Vous travaillez à domicile ? Les cybercriminels adorent ça !

La Dernière Heure - 25 Mar. 2020

Le télétravail est devenu la norme pour beaucoup. Il crée un environnement propice aux attaques numériques, mais pas seulement.

La semaine passée, le gouvernement belge a imposé aux entreprises le télétravail pour toutes les fonctions qui le supportent. Ceci n'est pas sans impact sur la vie des responsables informatiques, qui sont, depuis lors, confrontés à une situation inédite. Une situation qui comporte des risques, comme nous le confirme Maarten Stassens, expert de la cybersécurité au sein du bureau d'avocats américain Crowell&Moring. "En fait, on se retrouve tous, moi y compris, dans une situation anormale dans laquelle nous essayons de travailler au mieux. Mais nous ne sommes pas dans notre environnement de travail habituel, nos repères sont faussés", nous explique-t-il. Le helpdesk, s'il existe, est submergé de demandes, tout le monde envoie des courriels, et ce n'est pas sans conséquences sur l'organisation personnelle. Une visibilité numérique dangereuse Et puis, l'entreprise et le personnel communiquent. Sur les réseaux sociaux, par courriel, les entreprises font savoir qu'elles poursuivent leurs activités via le télétravail. Les employés s'en plaignent ou s'en réjouissent en ligne. "C'est une attitude naturelle, mais elle est à proscrire", explique Maarten Stassens. "En fait, nous donnons, de cette manière, beaucoup trop d'informations personnelles à des cybercriminels qui adorent ça. Ils savent dans quelles dispositions psychologiques se trouvent les employés projetés dans une situation inhabituelle et ils sont capables d'en tirer profit". Comment cela se passe-t-il ? "En fait, lorsqu'on est en télétravail, on veut bien faire, on veut aider les collègues et réaliser son boulot dans les temps. Et c'est là que l'on est vulnérable. Le cas le plus courant est le courrier que l'on reçoit de la part du directeur financier qui a, et c'est possible, des problèmes de connexion. Il demande que soit effectué un paiement urgent. Le tout est libellé par des spécialistes en fonction des éléments d'information pêchés sur les réseaux sociaux. C'est crédible, et on peut passer à l'action en toute bonne foi. Les techniques sont nombreuses. Il suffit de signaler en ligne un problème d'accès au réseau via le VPN, en redemandant les identifiants et mots de passe". Des e-mails et de la paperasse Que convient-il de mettre en place ? "L'entreprise doit informer sur les risques. Une fois que les employés sont éveillés à une telle situation, ils voient ce qui sort de la norme". Et, en dehors de ce type d'arnaques ? "Il y a aussi les risques techniques. Encore une fois, on se retrouve dans un univers différent. Les enfants sont à la maison et, eux aussi, utilisent le réseau familial qui est quelquefois ralenti. Alors, quand on travaille à la maison, on cherche des solutions. On utilise des serveurs mails externes pour transférer des documents, des contrats. Et on s'y fait vite. Mais sait-on où se trouvent ces documents par la suite? Est-on au courant que les gros opérateurs de courrier électronique disposent de robots qui lisent les échanges, à des fins de ciblage publicitaire, ou autres…? L'Union européenne s'est dotée d'un cadre régulatoire très strict, le Règlement général sur la protection des données privées (RGPD), qui peut sévir lors de manquements sur la gestion de ces documents". On le sait, les entreprises belges sont souvent citées pour leur retard en la matière. Ici aussi, l'entreprise doit donc communiquer sur ses règles internes. Mais, pour Maarten Stassens, le problème peut aussi être matériel, même si c'est un peu surprenant. "Beaucoup de gens préfèrent encore imprimer les documents et les courriers pour les lire et les annoter. Que feront-ils de tous ces papiers une fois de retour au bureau ? Tout cela va se retrouver à la poubelle. Et cela aussi, les cybercriminels le savent".