10 questions à se poser pour protéger votre entreprise des cyberattaques

---

Le nombre de cyberattaques est en constante augmentation ces dernières années, avec une hausse de 51% en 2015. Majoritairement perpétrées via le phishing en exploitant les faiblesses des messageries électroniques, 20 % des attaques cybercriminelles touchent des entreprises. La grande crainte du moment : les Ransomwares dont le plus courant est LOCKY. Comme leur nom l'indique, la démarche de ces cyberattaques est de crypter tous vos fichiers sensibles et de vous demander une rançon (15 000 € en moyenne) pour les restaurer !

#1 – Cyberattaques, ransomware, phishing… Qu'est-ce que c'est ?

Tous ces termes ne vous sont sûrement pas inconnus, mais soyons un peu plus précis. Les cyberattaques sont l'ensemble des intrusions malveillantes, souvent engendrées par un téléchargement web ou la réception d'un email frauduleux, visant à créer des dysfonctionnements dans vos systèmes informatiques (perte de fichiers, postes de travail inutilisables…). Les cybercriminels utilisent souvent le phishing pour sévir : se faire passer pour un organisme faisant foi par email pour soutirer vos informations personnelles… et ils sont de plus en plus performants ! Les Ransomwares sont quant à eux des cyberattaques qui s'introduisent généralement via un email et cryptent vos données, que les ravisseurs vous proposent de restaurer en échange d'une rançon.

#2 – Où se trouvent vos données informatiques ?

Pour se prémunir des cyberattaques, il est primordial de connaître parfaitement son infrastructure et son système d'information. Vos données se trouvent-elles dans un serveur centralisé en local ? Dans les disques durs de chaque poste de travail ? Sur des périphériques externes ? En hébergement privé (Data Center) ? En hébergement public (Dropbox, Google Drive, Icloud…) ? Et en tant que dirigeant d'entreprise ou DSI, avez-vous la maîtrise totale de ces données ?

#3 – Votre antivirus est-il déployé sur l'ensemble de votre infrastructure ?

Un antivirus est bien entendu le premier barrage aux cyberattaques ; encore faut-il savoir l'utiliser pour être bien protégé. Un bon antivirus est avant tout un antivirus qui se met à jour régulièrement, prenant en compte les dernières attaques. Faites-vous conseiller pour choisir un antivirus adapté à votre activité, mais aussi en effectuant les bons paramétrages selon vos besoins, et des mises à jour régulières. Déployé à la fois sur vos serveurs (physiques et virtuels) et postes locaux, la protection de vos données sera ainsi assurée !

#4 – Votre messagerie est-elle bien protégée ?

Véritable porte ouverte sur le monde, votre messagerie est la principale source de cyberattaques (65 % du total). Vous devez donc prêter attention à bien la protéger via un anti spam couplé à un antivirus de pièces jointes. Ce dernier analyse la pièce jointe contenue dans votre email en amont pour assurer sa non délivrance en cas de virus détecté.

#5 – Avez-vous une sauvegarde opérationnelle de vos données ?

En cas de cyberattaque, la sauvegarde régulière de vos données est primordiale : elle vous assurera une restauration et préservera votre entreprise d'une coupure d'activité pouvant être particulièrement problématique. Néanmoins, une bonne sauvegarde de vos données doit être mise en place. Pour cela vous devez vérifier son bon fonctionnement et sa régularité. Assurez-vous qu'un plan de reprise d'activité (PRA) soit mis en place ou bien que vous disposiez d'une sauvegarde externalisée (grâce à une solution cloud par exemple). La sauvegarde externalisée est beaucoup plus sûre qu'une sauvegarde dans vos locaux en cas d'incendie et de vol par exemple.

#6 – Avez-vous une bonne gestion des droits utilisateurs ?

La gestion des droits d'accès aux données, aux fichiers pour vos utilisateurs est un sujet sensible, tant en interne qu'en externe. Il est important de mettre en place une gestion des droits d'accès en fonction des profils de vos utilisateurs. Si vous n'y prenez pas garde, vous vous exposez à une double peine : si un virus s'installe en interne, il vérolera l'ensemble des réseaux externes si tous les droits sont ouverts ! Pensez donc à créer des droits d'accès en contrôle total ou lecture seule pour les fichiers communs en internes, afin de limiter les risques de propagation.

#7 – Quelle est votre politique de liberté informatique ?

La politique de liberté informatique d'une organisation correspond aux droits web octroyés à vos collaborateurs ; quels sont leurs possibilités de navigation, de téléchargement… Il ne s'agit pas là de les brider, sachez leur expliquer qu'il s'agit de les protéger !

#8 – Votre environnement informatique est-il « up to date » ?

La tenue à jour de votre système d'information (SI) est elle aussi un point crucial contre les cyberattaques. Pour éviter toute faille de sécurité, il convient de vérifier que votre SI est homogène (mêmes versions sur tous les postes de travail), et que les mises à jour de votre système d'exploitation et de vos logiciels soient encore disponibles chez les éditeurs.

#9 – Etes-vous protégé des attaques extérieures ?

Le principal moyen de se prémunir des attaques externes reste le pare-feu. Véritable protection de votre réseau d'ordinateurs connectés en permanence à Internet, le pare-feu est l'intermédiaire entre le réseau local et le réseau externe. Comme tout logiciel et système installé, il convient de vérifier son bon paramétrage et ses mises à jour régulières pour en assurer un fonctionnement optimal.

#10 – Etes-vous assisté par un expert en cybersécurité ?

Les experts en cybersécurité sont un gage de protection contre les cyberattaques. Ils pourront expertiser votre SI de manière globale et vous

orienter vers des pistes d’amélioration pour protéger votre entreprise des cybercriminels. Ils sauront notamment vous montrer l’importance d’un hébergement privé, comprenant à la fois l’hébergement de vos fichiers ainsi que de votre messagerie par laquelle entrent la plupart des virus comme vu précédemment.