Sécurité informatique : comment armer son entreprise en 3 étapes clé

Le recours à une sécurité de pointe est plus que nécessaire, et pourtant, bien des sociétés ne savent pas comment s'armer efficacement pour lutter contre ces attaques qui font beaucoup de dégâts. Les menaces et les répercussions promettent à l'avenir d'être si spectaculaires, que plusieurs États membres de l'Union européenne, dont la France, ont décidé à travers la Commission européenne la mise en place d'un paquet cybersécurité.

Portant le nom d'Acte européen pour la cybersécurité, il viserait à renforcer la résilience de l'Union européenne dans le domaine de la sûreté informatique. Faisant écho au RGPD entré en vigueur il y a quelques semaines, cet Acte fixerait des règles pour les entreprises. Encore débattu au Parlement européen, l'objectif de cet Acte vise à mettre la lumière sur le fait que beaucoup trop d'entreprises ne soulèvent pas vraiment l'impact que peut avoir une politique de sécurité numérique même minime pour les préserver d'attaques malignes.
Bien des entreprises continuent d'ignorer l'évolution des menaces et s'en remettent à la bienveillance de leurs employés pour éviter au maximum d'être attaqués, sans pour autant leur donner les bons moyens et outils pour le faire. L'une des portes d'entrée utilisées par les pirates informatiques concerne les mots de passe vulnérables des utilisateurs qui permettent d'accéder aux réseaux et de les infiltrer. D'ailleurs, 59% des internautes[1] avouent utiliser le même mot de passe pour tous leurs comptes, qu'ils soient privés ou professionnels. L'éducation des salariés aux règles simples de cybersécurité et de santé numérique est un point très important qui ne doit pas être mis de côté. Si des équipes performantes doivent aussi être là pour assurer la bonne sécurité des systèmes des entreprises, il existe des leviers à mettre en place par ces mêmes sociétés.
Avant d'enclencher une refonte complète de la sécurité de son entreprise, voici 3 étapes clés à considérer.

Une culture de la surveillance à 360 degrés

L'erreur humaine est souvent la première cause soulignée pour expliquer et blâmer une atteinte à la sécurité. L'humain est un élément important de cette chaine, mais l'adoption d'une vision à 360 degrés implique la reconnaissance du rôle à la fois humain et technologique.

Le rôle des équipes informatiques est aussi d'identifier le changement des comportements au travail. La frontière entre vie privée et vie professionnelle devient de plus en plus floue. Avec la multiplication des pratiques comme le BYOD[2], ou encore le fait que les salariés consultent à la fois leurs comptes professionnels et personnels sur les mêmes appareils au travail intensifie le risque de danger pour l'entreprise. Si un employé clique sur un lien contenant un logiciel malveillant, l'ensemble du réseau de l'entreprise peut alors se trouver en danger.

La brèche subie par Yahoo en 2017 est un exemple qui remet en contexte la force de nuisance des cybermenaces. Avec 3 milliards de mots de passe volés, c'est tout autant de points d'entrée qui peuvent être utilisés pour que les attaquants accèdent aux données d'une entreprise. Ces chiffres stupéfiants démontrent l'ampleur du problème et le besoin de trouver des remèdes efficaces.

Une technologie adaptée aux besoins de chaque entreprise

Bien que la technologie se soit très vite développée ces dernières années, bien des sociétés sont restées sur le carreau quant à la mise en place d'outils adéquats pour se protéger efficacement. Certaines pratiques, qui devraient faire bondir, sont encore monnaie courante. Par exemple, il n'est pas rare de voir certaines personnes garder des détails de cartes de crédit et de mots de passe référencés dans des documents Excel. Partagés avec plusieurs salariés par email et par chats, ces habitudes sont la garantie d'augmenter le niveau de menace en entreprise. C'est ici que les services informatiques doivent absolument évaluer les pratiques internes de la société, et lister les outils existants pour se protéger. Alors, un vrai plan d'action de sécurité pourra être envisagé.

Chaque entreprise étant différente, il n'est pas besoin d'adopter des niveaux de sécurité militaire pour une PME familiale, ce qui sera sûrement le contraire pour une société qui compte des centaines de salariés. Néanmoins, il existe bien des niveaux de sécurités dits de base pour tous, peu importe la taille des effectifs. Des outils de stockage de mots de passe et de partage existent et donne la possibilité de se connecter sans avoir à mémoriser plusieurs identifiants, voire d'utiliser toujours le même, par peur de l'oublier. Ce genre d'outils peut s'avérer très utile s'il on a besoin d'accéder à une variété d'outils de travail. A cela s'ajoute la mise en place d'authentification multifactorielle (authentification forte) qui devrait être appliquée à tous les comptes. Quant aux mesures d'urgence, cette procédure devrait être fortement considérée par toutes les entreprises, pour s'assurer qu'un employé qui quitte l'entreprise, n'ait plus accès aux données sensibles de la société.

La priorité absolue reste la formation et l'éducation

La prise de contrôle de la sécurité de l'entreprise doit également aller au-delà de la technologie. Les équipes informatiques devraient prendre le temps de régulièrement former leurs employés aux meilleures pratiques. Toutes les bases de la sécurité devraient être couvertes, y compris l'importance des mots de passe complexes et uniques, les risques entourant le fait d'apporter son propre appareil sur son lieu de travail et l'accès aux différents comptes sur les réseaux Wi-Fi publics. Idéalement, une politique de sécurité claire et concise devrait être élaborée – plus les conseils sont complexes et moins ils seront faciles à assimiler. La sécurité informatique en entreprise devrait avant tout être inclusive et l'utilisation d'un langage adapté à chacun une règle à suivre.
Plus les employés comprennent la nécessité de rester en sécurité, plus ils sont susceptibles d'adopter des pratiques et des technologies nouvelles. Tout cela a évidemment pour objectif, de préserver leurs données et celles de l'entreprise.

[1] D'après une étude réalisée en mai 2018 du cabinet américain Lab 42.
[2] « Bring Your Own Device » (Apportez vos appareils personnels). Pratique consistant à utiliser ses équipements personnels dans une contexte professionnel.