LA SÉCURITÉ INFORMATIQUE : L'AFFAIRE DE TOUS

La cybercriminalité explose. Avec la pandémie de coronavirus, tout le monde s'est retrouvé plus connecté que jamais, les transactions en ligne ont explosé, … et les cybercriminels en ont profité pour essayer de s'immiscer dans les brèches.

Chez Portima, en tant que partenaire informatique des courtiers et des compagnies, la sécurité fait partie intégrante de notre métier. Nous mettons tout en œuvre et investissons énormément afin de protéger au maximum notre réseau et les données qui y transitent.

Mais aujourd'hui, un nouvel élément est devenu capital dans la lutte contre la cybercriminalité : le facteur humain. La cybersécurité devient véritablement l'affaire de tous.

Un accès hautement sécurisé au réseau et à vos données

La cybersécurité relève de nombreux domaines. Elle comprend, entre autres :

- La sécurité des infrastructures avec notamment la mise en place de barrières de protection comme les firewall, viruswall et spamwall pour protéger le réseau, les PC et les serveurs des intrus.

- La sécurité des informations, qu'elles soient stockées ou en transit. Ainsi, par exemple, toutes les données qui passent par notre réseau sont

- **Confidentielles** : elles sont illisibles pour toute personne qui les intercepterait car elles sont cryptées.
- **Intègres** : l'information ne peut subir aucune modification. Si tel devait être toutefois le cas, le récepteur saurait immédiatement que le message a été falsifié.

- La sécurité opérationnelle: il s'agit par exemple des autorisations des utilisateurs pour accéder au réseau. Comme vous le savez, chaque personne se connectant à notre réseau est authentifiée, ce qui lui permet d'accéder à ses données et aux services auxquels elle a droit… et uniquement à cela.

Quand la cybersécurité devient l'affaire de tous

Avec la mise en place de toutes ces techniques et procédés hautement compliqués à pirater, les 'hackers' se tournent vers un autre élément plus « facile à piéger » : l'homme. En effet, c'est la faiblesse humaine que les pirates informatiques vont cibler tout particulièrement pour arriver à leurs fins, en misant sur la peur, l'urgence d'une action ou sur l'actualité.

Pour donner une petite idée de ce phénomène chez Portima, au cours du mois de novembre dernier, nous avons arrêté pas moins de 6700 e-mails frauduleux destinés à … 10 courtiers différents seulement.

Il est donc plus indispensable que jamais que chacun se protège et soit vigilant afin d'éviter les pièges des pirates informatiques.

Que faire pour protéger votre bureau des pirates informatiques ?

- Installez un antivirus que vous mettrez régulièrement à jour : c'est un élément capital et c'est la raison pour laquelle Portima vous en propose un, compris dans votre abonnement Portima Connect : F-Secure

- Prenez des back-ups des données présentes localement sur votre PC.

- Apprenez à détecter les e-mails frauduleux.

Pour cela, vérifiez que l'e-mail s'adresse à vous et que vous connaissez l'expéditeur (contrôlez l'adresse mentionnée). Si l'e-mail contient un lien vérifiez la page vers laquelle il redirige, sans cliquer dessus. S'il s'agit d'une url abrégée, vous pouvez utiliser un outil pour développer le lien et vous assurer de la destination.

Il est à noter que le phénomène de 'smishing' se répand également de plus en plus. Il s'agit cette fois d'arnaques par SMS ('smishing' provenant de 'SMS' et 'phishing' ou hameçonnage en

français). Un exemple ? un SMS provenant de Bpost ou Amazon vous informant que vous devez payer des frais supplémentaires pour un colis en cours d'acheminement ou un SMS vous indiquant que votre compte itsme © est bloqué et qui vous demande vos informations personnelles pour le débloquer…

La technique est identique à celle du phishing (hameçonnage par e-mail) : vous inciter à cliquer sur un lien frauduleux pour tenter ensuite d'obtenir vos données personnelles et les utiliser à vos dépens.

- Protégez vos comptes

- Créez des **mots de passe longs et forts**, sans lien avec votre vie privée et donc plus difficiles à deviner.
- Utilisez des **mots de passe différents** pour vos comptes privés et professionnels
- Si vous voulez enregistrer vos mots de passe, **utilisez un outil professionnel** mais bannissez, bien entendu, les notes visibles ou un fichier facilement accessible
- Utilisez **l'authentification à deux facteurs.**

L'authentification à deux facteurs demande deux moyens différents pour prouver que vous êtes bien la personne que vous prétendez être. En général, le premier facteur est un mot de passe ou code PIN. Le second facteur peut être l'envoi d'un code à votre téléphone portable ou votre empreinte digitale, par exemple. Seule la combinaison des deux facteurs vous donne alors accès à votre compte. C'est légèrement plus contraignant pour vous mais bien plus sécurisé.

- Protégez vos appareils mobiles

On n'y pense peut-être pas immédiatement, mais les appareils mobiles (tablettes et autres smartphones) sont aussi la cible des pirates : si vous détenez des informations professionnelles sur ces appareils, les pirates peuvent utiliser ceux-ci comme voie aux données de votre société. De même le contenu et les contacts de votre smartphone sont peut-être exactement ce que les pirates recherchent.

Aussi, comme pour votre PC, nous vous conseillons de tenir vos applications à jour. En effet, dès qu'une faille de sécurité est détectée dans une application, l'éditeur la corrige immédiatement. En mettant régulièrement à jour vos applications, vous disposez dès lors des derniers correctifs de sécurité. La même vigilance s'impose pour l'authentification à vos applications, le choix de vos mots de passe, les e-mails et les sms reçus, …

En outre, nous vous conseillons d'autoriser votre appareil à effacer à distance les données qu'il contient. En cas de perte ou de vol, cela peut s'avérer extrêmement utile.

Utilisez uniquement le 'store' de votre appareil pour télécharger des applications. Ces plateformes effectuent des tests de sécurité avant de mettre les applications à disposition. C'est donc plus fiable que le navigateur Internet.

Enfin, mieux vaut désactiver la connexion Wifi quand vous n'en avez pas besoin, de même qu'il est préférable de ne pas permettre à votre appareil d'accéder automatiquement à un réseau inconnu.

Pour plus d'informations à propos de la cybersécurité, regardez notre Sofa Chat sur le blog de notre site www.portima.com

PORTIMA