Plus de menaces. Moins d'experts. Le déficit de compétences continue de se creuser. Comment allez-vous gérer ?

Face à une menace toujours plus présente, la pénurie mondiale de compétences en sécurité informatique ne fait que s'aggraver.

États, entreprises, individus… à tous les échelons de la pyramide, notre vulnérabilité croît de jour en jour. En cause ? Notre dépendance vis-à-vis des technologies, combinée à la sophistication, la fréquence et la mutation constante des cybermenaces. Si on les laisse agir, ces menaces gagneront en ampleur, en complexité et en furtivité. En parallèle, on assiste à l'avènement de nouvelles tendances, des services cloud à l'Internet des objets (IoT), en passant par les terminaux mobiles et le Big Data. Autant de phénomènes qui viennent dissoudre les frontières traditionnelles des réseaux, créant par là même de nouveaux défis pour la sécurité des utilisateurs, où qu'ils se trouvent. Mais pour relever ces défis, encore faut-il disposer d'effectifs qualifiés en nombre suffisant – un objectif difficile à atteindre en ces temps de pénurie de spécialistes dans le monde entier.

Évolution du cadre réglementaire

Faute de compétences suffisantes en interne, bon nombre d'entreprises ne peuvent plus gérer seules tous les aspects de leur sécurité informatique. Pour ne rien arranger, la machine du cybercrime, elle, ne s'arrête jamais. Avec l'éclosion de nouvelles techniques comme le « malware en SaaS », même l'aspirant cybercriminel lambda devient une menace de taille.

Hormis la fréquence et la complexité accrues des attaques, les RSSI doivent s'adapter au durcissement des réglementations partout dans le monde. Des réglementations qui appellent au renforcement des ressources et compétences dans le domaine la cybersécurité. Comme vous le savez sans doute, le Règlement Général sur la Protection des Données (RGPD) est entré en vigueur en mai 2018. Avec ce nouveau texte, l'UE entend asseoir un cadre plus strict en matière de protection des données, notamment par l'alourdissement des sanctions financières. Pour se mettre au diapason, l'Allemagne a pris les devants en promulguant sa nouvelle Loi fédérale sur la protection des données. De leur côté, la Chine et l'Australie resserrent également la vis : la première avec l'application d'une nouvelle loi de cybersécurité depuis le 1er juin 2017, la seconde avec l'adoption du « Privacy Amendment (Notifiable Data Breaches) Act 2017 », texte qui établit une obligation de notification des violations de données sous certaines conditions. Outre-Atlantique, les régulateurs ne sont pas en reste non plus. Une loi fédérale sur les violations de données pourrait en effet obliger les entreprises piratées à révéler l'intrusion dans les 30 jours en cas de vol potentiel de données personnelles.

Pour les équipes de sécurité interne, une chose est sûre : l'année 2019 et les suivantes promettent d'apporter leur lot de difficultés en termes d'effectifs, de respect des obligations réglementaires, de gestion de l'IoT, et de lutte contre la cybercriminalité.

En 2015, 62 % des entreprises faisaient état d'une pénurie de professionnels de la cybersécurité. En 2017, elles sont 66 %.

Besoin de compétences élargies

Aujourd'hui, les entreprises doivent affronter des défis sécuritaires qui n'existaient pas l'année dernière, et encore moins il y a dix ans. Alors que le cybercrime se structure et se professionnalise, les entreprises butent chaque jour sur de nouvelles problématiques. Selon les prévisions du Gartner[1], l'IoT représentera plus de 20,4 milliards d'appareils connectés d'ici à 2020 – soit autant de nouveaux défis de sécurité à relever. Quant au rapport NTT 2016 sur l'état des menaces dans le monde, il constate que les entreprises ne se protègent toujours pas contre des vulnérabilités et menaces existantes – et encore moins contre les nouveaux schémas d'attaques sophistiquées.

La vitesse constitue l'autre grand défi des équipes de sécurité, qui doivent réagir sans délai devant chaque nouvelle vulnérabilité. Après le signalement de failles dans Apache Struts, NTT Security a pu observer des attaques tentant de s'engouffrer dans la brèche dans les 24 heures qui ont suivi. Les nouvelles attaques se propagent rapidement à travers la communauté des cybercriminels. Pour des équipes IT déjà débordées, identifier les vulnérabilités puis tester et appliquer les correctifs adéquats relève quasiment de

Copyright© NTT Security 2019

l'impossible. Et pour compliquer un peu plus la donne, les attaquants ciblent de plus en plus des vulnérabilités vieilles de quelques jours, et non plus quelques années. Pour faire face, les entreprises doivent pouvoir réagir rapidement sur la base d'une cyberveille de haute qualité. Or bien souvent, c'est là que le bât blesse.

Pénurie de compétences au niveau mondial

Pendant ce temps, la pénurie de compétences continue de se creuser. On estime ainsi qu'au niveau mondial, un million de postes restent à pourvoir dans le domaine de la sécurité informatique. D'après une récente enquête (ISC)[2], ce chiffre devrait passer la barre des 1,8 millions d'ici 2022[2] (+ 20 % par rapport à 2015). Réalisée auprès de 19 000 professionnels de la cybersécurité, cette même enquête montre que 66 % des cadres estiment manquer d'effectifs pour se protéger contre l'augmentation des menaces (contre 62 % en 2015).

Pour l'heure, face à une menace croissante, l'écart continue de se creuser entre l'offre et la demande en experts cybersécurité. Quant à la prolifération des fournisseurs, des technologies de protection et des consoles de gestion, elle complique encore un peu plus la donne au niveau mondial.

Dénicher les talents

Pénurie ou pas, les entreprises, elles, sont confrontées à un nombre croissant de cyberattaques. Face à des cybercriminels habiles, organisés et obstinés, la plupart ne peuvent que constater leur manque de compétences et d'effectifs.

En un mot, il leur faut plus de ressources. Et des ressources qualifiées. D'un côté, il est essentiel d'aller chercher des compétences purement IT : spécialistes en forensique, de la gestion d'incidents, de la sécurité mobile, de la conformité, de la protection du cloud, etc. Bref, des collaborateurs dotés des compétences analytiques et du bagage nécessaire pour détecter ce que d'autres pourront manquer. De l'autre, il faut aussi ouvrir la porte aux professionnels issus de trajectoires et parcours hors IT. À ce propos, l'étude ISC[2] souligne que 30 % des professionnels de la cybersécurité sont des non-techniciens (comptabilité, marketing, stratégie, etc.)

Autre point à ne pas négliger, la complexité des opérations. Typiquement, un département informatique doit pouvoir jouer sur une gamme de compétences variées pour couvrir l'ensemble de ses besoins. Or, bien souvent, la réalité du terrain est très différente, les collaborateurs étant contraints de porter plusieurs casquettes et de jongler entre des missions complexes. C'est ainsi qu'un administrateur Windows prendra en charge la gestion des pare-feux, avec pour seul bagage la lecture d'un manuel de formation. Un tel constat ne peut qu'inciter à une remise à plat totale des politiques RH dans ce domaine.

Situation du marché mondial de l'emploi dans le secteur de la sécurité informatique

- 66 % estiment que leur entreprise ne dispose pas d'effectifs suffisants en sécurité informatique
- 1,8 millions de postes seront non pourvus d'ici 2022
- 49 % citent la difficulté à trouver du personnel qualifié comme le principal facteur de la pénurie
- Le taux de chômage est de 2 % seulement à l'échelle mondiale du secteur
- Entre 2016 et 2017, 21 % des professionnels du secteur ont changé d'emploi
- Ce secteur se compose d'hommes à 90 %

Enquête 2017 (ISC)[2] Global Information Security Workforce Study, Frost & Sullivan

68 % des entreprises reconnaissent que le recrutement de spécialistes les aiderait à faire face à la hausse des cybermenaces.

Face à la pénurie de spécialistes, quelles sont vos options ?

Ne rien faire

L'attentisme reste toujours l'option de la facilité en matière de recrutement. Mais tout indique que la pénurie de compétences en sécurité est là pour durer.

Fréquence et sophistication des cybermenaces, complexité des réseaux, volumes de données disponibles : tous ces indicateurs sont à la hausse. Or, nous manquons de ressources compétentes pour analyser ces données et en extraire des informations pertinentes sur les menaces en présence.

Quant aux équipes internes, elles sont déjà débordées. D'après un rapport Frost & Sullivan, les oublis et erreurs de configuration représentent un risque réel, tandis que les délais de resolution en cas de compromission de systems ou de données s'allongent sans cesse. À cet égard, il est préoccupant de constater la stagnation ces dernières années du nombre d'entreprises ayant mis en place un plan formel d'intervention sur incidents. Le rapport Risk:Value 2019 indique que 48 % des organisations à l'échelle mondiale n'ont pas de plan de réponse à incident[3]. Ce chiffre est en augmentation depuis 2018. Conséquences ? Elles adoptent une démarche réactive, plutôt que de prendre le problème de la sécurité à bras le corps. Faute de personnel qualifié, les départements IT en seront réduits à la gestion des affaires courantes. Une chose est sûre : l'attentisme est loin de fournir une solution.

Évaluez votre exposition aux risques

Vouloir agir, c'est bien, mais savoir comment agir, c'est mieux. Un bon point de départ consiste à établir un diagnostic de votre exposition aux risques dans tous vos métiers, puis de les classer par ordre de priorité. Cette première étape permet de mieux définir les ressources en fonction du risque. Toutefois, en l'absence de personnel qualifié en interne, les entreprises doivent souvent renoncer à ce bilan. Si la gestion des risques et de la sécurité est un impératif pour toutes les entreprises, la nouvelle physionomie des menaces les contraint à évaluer leur exposition à l'aune de leurs objectifs commerciaux.

D'où l'intérêt d'un diagnostic indépendant pour mieux cerner cette exposition, réfléchir à la mise en place de bonnes pratiques, prioriser vos activités et les orchestrer à tous les échelons de l'entreprise. D'un point de vue économique, il peut donc s'avérer judicieux d'embaucher du personnel supplémentaire, voire d'externaliser votre sécurité en tout ou partie.

D'ici 2022, il manquera 1,8 million de spécialistes en sécurité informatique dans le monde – une hausse de 20 % par rapport à 2015.

Copyright© NTT Security 2019

Investissez dans vos ressources internes

Votre équipe IT interne ne maîtrise pas seulement tous les fondamentaux, elle connaît sur le bout des doigts toutes vos opérations au quotidien. Qui mieux qu'elle pour assurer votre cybersécurité ! Mais attention : la sécurité informatique demande des années de pratique. Inutile d'espérer une solution miracle, le développement interne d'un tel pôle de compétences doit s'inscrire dans un plan à long terme. Vos experts en sécurité devront posséder des qualités à la fois techniques et humaines pour bien communiquer avec les acteurs hors IT, comprendre les processus métiers, les questions de conformité et les outils analytiques – sans oublier un véritable intérêt pour la sécurité de l'information.

Sur le long terme, la formation de vos équipes internes pourrait se révéler un formidable investissement. Toutefois, les technologies informatiques évoluent plus vite que vous ne pourrez former vos collaborateurs, sans compter qu'un investissement dans la formation et le développement professionnel est une décision stratégique qui coûte cher. D'autre part, sur le court terme, cela ne suffira pas.

Revoyez votre stratégie de recrutement

Concernant les stratégies de recrutement, un récent rapport met en lumière diverses pistes d'amélioration possibles pour combler le fameux abîme des 1,8 million de postes non pourvus à l'horizon 2022.

Aujourd'hui, on observe une forte prédominance des hommes dans le secteur, les femmes ne comptant que pour 11 % des professionnels de la cybersécurité[4]. Outre des discriminations plus fréquentes au travail, les femmes doivent aussi composer avec des rémunérations moins élevées, et ce même lorsqu'elles sont plus qualifiées à l'entrée. À tous les niveaux, des mesures sont donc nécessaires pour promouvoir la sécurité informatique comme une voie professionnelle possible pour les femmes. Cela passe non seulement par la sensibilisation des conseillers d'orientation dans le secondaire et le supérieur, mais aussi par l'élimination d'une rhétorique traditionnellement machiste qui voudrait que les femmes n'aient pas leur place dans ce domaine.

Autre point fondamental : un tiers des professionnels de la cybersécurité n'ont aucune formation technique, ce qui n'entrave en rien leur progression et leur réussite dans la profession.

Pour les recruteurs, c'est là un point à bien retenir. Les salariés issus d'une fonction hors IT ont toute leur place dans notre secteur. Ils possèdent en effet des compétences humaines et relationnelles précieuses, comme la capacité à écouter et prendre en compte l'avis des collaborateurs, ou encore à communiquer dans un langage clair et intelligible qui favorise de meilleures décisions.

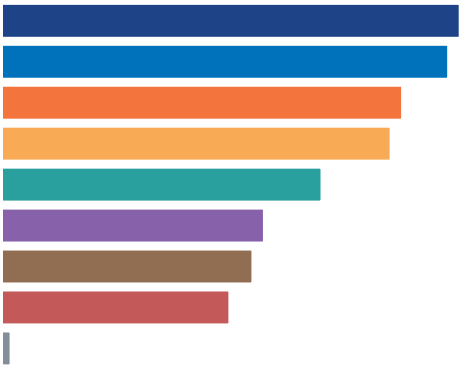
Néanmoins, cette réalité est à replacer dans le contexte, plus large, du papillonnage professionnel caractérisé chez les milléniaux, moins motivés par l'aspect purement financier que leurs ainés.

C'est pourquoi les entreprises doivent sortir des codes traditionnels du recrutement. Aujourd'hui, les responsables de la sécurité informatique doivent accueillir des salariés aux trajectoires et parcours variés. Ils doivent aussi mieux comprendre les motivations de leurs équipes. Bien souvent, il existe un décalage très net entre leurs attentes et celles de leurs recrues, notamment en termes de développement professionnel. Pour résorber la pénurie mondiale de compétences, il est donc essentiel de mieux prendre en compte les attentes des professionnels dans le secteur.

Investissez dans l'externalisation

Le recrutement et la gestion d'une équipe de professionnels de la sécurité apportent avec elles leur lot de problématiques. À commencer bien évidemment par le coût du recrutement et les délais de pourvoi des postes. Viennent ensuite les besoins permanents de formation de l'équipe et d'actualisation de ses compétences et certifications. Et sitôt qu'une personne quitte l'entreprise, il faut tout reprendre à zéro. Dans une étude mondiale publiée récemment, NTT Security met en exergue les principaux arguments en faveur de l'externalisation. Sans surprise, on y retrouve le manque de compétences et de ressources en interne (cf. Figure 1 ci-dessous).

Figure 1 – Les raisons de l'externalisation



40% Accès à des technologies plus performantes
39% Aide à la gestion de données
35% Aide à la modernisation de nos systèmes
34% Stockage de données
28% Aide à la migration vers le cloud
23% Externalisation de processus métiers (ex. RH et paie, traitement des commandes, comptabilité-finance, etc.)
22% Pénurie de compétences internes
20% Pénurie de ressources internes
1% Je ne sais pas

Source : Rapport Risk:Value, NTT Security, 2019

Externalisation des services de sécurité

L'externalisation de tout ou une partie de vos opérations de sécurité peut apporter une réponse au manque de ressources en interne. Ces prestataires savent où et comment trouver les experts qualifiés pour votre secteur. Ils investissent dans leur formation et le développement de leurs compétences professionnelles. Ils surveillent également vos réseaux en continu, 365 jours par an. Enfin, ils vous épargnent toutes les tâches répétitives et fastidieuses, ce qui vous permet de vous concentrer sur vos projets métiers.

Les services de sécurité managés sont en constante évolution. L'intervention du prestataire externe pourra se limiter aux seuls domaines pour lesquels vous peinez

« Nous ne pouvons plus ignorer la pénurie croissante de compétences dans la sécurité informatique. Dans le secondaire comme dans le supérieur, mais aussi à l'échelle du secteur tout entier, il nous faut mettre en valeur le rôle de la cybersécurité. Nous devons aussi garantir des perspectives d'évolution valorisantes, des contrats stables, des niveaux de rémunération attractifs et, surtout, une grande satisfaction professionnelle. »

Garry Sidaway, VP senior Security Strategy & Alliances, NTT Security

« L'abonnement à un service managé présente un grand avantage : les fournisseurs de ces services disposent souvent d'une meilleure compréhension globale de la situation, qui dépasse le simple cadre du réseau surveillé par votre équipe de sécurité interne. »

Dark Reading

Copyright© NTT Security 2019

à recruter en interne (diagnostic risques, développement d'un plan d'intervention sur incidents, gestion d'un projet de mise en conformité, etc.) Toutefois, de nombreuses entreprises choisissent de confier la totalité de leurs opérations de sécurité à des experts indépendants.

Dans ce cas de figure, il ne s'agit plus simplement de gérer des réseaux complexes dans une perspective de continuité opérationnelle. L'heure est à une protection permanente et proactive de votre entreprise face à des menaces multiples et complexes. Votre prestataire devra également se projeter au-delà de la simple gestion des équipements informatiques pour produire des analyses et des éclairages approfondis. En externalisant votre sécurité, vous bénéficiez de la mutualisation des savoirs et systèmes de votre partenaire à l'échelle mondiale, sans oublier l'expérience incomparable de ses collaborateurs.

Les prestataires de services de sécurité suivent attentivement l'évolution des menaces et des vulnérabilités actuelles et futures. Ils disposent également d'un système de veille permanente des menaces au niveau mondial ou régional. Vous êtes ainsi en mesure d'adopter une approche proactive qui vous permet de garder un coup d'avance sur les cybercriminels, plutôt que de simplement réagir une fois les incidents survenus. Un prestataire compétent peut gérer les infrastructures les plus complexes et les applications les plus hétérogènes – sur site, dans le cloud ou en environnement hybride.

« Il est essentiel d'identifier les aspects plus routiniers de votre sécurité (par exemple la gestion des logs), dont les procédures et processus répétitifs se prêtent bien à l'externalisation. Bon nombre d'entreprises misent sur des services de sécurité managés pour résoudre le problème du manque d'effectifs. »

John Petrie, CEO Americas, NTT Security

Conclusion

La physionomie des menaces évolue à un tel rythme que les entreprises ne peuvent plus tenir la cadence. Quant à l'expansion de notre empreinte digitale via les services cloud, les terminaux mobiles, le Big Data et l'Internet des objets, elle ne fait que leur compliquer la tâche. L'explication est simple : les experts qualifiés en sécurité de l'information arrivent en nombre insuffisant sur le marché du travail. En outre, la formation des collaborateurs internes ou l'embauche de nouveaux salariés n'offrent aucune solution miracle. Il est grand temps de présenter la sécurité informatique comme un véritable choix de carrière et de sensibiliser davantage les étudiants du monde entier afin d'éveiller des vocations sur cette voie.
D'ici là, les entreprises devront soigneusement peser le pour et le contre entre un recours exclusif à leurs ressources existantes et l'externalisation de tout ou partie de leurs opérations de sécurité auprès d'un partenaire de confiance. Le moment est venu pour elles de prendre cette décision.

L'entreprise NTT Security

NTT Security est la branche et centre d'excellence sécurité du groupe NTT. Nous mettons notre expertise au service des entités du groupe NTT en délivrant des solutions métiers résilientes pour accompagner leurs clients dans leur transformation numérique. Forte de ses 10 centres opérationnels de sécurité (SOC), ses 7 centres de R&D et plus de 1 500 experts en sécurité, NTT Security intervient chaque année sur des centaines de milliers d'incidents à travers six continents.

Pour optimiser l'utilisation de nos ressources locales et libérer le potentiel de nos capacités mondiales, nous offrons un ensemble adapté de services de sécurité managés (MSS) mais également de conseil stratégique ou technologique aux entreprises. NTT Security fait partie intégrante du groupe NTT (Nippon Telegraph and Telephone Corporation), l'une des plus grandes entreprises de TIC au monde. Visitez **www.nttsecurity.com/fr-fr** pour en savoir plus sur NTT Security ou **www.ntt.co.jp/index_e.html** pour le groupe NTT.

1. Gartner – Communiqué de presse 2. Enquête 2017 (ISC)² Global Information Security Workforce Study, Frost & Sullivan
3. Rapport Risk:Value, NTT Security, 2019 4. Livre blanc Frost & Sullivant – Global Information Security Workforce Study: Women in Cybersecurity

Copyright© NTT Security 2019