Comment identifier vos besoins en cybersécurité ?

Pour protéger leurs acquis ou convaincre leurs clients, les entreprises, en particulier les plus jeunes, doivent prendre les devants face à des cybermenaces toujours plus élaborées. Mais par où commencer ? Quelques conseils pour sortir du brouillard.

Temps de lecture : minute

28 juin 2019

"*Je n'ai jamais eu de mal à pirater la plupart des gens. Si vous les écoutez, les regardez, leurs vulnérabilités sont comme une enseigne au néon vissée au-dessus de leur tête.*" Elliot Alderson, personnage principal de la série Mr Robot, souligne à quel point il est facile pour des hackers de s'introduire dans les failles de certains systèmes informatiques. Les différentes attaques qui se sont succédé ces derniers mois ont contribué à accélérer la prise de conscience des acteurs institutionnels et économiques sur leurs vulnérabilités et la nécessité d'y remédier.

"*La cybersécurité est un sujet qui s'est démocratisé*, reconnaît Jean-Luc Gibernon, directeur Défense et Sécurité de Sopra Steria, qui travaille avec de nombreuses grandes organisations pour sécuriser leurs systèmes. *Mais si la prise de conscience a eu lieu, les organisations n'ont pas forcément encore mis en place de plan d'action ou débloqué de budget dédié.*" Une forme d'attentisme qui les rend particulièrement vulnérables face à des pirates toujours plus sournois.

Sécuriser les bases

Les startups ne font pas exception à la règle, pensant souvent que seuls

les grandes organisations sont dans le collimateur des hackers. Or, les startups étant moins bien protégées que les grands groupes, cela en fait des victimes idéales pour les pirates à la recherche de proies faciles. Paradoxalement, ce sont ces acteurs les moins protégés qui ont le plus à perdre ! Si un grand groupe a les moyens de se remettre d'une cyberattaque, une PME et *a fortiori* une startup joue sa survie. Quand un entrepreneur doit compter le moindre euro afin de respecter son business plan, une perte sèche de plusieurs milliers d'euros liée à une attaque informatique peut mettre en péril la santé financière de l'entreprise. "*Il ne faut pas être naïf mais ne pas verser non plus dans la paranoïa*, tempère Jean-Luc Gibernon. *Des solutions existent pour se protéger.*"

À lire aussi
Cybersécurité : les startups françaises plus nombreuses... mais moins innovantes ?

Tout d'abord, il est nécessaire de sécuriser vos bases. L'Agence nationale

de la sécurité des systèmes d'information (Anssi) rappelle sur son site dix règles de base de la sécurité sur Internet. Utiliser des mots de passe complexes, garder son système d'exploitation et ses logiciels à jour, effectuer des sauvegardes régulières… Cela peut sembler anodin mais ces bonnes pratiques, déclinées dans l'ensemble de l'entreprise, constituent une première barrière - essentielle - face aux menaces les plus évidentes. L'État s'implique aussi dans la sensibilisation des entreprises, grâce à une plateforme dédiée à la cybermalveillance, qui lui permet également de mieux accompagner les victimes.

Pas question, une fois ces dispositions prises, de relâcher vos efforts : la cybersécurité consiste d'abord en un travail constant de veille pour maintenir ses défenses à jour. Les menaces évoluent, les techniques de piratage se renouvellent et les défenses que vous mettrez en place nécessitent d'être elles aussi mises à jour pour répondre aux derniers standards en matière de cybersécurité afin d'être efficaces.

Hiérarchiser ses priorités

Le numérique dope la création d'entreprises dont l'activité est principalement voire exclusivement réalisée en ligne. Ces dernières sont donc davantage exposées à la cyber menace. Celles-ci doivent ainsi redoubler d'attention, par exemple en ce qui concerne la sécurisation du cloud dans lequel elles hébergent leurs données. Si les grands acteurs du cloud prennent en charge la sécurisation de ces espaces, leurs clients doivent toutefois faire attention à configurer correctement leur compte pour parvenir à un niveau de sécurité acceptable : définir un mot de passe complexe, prendre garde à ne pas dévoiler de lien direct vers le cloud qui pourrait être lu par un moteur de recherche, restreindre les accès à un nombre réduit de personnes.

La fuite de données ou le vol de propriété intellectuelle constituent des menaces tout aussi sérieuses pour les startups, dont le modèle

économique repose bien souvent sur le caractère innovant de leur produit ou solution. Une innovation mal protégée, copiée par un concurrent, et c'est la ruine ! Attention donc à bien identifier vos données les plus sensibles afin d'adapter leur protection. Le chiffrement de vos fichiers et communications peut aussi constituer une première protection à mettre en place pour limiter les risques.

Travailler en équipe

Reste un risque majeur en matière de cybersécurité, que nombre de startups oublient : le facteur humain. C'est pourtant une faille critique, dont les hackers se servent régulièrement pour piéger les entreprises. Seule solution : la formation ! En sensibilisant vos collaborateurs dès leur entrée dans l'entreprise à quelques bonnes pratiques élémentaires, vous limitez considérablement les risques qu'ils font courir à toute la société.

Cependant, une entreprise et *a fortiori* une startup ne peut gérer en interne toutes les menaces. A elle de déterminer, au moyen d'un audit qui recensera ses différentes failles, celles auxquelles elle est capable de faire face et celles pour lesquelles elle doit recourir aux services d'experts. "*Les entreprises doivent recourir aux bons prestataires et utiliser les bons produits*", prévient l'expert de Sopra Steria. Ainsi, l'Anssi trie le bon grain de l'ivraie en décernant des certifications et des qualifications à un nombre limité d'éditeurs de solutions de sécurité et de prestataires. Alors, même chez vous, restez couverts !

La cybersécurité, ça coûte cher ?
Les startups sont réticentes à débloquer des budgets dédiés à la cybersécurité, perçus au moment des choix budgétaires comme un coût dont elles peuvent se passer. "La sécurité coûte cher quand elle n'est pas prise en compte", tranche Jean-Luc Gibernon. Une rançon à payer, un système à sécuriser en vitesse : autant de dépenses non prévues qui seront forcément revues à la hausse face à l'urgence de la situation. C'est d'autant plus dommageable que "la sécurité peut être un facteur différenciant, un vecteur de performance". En effet, un niveau de sécurité optimal peut être une véritable opportunité pour une entreprise de se différencier de ses concurrents qui n'auraient pas pris les mêmes précautions. Et de susciter l'intérêt de grands groupes, qui portent une attention toute particulière à cette question avant d'engager d'éventuelles collaborations. Car, comme les clients et consommateurs, les partenaires sont de plus en plus sensibles à l'argument !

Article écrit par Maddyness, avec Sopra Steria