Communiqué de presse

Les bonnes pratiques à adopter pour faire face aux cyber-risques

Paris, le 27 février 2018 – **Le nombre croissant de cyberattaques et les dommages qu'elles causent aux entreprises sont des sujets régulièrement traités dans les médias. En revanche, celui des cyber-risques encourus par les salariés n'est que rarement abordé. C'est pourtant sur ces individus qu'il convient de se concentrer, afin de les sensibiliser aux bonnes pratiques et de prémunir les entreprises de possibles attaques informatiques. BlueFiles, la solution pour sécuriser le transfert de données, offre un tour d'horizon des « bons »réflexes à suivre !**

Prendre quelques minutes pour définir sa stratégie mot de passe

Il est bien souvent plus simple et pratique d'utiliser le même mot de passe pour l'ensemble de ses comptes, professionnels comme personnels. Les mots de passe professionnels doivent pourtant être uniques, sans relation avec la sphère privée des salariés, et surtout, ils doivent rester secrets ! Ils doivent également être définis en fonction de la criticité du compte utilisé. Exit les mots de passe trop simples, liés à une date anniversaire ou au nom de son animal de compagnie, en particulier pour la messagerie pro.

« *L'utilisation d'un mot de passe identique pour les services dit sensibles telle que votre banque, que pour les services secondaires, comme les forums, est à proscrire ! En particulier, lorsque votre boite mail vous permet de réinitialiser ces autres comptes. Soyez inventif : quelques minutes de réflexion suffisent - contre des heures pour le service informatique - à récupérer votre compte* », explique **Mathieu Gémo, co-fondateur de BlueFiles.**

Une authentification, c'est bien, deux, c'est mieux !

Aujourd'hui encore, trop peu de salariés sont sensibilisés à l'utilisation de la double authentification. C'est pourtant une garantie de sécurité supplémentaire, qui devient rapidement indispensable sur des services gratuits (messagerie, agenda, clouds publics comme privés) et des connexions sur plusieurs terminaux. En particulier lorsque les salariés sont amenés à faire du télétravail.

Ne pas tomber dans le piège de la simplicité

Tant dans l'usage personnel que professionnel, il est nécessaire d'être vigilant sur tout ce qui semble faciliter l'utilisation. Malgré la fiabilité des trousseaux d'accès des navigateurs, la meilleure protection reste encore d'éviter les connexions automatiques.

« *Nous pouvons avoir tendance à s'appuyer sur les machines pour retenir nos identifiants et mots de passe. C'est une erreur ! D'abord parce qu'on ne fait plus travailler notre mémoire,*

ensuite parce que cette confiance mal placée abaisse notre vigilance », précise **Mathieu Gemo, co-fondateur de BlueFiles.**

Ne pas céder à l'urgence du clic

En 2016, le phishing était l'attaque numéro 1 en France. Idéalement, une entreprise utilisera une messagerie chiffrée pour protéger ses échanges de mails internes, comme externes.

Malgré cela, les salariés doivent intégrer quelques bons réflexes, comme la vérification de l'adresse de l'émetteur et surtout son nom de domaine. Si le destinataire se sent obligé de cliquer ou ressent l'urgence d'ouvrir une pièce-jointe, c'est probablement une tentative de phishing. Si le moindre doute persiste, il est préférable de ne pas l'ouvrir.

« *Lorsque qu'une entreprise contacte un consommateur, le message se trouve généralement sur l'espace client. Dans un mail qui demande urgemment de cliquer un lien, il est préférable de se rendre sur le site afin de vérifier la véracité du message* », explique **Mathieu Gemo, co-fondateur de BlueFiles.**

Brouiller les pistes

Aujourd'hui, la plupart des sites placent des traceurs (ou cookies) sur les desktops et autres terminaux mobiles. Ces données collectées, récurrentes dans l'usage personnel (e-shopping, consultation des actualités, réseaux sociaux, etc), ne doivent pas interférer avec les accès professionnels et leurs outils web.

Même si les navigateurs tendent à cloisonner, notamment via la navigation privée, ils ne sont pas exempts de possibles failles à exploiter. La meilleure solution est d'utiliser deux navigateurs distincts pour les recherches professionnelles et personnelles.
« *Le cloisonnement est naturellement plus fort, même si l'utilisateur reste sensible au tracking lié au partage de connexion internet* », confirme **Mathieu Gemo, co-fondateur de BlueFiles.**

Rendre ses données invisibles

Trop de salariés transmettent encore des données sensibles en ligne, sans recourir au chiffrement. Cela rend ces données très vulnérables et surtout, facilement accessibles. Pour l'envoi de documents numériques importants, l'idéal serait de posséder un outil de chiffrement, à l'image de BlueFiles pour pallier à leurs vols et/ou fuites, et ainsi garantir que seul le dentinaire puisse y avoir accès.

Contact presse
Agence MilleSoixanteQuatre
Emilie Ménard
e.menard@millesoixantequatre.com
01 85 76 30 52