Comment gérer le BYOD dans l’entreprise ?

Entre le télétravail et la hausse du niveau d’équipement informatique des particuliers, il arrive souvent qu’un salarié utilise son propre ordinateur pour accomplir une tâche professionnelle. Un mélange des genres qui peut mettre en danger les données de l’entreprise. Explications.

Le BYOD ?

Le BYOD, pour « bring your own device » ou « apportez votre propre matériel », sur votre lieu de travail (ou l’utiliser chez vous en télétravail), est une pratique qui s’est fortement développée depuis que les smartphones, les ordinateurs portables et les tablettes se sont invités dans les foyers français. Un choix fait par ceux qui estiment (souvent à juste titre) que leur propre matériel est plus performant que celui fourni par l’entreprise ou qui souhaitent, via un seul et même outil, mener de front à la fois leurs activités professionnelles et leurs activités personnelles.

Or cette pratique n’est pas sans risque dans la mesure où elle met l’entreprise dans l’impossibilité d’assurer la protection de son réseau et des données qui y sont stockées. L’entreprise est ainsi exposée à la perte des données qu’abrite la machine de son collaborateur en cas de panne, de perte ou de vol, à des intrusions réalisées par des hackers via cette machine, à

des atteintes à la confidentialité des données stockées ou encore à la contamination du réseau par un malware.

La tentation d'interdire cette pratique

Assurer la sécurité d'un réseau suppose d'avoir la main sur chacune de ses composantes. Or, ce n'est plus le cas avec le BYOD. Raison pour laquelle dans ses « recommandations pour la protection des systèmes d'information essentiels », l'Agence nationale de la sécurité des systèmes d'information (Anssi) considère qu'un « SI maîtrisé ne peut intégrer les pratiques de bring your own device (BYOD) où des personnes peuvent connecter au SI des équipements personnels dont l'opérateur ne maîtrise pas le niveau de sécurité ».

Concrètement, pour l'Anssi, un poste maîtrisé est « un poste de travail fourni, configuré et maintenu par l'opérateur. D'une part, il ne peut s'agir d'un équipement personnel et d'autre part, l'utilisateur ne peut être administrateur du poste, le niveau de sécurité pouvant alors être directement modifié par l'utilisateur ».

Dans une optique purement sécuritaire, le BYOD est donc à proscrire.

Le choix des collaborateurs

Du côté des collaborateurs, plusieurs éléments expliquent le recours à des solutions logicielles ou matérielles autres que celles de l'entreprise :
– Le fait d'ignorer que ces pratiques sont interdites ou non recommandées ;
– L'impossibilité de ramener chez soi le matériel informatique de l'entreprise ;
– L'obsolescence ou la moindre qualité du matériel ou des solutions logicielles mis à disposition par l'entreprise ;

– Un excès de règles de sécurité qui dégradent les conditions d'utilisation des matériels et logiciels fournis ;
– Le refus d'utiliser plusieurs outils, notamment plusieurs smartphones.

Des motivations fortes et cohérentes qui doivent être prises en compte par les entreprises avant d'envisager une simple interdiction du BYOD. Car interdire le BYOD, sans autre forme de procès, les expose au « Shadow IT », autrement dit à devoir faire face à l'utilisation non déclarée de matériels et de logiciels de communication. Une pratique encore plus à risque pour l'entreprise car totalement clandestine.

Le recours au COPE…

Pour limiter ces risques du BYOD « clandestin », l'entreprise dispose de deux possibilités. La première consiste à proscrire l'utilisation d'une machine personnelle dans le cadre professionnel. Mais attention, cette exigence, comme nous l'avons déjà évoquée, ne sera entendue qu'à la condition que le matériel fourni soit aussi performant et convivial que celui du salarié.

Une phase d'échange devra donc être engagée pour mieux comprendre les besoins des collaborateurs, mais aussi pour leur rappeler les dangers que l'utilisation d'une machine ou d'un logiciel « extérieur » fait peser sur l'entreprise.

En outre, il conviendra d'autoriser les collaborateurs, dans un cadre restreint et sécurisé, à utiliser le matériel de l'entreprise pour mener quelques actions privées. On parle ici de COPE (« corporate owned, personally enabled » ou « propriété de l'entreprise avec accès privé »).

Ces échanges déboucheront sur la rédaction d'une charte définissant les règles d'utilisation du matériel de l'entreprise à des fins personnelles.

… ou au BYOD très encadré

La seconde solution revient à autoriser le collaborateur à utiliser son propre matériel à titre professionnel, mais uniquement si ce matériel peut être sécurisé par l'entreprise et que son usage soit encadré.

L'idée étant ici de protéger les données professionnelles traitées via l'appareil du collaborateur, mais aussi de consolider la frontière entre les usages et les données professionnelles et personnelles. Voici 5 grandes règles rappelées par la plate-forme gouvernementale Cybermalveillance.gouv.fr sur sa fiche dédiée à la sécurité des usages pro-perso.

Utiliser des adresses de courriel différentes

Une erreur de manipulation peut conduire à adresser un courriel à la mauvaise personne (un message intime à un collègue ou à un prestataire, un dossier professionnel confidentiel à une connaissance). En outre, les risques de voir sa messagerie piratée sont plus importants lorsque l'on utilise des services gratuits. Deux raisons qui plaident pour que l'on ne mélange pas sa messagerie personnelle et sa messagerie professionnelle.

Distinguer les espaces de stockage en ligne

Certains espaces de stockage (Dropbox, Drive…) sont utilisés par des particuliers en raison de leur praticité, mais également de leur gratuité. Mais là encore, leur utilisation pour stocker des données professionnelles, surtout sensibles comme par exemple des fiches clients, des contrats, doit être interdite. Les données professionnelles ne doivent être enregistrées que sur les serveurs sécurisés de l'entreprise (physique ou cloud).

Dans le même esprit, aucune donnée professionnelle ne doit

être enregistrée sur le disque dur de la machine au risque d'être perdue ou exposée en cas de panne, de perte ou de vol.

Utiliser des mots de passe différents

La tentation est forte d'utiliser le même mot de passe pour l'ensemble de ses comptes sécurisés. Toutefois, cette pratique est fortement déconseillée dans la mesure où si ledit mot de passe vient à être découvert, toutes les données se trouvent en danger : les données personnelles, mais également celles de l'entreprise. L'utilisation d'un mot de passe différent pour chaque type de compte est donc nécessaire.

Ne pas installer n'importe quel logiciel

Certains logiciels ou applications mis gratuitement à disposition sur internet ou sur des plates-formes de téléchargement peuvent contenir des virus ou des fonctions destinées à espionner leurs utilisateurs. Raisons pour lesquelles il convient d'être très prudent et de n'installer sur les machines utilisées pour des usages pro-perso que des programmes provenant de plates-formes ou d'éditeurs ayant pignon sur rue.

Assurer les mises à jour de sécurité

Comme pour les machines de l'entreprise, les mises à jour de sécurité (systèmes d'exploitation, logiciels anti-malwares, navigateurs…) doivent être installées dès leur publication. Adopter une mise à jour automatique est ici conseillée.

Là encore, une charte définissant les conditions d'utilisation des machines BYOD devra être mise en place dans l'entreprise.