Conseils pour assurer la sécurité numérique des nomades | Denis JACOPINI

Conseils pour assurer la sécurité numérique des nomades

Même lorsqu'il s'aventure dans le vaste cybermonde, le collaborateur nomade doit avoir accès aux ressources internes de l'entreprise. Il représente alors un danger. Comment se protéger ? Quelques conseils de Gérard Peliks, expert et enseignant en sécurité de l'information.

#Identification et authentification fortes de l'utilisateur
Ce n'est pas l'outil qui doit être tracé, mais l'individu qui s'en sert. « Il s'agit d'identifier et d'authentifier, avec la plus grande attention, l'ayant-droit aux ressources de l'organisation », indique Gérard Peliks, expert et enseignant en sécurité de l'information. Première étape : l'identifiant ou login. Seconde phase : l'authentifiant, autrement dit la preuve de l'identité de l'utilisateur. « Le plus fiable est la combinaison de deux paramètres : ce que l'on a (par exemple une calculatrice, un token usb…) et ce que l'on sait (un code pin). En attendant les solutions de biométrie multimodale… », précise Gérard Peliks.

#Intégrité et confidentialité des transactions
Les échanges entre l'organisation et le collaborateur nomade doivent être sécurisés dans leur confidentialité et leur intégrité. « Il s'agit de créer un tunnel chiffrant dont les deux extrémités sont mutuellement identifiées », souligne Gérard Peliks. Les virtual private networks (VPN) ou réseaux privés virtuels (RPV) garantissent la confidentialité des données transmises, donc vulnérables, sur Internet. La signature électronique peut en garantir l'intégrité. Ce qu'on appelle le protocole de « tunnellisation » ou d'encapsulation consiste à chiffrer les transmissions entre le poste nomade et l'Intranet de l'organisation.

#Chiffrement des données sur disque
En cas de perte ou de vol d'un PC, ou d'un téléphone portable, la confidentialité des informations contenues n'est plus assurée, si elles sont stockées en clair. « On ne perd pas seulement l'objet, mais des données, avec tout ce que cela peut entraîner comme risque d'image, de réputation et même de conséquences juridiques », pointe Gérard Peliks. Tout l'enjeu est donc de rendre illisibles les informations contenues dans l'appareil, si on ne possède pas les clefs pour les déchiffrer. « Le chiffrement de fichiers, de partitions, voire même de l'intégralité du disque, permet de sécuriser les contenus sensibles », explique-t-il.

#Destruction des fichiers
Quand il s'agit d'éliminer un fichier, la touche « delete » et le vidage de la corbeille ne détruisent rien mais se contentent de cacher le document. Et des outils de récupération permettent de pister les anciennes données. Pour effacer définitivement, ou « massicoter » les contenus, il convient d'utiliser des méthodes de suppression sécurisée. « En utilisant des utilitaires de destruction, on s'assure que les fichiers sont réellement passés à la « déchiqueteuse », préservant ainsi leur confidentialité », indique Gérard Peliks.

#Sensibilisation des collaborateurs
Dans un contexte de dématérialisation généralisée, tous les collaborateurs sont potentiellement amenés à travailler un jour en mode nomade, ou avec des collègues en télétravail. D'où l'importance de sensibiliser l'ensemble des collaborateurs de l'organisation aux processus de sécurité. « Dès le début de la collaboration, mais aussi tout au long de la vie du collaborateur dans l'organisation, les règles de sécurité et de confidentialité doivent être rappelées », insiste Gérard Peliks. En plus de faire signer une charte sur l'utilisation du réseau, l'organisation doit communiquer sur les conséquences juridiques de tout manquement au règlement intérieur.

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l’été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d’usurpation d’identité sur facebook, tweeter ? Portez plainte mais d’après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : http://www.lesechos.fr/thema/02167451759-conseils-pour-assurer-la-securite-numerique-des-nomades-1121036.php
Par Julie Le Bolzer