La cybersécurité : le rôle de l'organisation et la nécessité d'avoir les bons réflexes

La cybersécurité est incontestablement une préoccupation majeure pour les professionnels. Abordant différents visages, elle est complexe à identifier et amène les entreprises à adopter une veille continue pour se prémunir de nouvelles menaces. Si la technologie permet de réduire les risques, elle n'est pas pour autant infaillible. Ce constat est d'autant plus vrai pour les personnes non informaticiennes ou les hommes et femmes-clé des entreprises qui sont des cibles de choix pour les hackers. Dans ce contexte, une éducation constante de ces populations est incontournable. On notera enfin que les PME/ETI sont particulièrement concernées par les cyber attaques, car souvent moins bien protégées et moins sensibilisées que les grands groupes. Prenons deux exemples :

Le cas des ransomwares : un fléau à grande échelle

Cet exemple est assez caractéristique du type de menaces qui visent les entreprises. Ainsi, ces dernières années, une vague d'attaques a frappé les PME et ETI dont de nombreuses se sont trouvées paralysées, voire dans certains cas ont dû fermer leurs portes définitivement. La raison est simple, ces dernières n'ont pu accéder à leurs systèmes d'information et ont été dans l'impossibilité de poursuivre leurs activités. Cette situation s'explique aisément : nombre de personnes ont reçu un simple mail les invitant à consulter une pièce jointe ou cliquer sur un lien pour accéder à un document important (administratif et réglementaire par exemple). Bien entendu, il s'agissait ici d'une démarche frauduleuse qui avait pour objectif d'infecter et bloquer les serveurs et ordinateurs des entreprises et de leur demander une rançon pour les débloquer.

La fraude au Président : une pratique en croissance

Sur ce point, différents cas d'école existent et visent le Top Management et son entourage. Il s'agit dans ce cas de figure de se faire passer pour le dirigeant d'une entreprise et de contacter différents collaborateurs pour leur demander d'exécuter telle ou telle action. L'imagination des pirates est alors débordante : demander un ordre de virement, demander des dossiers confidentiels, diffuser des informations erronées, … Sont alors concernés les assistantes de direction, les directions financières, les départements Innovation, les partenaires externes, etc. Nous pouvons également évoquer l'ingénierie sociale qui elle aussi se développe à grande échelle.

À travers ces éléments, force est de constater que les managers des entreprises et leur entourage (interne et externe) sont particulièrement concernés par les menaces cyber qui continuent de se développer. Pour lutter au mieux contre ce fléau, il est donc important de prendre de la hauteur sur ce sujet de la sécurité informatique et de l'étudier avec attention. Les managers et non-informaticiens des PME/ETI étant les premières victimes, ils doivent absolument réagir, ne pas rester passifs et adopter une attitude prudente avant de réaliser une action qui pourrait être compromettante. Une chose est sûre, en cas de doute, mieux vaut d'abord contacter les soi-disant interlocuteurs ou vérifier la véracité des demandes et sollicitations avant de lancer la moindre opération.

Par Philippe PELFORT, Directeur Général de SEA TPI

Philippe PELFORT a été invité à intervenir à la conférence « Cybersécurité et entreprises : il y a urgence! » organisée dans le cadre du mois européen de la cyber sécurité par le ministère de l'économie et la DFCG, le 30 Septembre dernier. Il a apporté son témoignage de chef d'entreprise et partagé les bonnes pratiques mises en place au sein de SEATPI.