de l'entreprise comme jamais auparavant. (En guise d'exemple, Gartner estime que 8,4 milliards d'appareils seront connectés à Internet d'ici la fin de 2017.[1]) Parallèlement, les plateformes mobiles et en nuage deviennent d'autant plus essentielles aux opérations quotidiennes. Cela procure aux pirates plus d'options pour l'infiltration et l'infection que jamais auparavant — et donne aux entreprises une surface d'attaque potentielle beaucoup plus grande à surveiller et à défendre.

Des attaques plus complexes

Auparavant, seuls les équipements Windows étaient vulnérables aux attaques. Aujourd'hui, il existe des logiciels malveillants efficaces pour macOS, Linux, Android et iOS. De plus, ils sont désormais conçus pour cibler spécifiquement les périphériques intégrés tels que les routeurs et les modems. Les logiciels malveillants ont également évolué pour échapper aux défenses traditionnelles, avec des pirates utilisant des exploits (codes malveillants, jusqu'alors inconnus, qui exploitent une faille de sécurité et ne sont jamais gravés sur le disque dur de la victime), ou encore des logiciels malveillants qui s'intègrent dans le micrologiciel d'un appareil, mais aussi les logiciels malveillants polymorphes qui changent ses caractéristiques chaque fois qu'ils s'exécutent.

Les pirates tiennent également à leur disposition une plus vaste gamme de méthodes d'attaque potentielles. Les organisations doivent se défendre contre les logiciels malveillants qui peuvent donner accès à leurs systèmes, les rançongiciels qui emprisonnent des fichiers et des données critiques à moins de payer le pirate, les attaques du jour zéro qui ciblent les vulnérabilités spécifiques auparavant inconnues des éditeurs de logiciels, les attaques de déni de service distribué (DDoS) qui détruisent les sites Web ou les services en ligne en les accablant avec une quantité massive de bande passante ainsi que les violations dans lesquelles les pirates volent des informations personnelles ou financières sensibles.

On peut mener ces attaques de différentes façons, notamment par hameçonnage (logiciels malveillants distribués par l'entremise de courriels qui semblent légitimes), logiciels de publicité malveillants (charges malveillantes injectées dans la publicité d'applications et de sites légitimes), ingénierie sociale (incitant les utilisateurs à effectuer des actions qui donnent aux pirates l'accès à des systèmes et actifs importants), etc.

À mesure que les attaques deviennent plus complexes, elles prennent également plus de temps à détecter et sont plus coûteuses à corriger. Le temps moyen pour identifier une attaque est de 99 jours[2] et le coût moyen par enregistrement de données volées au Canada est de 255 $[3].

[1]Campus Technology. Gartner: 2017 verra 8,4 milliards de « choses » connectées. Disponible en anglais sur: https://campustechnology.com/articles/2017/02/09/gartner-2017- will-see- 8.4-billion-connected-things.aspx

[2]FireEye. FireEye publie le rapport Mandiant M-Trends 2017. Disponible en anglais sur : http://investors.fireeye.com/releasedetail.cfm?ReleaseID=1017295

[3]Ponemon Institute, Étude de 2017 sur le coût des violations de données. Disponible en anglais sur : https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

Volume croissant d'attaque

Les attaques deviennent non seulement plus complexes, mais se produisent également en plus grand nombre, les pirates combinant souvent plusieurs vecteurs et techniques d'attaque pour infliger le plus de dommages possible. Le nombre d'attaques réussies a augmenté de 46 % au cours des quatre dernières années[4] (le nombre de violations de données signalées aux États-Unis s'est accru de 40 % en 2016 seulement[5]). De plus, les attaques deviennent plus importantes. Selon les données du réseau de Bell, l'attaque DDoS la plus importante a eu lieu au Canada à 202,5 Mb/s; l'attaque la plus longue a duré plus de 16 heures. Globalement, certaines attaques DDoS ont dépassé 1 Gbit/s avec la montée en puissance des zombies de l'IdO. Plus d'attaques engendrent plus de coûts : les dommages de rançongiciels ont atteint 5 milliards de dollars en 2017, soit 15 fois plus que deux ans plus tôt.

Les pirates sont mieux organisés

Les pirates d'aujourd'hui emploient des tactiques et des techniques évoluées, profitant d'une chaîne d'approvisionnement mature, riche en outils, services et infrastructures — comme le Dark Web — pour alimenter leur cybercriminalité et pour faciliter leurs opérations. Les pirates informatiques ont infiltré l'App Store d'Apple et le Google Play Store, par exemple, pour propager des logiciels malveillants dans un grand nombre d'applications et ont exploité les systèmes de points de vente pour faciliter les violations de données. Les mêmes tactiques utilisées par le crime à but lucratif sont également disponibles pour les « hacktivistes » qui ciblent les gouvernements ou les entreprises comme une forme de protestation.

Les attaques sont moins chères et plus faciles à exécuter

La grande disponibilité et le faible coût des outils de cybercriminalité encouragent les criminels à exploiter les données d'entreprise. Il existe maintenant des services d'abonnement où l'on peut louer des zombies DDoS ou payer quelqu'un pour lancer une attaque de bout en bout sur une cible de leur choix. À un coût de seulement quelques dollars par semaine, n'importe qui avec une carte de crédit et un motif peut rapidement et facilement lancer une attaque. Avec l'émergence du rançongiciel en tant que service (RaaS), les personnes sans compétences de programmation ou de codage ont accès à ce type d'attaque très efficace. Les cybercriminels créent le code malveillant et le mettent ensuite à la disposition des autres, souvent moyennant une petite commission ou en prélevant une partie de la rançon, ce qui, à son tour, encourage davantage d'attaques et de demandes de rançon plus élevées[6].

Cybercriminalité : Étude de cas

Un compte de carte de crédit volé peut être vendu sur le marché noir pour seulement 20 $. Si une violation rapporte 10 millions d'enregistrements, même à un prudent dollar pour chaque carte, cette attaque vaut potentiellement 10 millions de dollars.

Les criminels peuvent constituer un ensemble d'attaques robustes (c.-à-d. code source de logiciel malveillant, ensemble d'exploits, hébergement pare-balles, installations malveillantes, exploits du jour zéro) pour moins de 500 000 $. Cela équivaut à un retour sur investissement de l'ordre de 2 000 %.

L'augmentation du nombre de rançongiciels s'explique en partie par le fait qu'ils peuvent offrir un paiement beaucoup plus rapide que le vol de données de carte de crédit — avec un risque beaucoup plus faible d'être pris en raison de l'anonymat lié à l'échange en Bitcoin.

Visitez notre blogue pour en savoir plus sur ce que vos données pourraient valoir pour les cybercriminels.

Peu importe la façon dont elles sont perpétrées, les cyberattaques peuvent être classées en deux grandes catégories : les attaques visibles et les tueurs silencieux.

Comme le rhume, on peut aisément déceler les attaques visibles telles que les attaques DDoS, les tentatives d'hameçonnage et autres. En revanche, d'autres attaques ressemblent plus à des maladies cardiaques et des cancers : des attaques multiétapes et multivecteurs qui passent inaperçues pendant de longues périodes avant de devenir fatales. Parmi ces tueurs silencieux, on compte les violations stratégiques et les menaces persistantes

[4] Forbes. Un cybercrime « moyen » coûte 15,4 millions de dollars à une entreprise des États-Unis. Disponible en anglais sur : www.forbes.com/sites/moneybuilder/2015/10/17/an-average-cyber-crime-costs-a-u-s-company-15-4-million/#5dd7996032cb

[5] Cision PR Newswire. Selon le rapport de Identity Theft Resource Center and CyberScout, les violations de données ont augmenté de 40 % en 2016. Disponible en anglais sur : https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html

[6] Forbes. Le rançongiciel-service : la prochaine grande cybermenace? Disponible en anglais sur : www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat

avancées — conçues pour rester dans le système ciblé à long terme afin de faciliter l'accès aux données — et l'exfiltration. La défense contre ces attaques exige une diligence inébranlable en matière de détection et de suppression précoces, ce que les méthodes traditionnelles de sécurité informatique ne sont pas en mesure de procurer.

La difficulté de préserver sa cybersanté

Lorsque vous entrez dans une pièce où les gens toussent — disons dans la salle d'attente d'une clinique sans rendez-vous — vous éviterez probablement de toucher trop de surfaces communes et vous vous laverez les mains régulièrement pour éviter de tomber malade. Guidé par vos instincts de conservation, vous anticipez les menaces potentielles et agissez de façon à les minimiser.

Voilà un autre parallèle avec la cybersécurité consistant à maintenir une solide position de sécurité. Pourtant, beaucoup d'organisations affaiblissent cette position par inadvertance lorsqu'elles s'empressent de transformer leurs infrastructures informatiques et déplacent une plus grande partie de leurs activités vers le nuage.

Chaque nouveau système et nouvelle application introduits sur le réseau de l'entreprise augmentent le risque de voir ses vulnérabilités au jour zéro exploitées. Les anciennes technologies autonomes comme les réseaux de système d'acquisition et de contrôle des données (SCADA) qui exploitent des centrales électriques et autres infrastructures critiques deviennent soudainement vulnérables lorsqu'elles se connectent à Internet pour la première fois. Elles manquent simplement de défenses contre les menaces qui accompagnent la connectivité au réseau public. Et avec l'adoption continuelle du nuage et de l'informatique mobile, les informations historiquement protégées dans le périmètre de l'entreprise sont désormais diffusées sur plusieurs sites.

Dans ce contexte, les organisations sont confrontées à deux défis majeurs lorsqu'il s'agit de protéger leurs données :

1. Un manque de conscience de la situation

Tout comme en santé publique, où les organismes surveillent les tendances de la maladie et les données au niveau de la population pour identifier les épidémies potentielles ou les « points chauds » de l'activité de la maladie, les organisations doivent comprendre le contexte de menace dans lequel elles évoluent. Aujourd'hui, plusieurs sont confrontées à des menaces numériques à leur insu et sans en apprécier les conséquences potentielles, jusqu'à ce qu'il soit trop tard. Malheureusement, plusieurs manquent de ressources ou de capacités pour constamment surveiller et agir sur les menaces potentielles.

2. Rester à l'affût de la « course aux armements »

Malgré les investissements et les mises à jour continuels dans leur infrastructure défensive, plusieurs organisations n'arrivent pas toujours à suivre l'évolution rapide de l'environnement informatique. L'introduction d'une nouvelle application de productivité, de services en nuage ou de portail client implique des investissements dans de nouvelles solutions de sécurité. Voilà qui complexifie l'infrastructure informatique et accroît l'exposition et les vulnérabilités potentiellement exploitables par les pirates.

Dans d'autres cas, les entreprises sont confrontées à des cycles d'actualisation du matériel fréquents, ont du mal à maintenir une équipe adéquate de professionnels qualifiés ou se voient imposer des coûts de licence élevés pour les technologies de sécurité, ce qui limite leur capacité d'effectuer les actualisations requises pour devancer les capacités des pirates. Les ressources que consacrent les organisations à suivre cette « course aux armements » le sont souvent aux dépens de leur mission principale.

Pour relever ces deux défis, les organisations devront commencer à se faire une idée globale de la manière dont elles protègent leur système immunitaire.

Adopter une approche holistique de la cyberimmunité

Comme les gens qui veulent rester en bonne santé préféreront éviter de fumer et de manger de la malbouffe plutôt que d'attendre pour traiter les symptômes d'une maladie à mesure qu'ils apparaissent, les organisations devraient adopter une approche holistique et préventive de la cybersanté.

Cela commence par la compréhension de l'environnement informatique de l'entreprise dans son ensemble. Parce qu'il devient de plus en plus difficile de protéger chaque partie de l'entreprise au plus haut niveau possible, il est souvent nécessaire de hiérarchiser les efforts de sécurité. Ainsi, les entreprises doivent évaluer où se situent leurs vulnérabilités et quelles parties de l'entreprise exigent le plus de protection. Autrement dit, elles doivent se concentrer sur le risque. Pour les entreprises, les risques les plus importants sont ceux qui visent le résultat net, la réputation de la marque et les relations avec la clientèle.

Évaluer le risque sous plusieurs angles

Les évaluations traditionnelles de risques liés à la sécurité informatique des entreprises adoptent le point de vue du défenseur : quelle est la menace? À quel point l'organisation est-elle vulnérable? Quel est l'impact commercial potentiel d'une violation? Cette évaluation permet de déterminer combien dépenser sur quels types de ressources pour bloquer un type d'attaque précis.

Mais dès que les types d'attaques et leur provenance se multiplient, cette approche ne suffit plus. Les évaluations doivent également considérer la perspective du pirate. Par exemple, en calculant le retour sur investissement potentiel du pirate, une organisation peut déterminer laquelle de ses données présente réellement une cible lucrative. Sachant combien ses données valent pour un pirate, l'entreprise peut mieux attribuer des ressources de sécurité pour protéger ses données les plus précieuses. Il s'agit d'imaginer le tout du point de vue d'un virus contagieux. Si vous cherchiez à infecter quelqu'un, comment pénétreriez-vous dans son corps? Et quels types de personnes seriez-vous le plus susceptible de cibler?

Dans le cadre du processus d'évaluation, les organisations doivent étudier scrupuleusement les forces et les faiblesses des différentes méthodes de protection et activer les leviers qui permettront à leur organisation de remplir au mieux sa mission et de gérer efficacement ses risques.

Les organisations doivent également examiner leur chaîne d'approvisionnement pour identifier les partenaires qui peuvent les aider à renforcer leur position de sécurité — et tous ceux qui pourraient présenter un risque de la compromettre.

Obtenir la visibilité et l'information pour prévoir et prévenir les menaces

L'approche globale consiste en partie à adopter une vision systématique de la cybersécurité, et donc à envisager la sécurité autrement que comme un simple pare-feu ou tout autre appareil de sécurité. Il faut plutôt appréhender comment la sécurité peut permettre à l'organisation d'assurer son cœur de métier, tout en minimisant les risques. Quelles approches pourraient procurer une protection optimale? Qu'est-ce qui aura le moins d'impact négatif sur les principaux objectifs commerciaux de l'organisation — ou même aidera l'organisation à faciliter sa mission principale synergiquement?

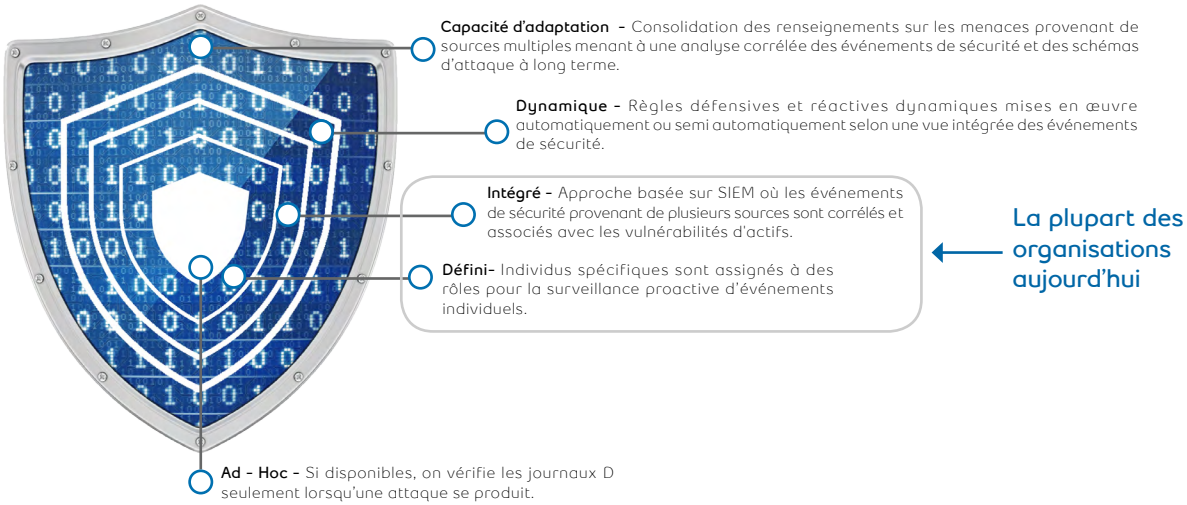
Les entreprises peuvent y parvenir en améliorant leur connaissance de la situation et de la visibilité sur les attaques potentielles ainsi qu'en formant le personnel à reconnaître et à éviter les risques de cybersécurité (par exemple, en utilisant un protocole de courriel et de mot de passe approprié pour réduire le risque d'hameçonnage et autres attaques courantes).

Pour mieux anticiper les menaces, les entreprises doivent exploiter la puissance de leurs réseaux d'approvisionnement plutôt que de se fier uniquement à leurs propres moyens de défense. En s'appuyant sur les renseignements provenant de l'ensemble de leur région, de leur industrie et de plusieurs autres sources, ils peuvent identifier plus rapidement les menaces émergentes et mieux cibler leurs défenses.

L'Organisation mondiale de la santé (OMS) a utilisé ce même principe pour établir un modèle pour ce qu'elle appelle « la coopération communautaire en matière de santé ». L'OMS recueille des données auprès des membres du monde entier et utilise sa perspective mondiale pour identifier les épidémies, les pathogènes agressifs, les substances cancérigènes et autres dangers pour la santé, dans le but de devancer les risques sanitaires émergents. Et lorsqu'adviennent des épidémies sévères, cela permet d'analyser les échantillons du Patient Zéro — l'origine de l'infection — pour accélérer le développement du vaccin.

Mieux comprendre les risques potentiels permet aux organisations d'aller au-delà des approches purement réactives pour se concentrer sur la prévention et arrêter les attaques avant qu'elles ne surviennent. La plupart des organisations n'en sont pas encore là — mais en adoptant des techniques comme la cyber analytique haut de gamme, ils seront en mesure de tirer parti des informations recueillies sur leurs réseaux pour détecter les menaces plus tôt et avec plus de précision. De tels outils continueront d'évoluer pour intégrer des mesures plus proactives et prédictives, permettant de mettre en place les mesures défensives les plus appropriées, le cas échéant.

Figure 1. Modèle de maturité de la connaissance de la situation



L'approche Bell

Tout comme l'OMS assure la protection et la promotion de la santé publique à l'échelle mondiale, les FAI et les opérateurs de télécommunications comme Bell sont idéalement positionnés pour jouer un rôle similaire dans le cyberespace. Ils voient la macro-activité de l'ensemble de leur réseau. Ils sont en mesure d'identifier les modèles, de mettre en œuvre des mesures préventives et de promouvoir des pratiques qui favorisent la bonne santé du réseau. Les solutions de sécurité du réseau hébergées par les opérateurs offrent généralement des niveaux d'évolutivité et de flexibilité qui dépassent les capacités des entreprises individuelles et peuvent être pourvues de manière rentable.

Bell pousse l'approche encore plus loin grâce à son approche très proactive de la sécurité, qui offre un certain nombre d'avantages distincts aux clients avec ses diverses solutions de sécurité réseau :

Meilleure visibilité et connaissance de la situation

Bell opère la majeure partie du volume de trafic Internet du Canada — plus de 10 pétaoctets de trafic chaque jour — et touche 99 % des particuliers et des entreprises. Cela procure à Bell une vue privilégiée sur le trafic Internet circulant dans les réseaux publics. Grce à l'accès à une telle quantité d'informations, Bell peut détecter les modèles de trafic anormaux avant tout le monde et arrêter les paquets malveillants avant qu'ils puissent atteindre les réseaux des clients.

Bell maintient également des mesures de sécurité avancées et de grande capacité (comme la détection des anomalies et les « pots de miel ») dans l'ensemble de son réseau national et aux points de liaison avec d'autres entreprises afin d'identifier et de comprendre les menaces émergentes. Combinant la connaissance de la situation interne et externe à la surveillance et à la corrélation 24/7 des événements de sécurité, l'analyse des logiciels malveillants et une vaste collaboration avec l'industrie et les organisations gouvernementales, Bell peut détecter les vulnérabilités et les menaces qui ne sont tout simplement pas visibles pour la plupart des entreprises avec les outils et les informations limitées qui sont à leur disposition aujourd'hui.

Observer le trafic Internet canadien à la loupe

Bell utilise ce que l'on appelle le renseignement sur les menaces cybernétiques (RMC) pour analyser les données provenant d'un certain nombre de sources différentes et créer des informations de sécurité informatique exploitables pour ses clients. Grâce à sa plateforme RMC, Bell met en corrélation les flux provenant de plus de 150 sources de données à travers son propre réseau national, ses clients, ses partenariats industriels, ses principaux fournisseurs de sécurité, les gouvernements et la communauté de la sécurité mondiale. Elle utilise ensuite l'automatisation, l'apprentissage automatique, l'intelligence artificielle, la détection d'anomalies et autres techniques pour agréger et analyser ce vaste ensemble d'informations sur les cybermenaces.

En plus de permettre la détection précoce des menaces, la plateforme RMC :

- Favorise une meilleure compréhension de l'environnement des menaces d'une organisation (par exemple en fournissant un contexte dans lequel les menaces sont ciblées et de nature plus opportuniste), lui permettant de prendre des décisions de gestion des risques mieux informées et d'optimiser ses investissements sécuritaires
- Permet des comparaisons transversales et sectorielles
- Procure la capacité de recréer rapidement la chronologie précise d'une faille de sécurité, en réduisant le temps et le coût de la récupération et en veillant à ce qu'aucune zone résiduelle ne soit omise

Lorsqu'émergent de nouveaux « pathogènes » agressifs, nous voulons identifier rapidement la victime initiale, analyser la source de l'infection et synthétiser un « vaccin » efficace pour inoculer la communauté – autrement dit, pour prodiguer la bonne réponse cybernétique.

Une réponse préventive et prédictive aux menaces

Les coûts et les efforts associés au maintien, au renouvellement et à la gestion de plusieurs niveaux de sécurité périmétrique — le modèle « classique » — peuvent être assez importants. Mais en profitant du modèle de sécurité préventive et prédictive d'un opérateur, les entreprises peuvent réduire leurs coûts et accroître leur efficacité tout en améliorant leur sécurité globale.

Bell aide à fournir ce modèle en adoptant la première ligne de défense, offrant une approche approfondie de défense en profondeur qui consiste en trois couches de protection :

- **Périphérie du réseau :** La première ligne de défense se trouve aux points d'appairage du réseau de Bell. Bell exploite ici un certain nombre de fonctions de sécurité de base, notamment le filtrage du trafic à partir d'adresses IP signalées pour empêcher certains types d'attaques DDoS et le retrait du trafic à partir de sources signalées pour une réponse plus rapide aux attaques DDoS volumétriques. Bell neutralise également les grandes attaques DDoS ciblant des protocoles d'infrastructure réseau spécifiques (tels que NTP ou DNS), régit le trafic pour empêcher le circuit d'accès d'un client de devenir un point de transit pour le trafic malveillant, et surveille l'usurpation d'adresse IP (un vecteur commun pour les attaques DDoS).
- **Réseau :** En fournissant une passerelle vers Internet, Bell développe et intègre des services de sécurité dans le réseau. Grâce à son service Sécurité du réseau contre les attaques DDoS, par exemple, Bell inspecte le réseau lors de la circulation de trafic, à la recherche d'éventuelles attaques.
- **Chez le client :** En dernière ligne, la protection est assurée à la périphérie du réseau du client. Bell peut déployer et gérer de nombreuses fonctions technologiques, en profitant de la surveillance disponible 24 heures sur 24 et 7 jours sur 7 par l'intermédiaire de ses centres d'opérations de sécurité, ainsi que de sa gestion centralisée pour fournir des renseignements supplémentaires sur la prévention des menaces.

De plus, Bell élargit actuellement son portefeuille de services réseau pour fournir une protection clé en main aux clients d'affaires, en s'appuyant sur RMC pour obtenir des renseignements précieux sur les menaces émergentes. Par exemple, son approche « réseau-périmètre-en-service » offrira une protection complète, toujours en fonction et toujours à jour aux entreprises qui utilisent Bell comme passerelle vers Internet. À l'instar de l'OMS qui veille à la santé de la collectivité, Bell s'efforce de protéger les entreprises canadiennes contre les cybermenaces.

Bell travaille également à profiter des connaissances acquises lors de l'inspection des gros volumes de trafic traversant son réseau, en utilisant RMC pour détecter rapidement et éventuellement prédire les attaques avant qu'elles ne surviennent. Cette capacité permettra à toutes les organisations, pas seulement aux victimes d'une attaque, d'orchestrer proactivement les défenses pour contrer le vecteur d'attaque — en fin de compte, réduire le coût de l'infrastructure défensive.

Ensemble, ces trois éléments reflètent le système immunitaire du corps humain, comprenant un écosystème dans lequel chaque partie travaille ensemble pour protéger l'ensemble.

Conclusion

Les cyberattaques devenant de plus en plus fréquentes et complexes, les organisations doivent changer leur vision de la cybersécurité — loin des pare-feu et autres « solutions logicielles en boîte » et vers des solutions proposée par les FAI, offrant une visibilité et une connaissance de la situation plus grande face aux menaces potentielles. Ce faisant, il fournit les informations nécessaires pour prendre des décisions de sécurité plus intelligentes qui stimulent le « système immunitaire » de l'entreprise tout en permettant au trafic stratégique de circuler à travers le réseau de l'entreprise.

Bell est particulièrement bien placée pour offrir des renseignements en amont sur les menaces cybernétiques et la sécurité des réseaux qui peuvent simplifier les architectures défensives des entreprises et mettre plus de distance entre les acteurs malveillants et leurs actifs. Grâce à son réseau hautement disponible, à ses 27 centres de données sécurisés et à ses trois centres de lavage (« scrubbing ») au Canada, Bell peut tenir et réagir face aux menaces et aux attaques avec une rapidité et une ampleur que peu peuvent égaler. Appuyée par une équipe chevronnée d'experts en sécurité, Bell offre une expertise avancée en matière de détection, d'atténuation et de prévention des menaces aux entreprises du pays — avec une expérience de protection des banques, des gouvernements et d'autres industries réglementées exigeant les niveaux de sécurité les plus élevés.

Communiquez avec votre représentant commercial de Bell pour discuter des solutions de sécurité réseau qui pourraient convenir à votre entreprise ou visitez le site bell.ca/solutionssecurite pour en savoir plus.