Auto-évaluation des risques personnels pour les vulnérabilités

Les mots de passe : incontournables lorsqu'on parle de cyber-sécurité, ces « codes » sont utilisés pour vérifier l'identité lors de la connexion à des services virtuels et à des réseaux. Si l'utilisateur dispose d'un mot de passe unique pour chaque compte, le niveau de risque qui lui est associé est minime, mais s'il dispose d'une sélection de mots de passe parmi lesquels il effectue son choix, le risque est un peu plus élevé. S'il possède un ou deux mots de passe qu'il réutilise sur plusieurs comptes, alors son niveau de risque est de 10 sur 10.

Les mots de passe sont probablement l'information la plus détournée en ligne ; beaucoup trop de gens utilisent un seul mot de passe pour plusieurs comptes – et les criminels adorent cela. Connues sous le nom d'attaques par « credential stuffing », les combinaisons d'e-mails et de mots de passe volées lors d'une violation de données seront testées sur d'autres services en ligne pour voir si elles fonctionnent. C'est comme essayer une clé dans une serrure pour voir si elle va s'ouvrir – si c'est un passe-partout, alors de nombreuses serrures seront ouvertes !

La meilleure façon de réduire le risque est de disposer d'un mot de passe unique pour chaque compte en ligne, lequel doit être difficile à déchiffrer, mais facile à retenir. L'utilisation d'un « gestionnaire de mots de passe » est sans doute encore plus pratique. Ces programmes stockent une base de données chiffrée contenant les informations de connexion uniques de tous les comptes en ligne d'un utilisateur. Ainsi, lorsqu'il navigue sur un site web, le gestionnaire de mots de passe est activé, l'utilisateur saisit le mot de passe principal et transmet ensuite les informations correctes associées à ce site.

Mise à jour du grille-pain : il est très courant de reporter plusieurs fois le message de mise à jour logicielle du smartphone, de la télévision ou encore de l'ampoule connectée. Ceux qui le font immédiatement s'exposent à un niveau de risque infime, tandis que ceux qui attendent quelques jours augmentent un peu le risque. En revanche, ne pas le faire élève considérablement le niveau.

Le problème vient souvent du fait que le moment où l'appareil cherche à se mettre à jour est généralement celui où l'utilisateur souhaite s'en servir. Cependant, ces mises à jour sont publiées par le fournisseur pour une bonne raison : parfois il ajoute de nouvelles fonctionnalités, parfois il supprime des fonctionnalités obsolètes, mais souvent il corrige une vulnérabilité dans le code pour empêcher les cyber-criminels d'exploiter la faille. Un exemple tristement célèbre est celui de Wannacry – un programme malveillant qui a tiré profit d'une vulnérabilité du système d'exploitation Windows et a fait des ravages dans le monde entier. C'est pourquoi il est conseillé de toujours procéder à une mise à jour dès que possible, des terminaux comme des applications.

Emails & finances : avant d'effectuer un paiement en ligne, en particulier si le paiement a été demandé par un tiers, il est nécessaire de vérifier son authenticité. Si un utilisateur effectue souvent des paiements en ligne sans vérifier les informations du compte, la situation est un peu plus risquée. S'il a des doutes, mais effectue quand même le paiement, alors le risque est maximal. Les escrocs ont en effet plus d'un tour dans leur sac : un appel téléphonique opportuniste affirmant qu'un paiement n'a pas été reçu, ou un email prétendument envoyé par une entreprise légitime. Il

est vivement recommandé de ne pas prendre pour argent comptant une information trop belle pour être vraie, et de vérifier la légitimité des informations bancaires.

Par ailleurs, en cas d'appel inattendu du service des impôts, de sa banque ou d'un autre organisme officiel requérant des détails de cartes de paiements ou autres informations personnelles, si l'utilisateur s'exécute et les transmets, il atteint alors un niveau de risque maximal. La plupart des organisations, telles que les banques ou le service des impôts fournissent des informations sur le type de communication à attendre de leur part. Tout autre type de communication est susceptible d'être frauduleux.

Habitudes de navigation : sur internet, les pages remplies de publicités, de pop-ups et le taux de réponses positives à des offres alléchantes constituent une prise de risques de la part de l'utilisateur. Les cyber-criminels utilisent souvent les réseaux publicitaires en place et les sites web compromis pour dissimuler des malwares. Si un individu se rend sur un site qui a été infecté, un malware de type ransomware par exemple pourrait se télécharger et compromettre son terminal. Cela peut se produire simplement en visitant la page, car il n'est pas toujours nécessaire de cliquer sur les nouvelles arnaques de type « malvertising » pour être infecté.

La technologie de blocage des publicités ou « ad blocker » empêche non seulement de voir des publicités indésirables et protège la confidentialité de la navigation, mais elle prévient également les infections par des malwares. Il est possible d'aller plus loin en utilisant un ad blocker qui arrête les publicités au niveau du réseau. En outre, le dispositif utilisé pour « surfer sur le net » doit être protégé par un logiciel antivirus et antispam régulièrement mis à jour afin de limiter les risques.

Couvrir ses traces : vu la multiplication des lieux qui proposent le Wifi public gratuit, il est courant de rester en ligne lorsque l'on est en déplacement. Or, pour rester protégé, il est recommandé de recourir à l'utilisation d'un réseau privé virtuel (VPN) pour se connecter à un hotspot public. Idéalement il vaut mieux éviter les réseaux Wifi publics, mais ceux qui l'utilisent doivent partir du principe que tout ce qu'ils transfèrent peut être consulté.
Un VPN peut améliorer considérablement la protection de la vie privée, mais le plus sûr est d'attendre d'être de retour sur un réseau de confiance avant d'effectuer des tâches sensibles.

Question de sécurité : le fait d'être une personne « sociable » peut également avoir une incidence sur son score de risque personnel. Ceux qui tweetent, postent et instagramment tous les aspects de leur vie quotidienne, la réponse à certaines questions de sécurité aurait pu être divulguée, comme par exemple si l'une des réponses de sécurité est le nom de jeune fille de sa mère.
Cela vulnérabilise alors considérablement la sécurité des données de l'utilisateur.

Les informations divulguées en ligne peuvent constituer un véritable trésor d'informations pour les cyber-criminels. Par exemple, être amis avec sa famille sur Facebook peut révéler certaines informations sur l'utilisateur, lesquelles peuvent alors être utilisées par les pirates informatiques à leur avantage. Il convient de songer aux questions de sécurité utilisées pour sécuriser ses comptes et de chercher des réponses que personne d'autre ne connaît, ou qui ne pourraient être devinées.

Quelque chose de connu et quelque chose de détenu : l'authentification à deux facteurs, ou 2FA, consiste en la combinaison de quelque chose de connu, comme un mot de passe ou un nom d'utilisateur, et de quelque chose que ce dernier possède – comme une empreinte digitale, une

reconnaissance faciale ou un code d'accès unique envoyé par SMS.
Il est très important d'utiliser la double authentification sur son compte de messagerie principal. Sans cela, si l'utilisateur perd le contrôle du compte parce que quelqu'un trouve son mot de passe, cette personne peut alors réinitialiser les mots de passe de tous les comptes.

Corruption réseau : il est important de penser à sa configuration domestique et à tous les appareils qui se connectent au routeur, de même que lorsque quelqu'un nous rend visite.
En effet, communiquer le mot de passe Wifi présente un risque, alors que configurer le routeur pour y autoriser deux réseaux permettrait de mieux protéger son réseau.

Tout appareil connecté doit être considéré comme « corrompu » et être connecté à un réseau distinct, ce que la plupart des organisations sensibles à la sécurité font depuis des années. Si une vulnérabilité non corrigée existe au sein d'un appareil, que ce soit un appareil utilisé en permanence ou le smartphone d'un visiteur, elle pourrait être mise à profit par un cybercriminel pour infecter l'ensemble du réseau. L'option la plus simple consiste à séparer tous les appareils connectés des réseaux où sont stockées des informations personnelles inestimables et sur lesquels fonctionnent les appareils.

Connecter ces derniers à un réseau distinct, permet de limiter les dégâts potentiels en cas d'accès par un pirate informatique. Dans le pire des cas, ce dernier aurait uniquement accès aux autres systèmes IoT du réseau, au lieu d'exposer les ordinateurs portables et les téléphones, dont le piratage aurait des conséquences personnelles plus graves.

Heureusement, les fournisseurs d'accès à internet et les fabricants de routeurs commencent à intégrer des réseaux « invités » dans les fonctionnalités de leurs produits, ce qui permet aux utilisateurs de définir des réseaux distincts – un pour tous les appareils de confiance et un autre pour les appareils potentiellement corrompus.

Toute prise de risque constitue une note de 10 sur 10 à l'auto-évaluation de vulnérabilité en ligne et faire un sans-faute n'est pas une bonne chose à l'heure actuelle. Ainsi, avant de se livrer à toute autre activité en ligne, il est essentiel de repenser son comportement et de prendre les mesures pour réduire son risque personnel.