Le BYOD et la sécurisation des appareils mobiles

Tablette, smartphone, PC portable… Les outils modernes permettent de répondre plus rapidement aux attentes des clients. Qu'ils appartiennent à vos collaborateurs ou que vous les mettiez à leur disposition, leur usage doit être encadré afin de protéger votre entreprise.

Tous les salariés possèdent un téléphone mobile, voire un ordinateur portable. À l'aise avec leur propre équipement, ils peuvent être plus productifs s'ils travaillent avec au bureau. C'est ce qu'on appelle le BYOD (**« Bring your own device »** ou « Apporter votre équipement personnel de communication »).

Même s'il est apparu en France il y a déjà quelques années, ce phénomène reste encore assez marginal. Selon une étude d'ISlean consulting (Cabinet de conseil en stratégie et organisation), **environ 5 % des PME et ETI françaises ont décidé de mettre en place une politique de BYOD généralisé en 2017**. Cela signifie que tous les employés peuvent travailler avec leur propre ordinateur et smartphone (d'un point de vue légal, des personnes peuvent refuser cette proposition et dans ce cas, l'entreprise leur fournit le matériel nécessaire).

Le BYOD « partiel » est plus important (10 % selon cette même étude). Il s'explique par l'usage mixte du téléphone. Les salariés l'utilisent à la fois pour consulter leurs emails personnels, mais aussi pour envoyer des courriers professionnels. D'autres utilisent leur tablette pour accéder à des logiciels en ligne (mode SaaS pour « Software as a Service ») et éditer un devis par exemple.

Ces appareils personnels peuvent donc contenir des données à caractère personnel et parfois des informations sensibles.

Quels sont les risques ?

- **Une infection du réseau ou de l'appareil**
  En accédant à votre réseau informatique avec son appareil mobile, un salarié peut être à l'origine (volontairement ou non) d'une infection virale ou d'une perte de données. « En 2018, nous devrions observer une évolution des attaques de type ransomware vers l'environnement mobile », avertit Lookout, une société spécialisée dans la sécurité des mobiles.
  Ce type de menace résulte très souvent d'une faible sécurité de l'équipement. Le collaborateur n'a pas forcément mis à jour son téléphone ou n'a pas installé un antivirus. Il peut aussi avoir téléchargé un clone d'un programme anodin qui va infecter son appareil. En novembre 2017, une fausse application WhatsApp, qui affichait de la publicité, a été téléchargée par 1 million d'utilisateurs d'Android.
- **Une perte de données**
  Les informations stockées sur les appareils mobiles des salariés peuvent être dérobées par un code malveillant (de type keylogger par exemple). Autre risque : la perte de ces équipements. Qui n'a jamais perdu son téléphone dans un taxi ? Qui n'a jamais été victime d'un vol de smartphone laissé par erreur sur une terrasse de café ?
- **Un vol de données à caractère personnel**
  En prenant le contrôle d'un smartphone ou d'un PC portable, un pirate peut récupérer des dossiers contenant des informations personnelles de vos salariés ou de vos clients. Cette faille de sécurité démontre une absence de conformité de votre entreprise avec le RGPD. En cas de fuite de données à caractère personnel, vous pouvez être sanctionné par la CNIL.

Le BYOD et la sécurisation des appareils mobiles : les mesures élémentaires à mettre en place

- **Première mesure : fournir des appareils mobiles**
  Afin d'avoir un parc homogène et identifié, vous pouvez interdire le BYOD et favoriser le… **COPE (« Corporate Owned Personally Enabled »**). Cela signifie que vous fournissez des appareils préconfigurés et qui vous appartiennent (d'où des obligations de maintenance, de gestion des licences et de protection des données).

Cette option vous permet de conserver le contrôle d'un terminal et de le sécuriser grâce à une solution logicielle appelée Mobile Device Management (MDM). Un MDM permet :
- un cloisonnement des usages,
- une sélection des applications autorisées.

- **Seconde mesure : désactiver la connexion automatique au Wi-Fi**
  Aucun smartphone ou PC portable ne doit pouvoir se connecter à votre réseau sans fil sans avoir été au préalable identifié et autorisé.

- **Troisième mesure : renforcer la sécurité des appareils mobiles**
  Les formations de sensibilisation aux risques numériques doivent être l'occasion de rappeler aux salariés quelques précautions de base :
  - Pour les smartphones et les tablettes : activer le code PIN pour qu'il soit demandé à chaque démarrage et **activer le code de verrouillage** afin qu'il soit exigé après chaque mise en veille réglée sur quelques minutes. Les mises à jour d'iOS et d'Android, ainsi que des applications, sont obligatoires. Enfin, **conserver le code IMEI** (15 à 17 chiffres) du smartphone. En cas de perte ou de vol, il permettra à l'opérateur de le bloquer à distance.
  - Pour les PC portables : comme pour les ordinateurs de bureau, il est indispensable d'avoir **un mot de passe « fort »** (c'est-à-dire comprenant majuscules, minuscules et caractères spéciaux), **d'activer le verrouillage de la session** de Windows ou de MacOS, de **télécharger les mises à jour** et **d'installer un antivirus et un pare-feu.**

Ce qu'il ne faut pas faire

- **Conserver des données sensibles sur sa messagerie mobile**
  Étant donné les capacités élevées de stockage des webmail, il peut être tentant d'y conserver des documents professionnels. Si l'appareil est volé ou perdu et qu'il est mal sécurisé, une personne malveillante (ou un concurrent…) pourra accéder à des informations confidentielles.

- **Ne pas mettre d'antivirus sur son smartphone**
  Un téléphone mobile est un PC de poche. Il peut donc être infecté par un virus. Il est donc important d'y installer un antivirus. Pas n'importe lequel. Sur le PlayStore d'Android, il y a en effet de multiples applications de sécurité qui ne sont pas développées par des éditeurs spécialisés. Ne vous fiez pas à leurs excellentes notes et **privilégiez les programmes proposés par les éditeurs connus sur Windows.**
  Sachez qu'il n'y a pas d'antivirus pour les iPhone. Cela ne signifie pas que ces smartphones ne peuvent pas être touchés par un virus. Mais Apple refuse ce type de solutions. Par ailleurs, sa politique d'intégration des applications est plus « stricte » que sur Android où les logiciels sont mis en ligne sans contrôle a priori.

Pour aller plus loin

Les obligations des employeurs

Différents textes de loi (dont l'article 34 de la loi du 6 janvier 1978) précisent que les entreprises ont des obligations en matière de sécurité informatique et notamment concernant les données à caractère personnel qu'elles traitent.

L'employeur étant maître de son Système d'Information (SI), il doit indiquer aux salariés désirant utiliser leur terminal qu'ils doivent respecter des règles très strictes en matière de sécurité (indiquées dans la charte informatique).

Generali IARD, Société anonyme au capital de 94 630 300 euros. Entreprise régie par le Code des assurances - 552 062 663 RCS Paris. N° d'identifiant unique ADEME FR232327_01NBYI.
Siège social : 89 rue Taitbout - 75009 Paris.
Société appartenant au Groupe Generali immatriculé sur le registre italien des groupes d'assurances sous le numéro 026.

SG2685MARK-25 - Décembre 2025 - Studio graphique