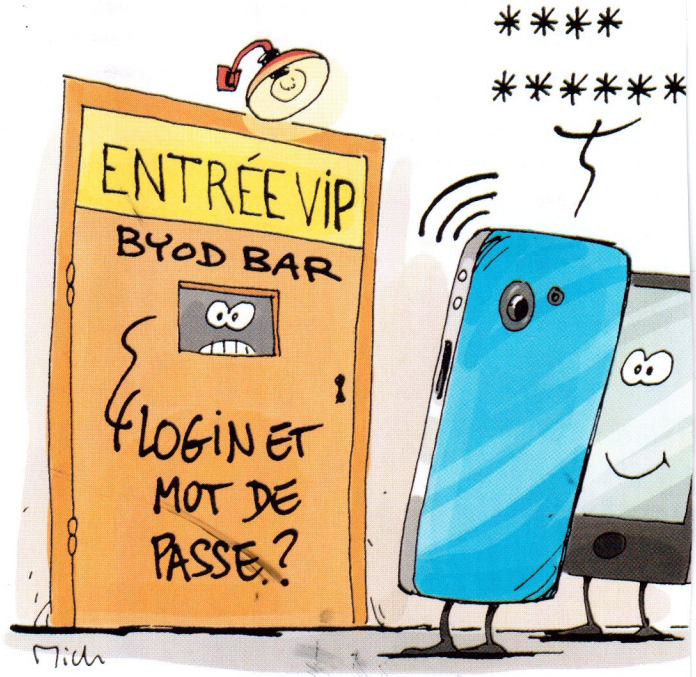
4 pistes pour **protéger votre entreprise** à l'heure du **BYOD**

L'heure est au Bring your own device (BYOD), c'est-à-dire l'utilisation de terminaux personnels (téléphone, tablette, ordinateur…) à des fins professionnelles. Une pratique qui n'est pas sans danger : cyberattaque, vol ou perte de fichiers sensibles… Bref, des risques tout sauf virtuels. Conseils pour vous protéger.



Si vous ne connaissez pas le BYOD, il est temps de vous y intéresser de près car il met en danger la sécurité de votre entreprise. En effet, derrière ce sigle barbare issu de l'anglais ("Bring your own device", alias "Apportez votre propre appareil"), se cache un phénomène en plein essor : l'utilisation de terminaux personnels (smartphone, tablette, ordinateur…) à des fins professionnelles. À l'heure où la mobilité des travailleurs et l'utilisation de smartphones se généralisent, le BYOD présente un certain nombre de risques (cyberattaque, virus, perte ou vol de données…). « *Outre les problématiques techniques liées à la sécurité de votre système informatique et à la protection des informations sensibles de l'entreprise, le BYOD peut bouleverser et désorganiser les méthodes et le rythme de travail des équipes s'il n'est pas bien encadré* », souligne Chadi Hantouche, manager chez Solucom, cabinet de conseil en management et système d'information. Sans compter le flou juridique qui entoure la question. Le BYOD, à la frontière entre vie privée et activité professionnelle, n'est en effet régi par aucune loi en France. « *Alors que le public et la doctrine s'intéressent de plus en plus au phénomène, le droit reste muet en la matière*, confirme Me Murielle Cahen, avocate du cabinet éponyme, spécialisé en droit de l'informatique et droit de l'Internet. *Hormis la loi du 22 mars 2012 sur le télétravail, il n'y a pas encore, pour le moment, de projets de réglementation du BYOD.* » Afin de vous prémunir contre les risques associés à cette pratique, quatre principaux leviers existent.

> « *Outre les problématiques techniques liées à la sécurité de votre système informatique, le BYOD peut bouleverser et désorganiser les méthodes et le rythme de travail des équipes s'il n'est pas bien encadré.* »
> **Chadi Hantouche,** manager, Solucom

1 Interdire cette pratique

Vous êtes en droit d'interdire à vos collaborateurs l'utilisation de leurs appareils privés dans le cadre professionnel. « *Une interdiction directement stipulée dans le contrat de travail est possible*, avance Me Murielle Cahen. *Toutefois, pour les contrats déjà conclus, il faudrait opérer une modification du contrat de travail qui doit emporter le consentement du salarié. Inclure l'interdiction dans votre charte informatique, en respectant les règles de diffusion aux employés, est plus simple.* » Néanmoins, interdire le BYOD revient

À lire sur Chef d'entreprise.com

Souvent négligée, la qualité d'un code d'accès est pourtant primordiale pour empêcher une intrusion dans ses différents comptes protégés. Voici **10 conseils pour trouver un mot de passe sécurisé**, mais aussi mémorisable.

à se priver de ses avantages. Si vos collaborateurs utilisent leurs appareils privés pour se connecter au réseau ou système d'information (SI) de l'entreprise, c'est pour les besoins de leurs missions. Dans ce cas, il est sans doute plus pertinent d'encadrer cette pratique plutôt que de la proscrire d'entrée de jeu. D'autant qu'interdire ne vous protège nullement d'une utilisation "sauvage" des terminaux personnels.

2 Définir des règles et des bonnes pratiques

Quoi que vous décidiez d'engager, placez vos équipes au cœur du processus. «*Aussi, s'il revient aux responsables du service informatique de déployer les solutions et applications métiers nécessaires, il est primordial d'associer également votre service RH et vos managers*», conseille Chadi Hantouche (Solucom). L'expert suggère ainsi de déterminer des règles de bonne conduite et de les intégrer, soit dans la charte informatique de l'entreprise, soit dans le règlement intérieur, ou encore en annexe du contrat de travail. «*L'encadrement de la pratique du BYOD via un écrit permet d'édicter des règles au sein de l'entreprise en l'absence de cadre légal*», souligne Me Murielle Cahen. Veillez notamment à y formaliser les conditions dans lesquels s'opèrent l'échange de données et l'accès au réseau par le BYOD (ex: horaires, catégories de données…), les modalités de contrôle des terminaux, l'indemnité éventuelle du salarié en échange de sa contribution, son obligation d'installer un antivirus…

3 Sécuriser l'accès aux données de l'entreprise

Un certain nombre de solutions simples et peu coûteuses vous permettent de limiter le risque de fuite, de perte d'informations ou d'attaque du SI, dans le strict respect, bien entendu, de la vie privée de vos salariés. Il est recommandé de commencer par catégoriser vos données et de sécuriser celles que vous considérez comme sensibles. Afin de sécuriser le système informatique de votre entreprise, vous pouvez par exemple installer un réseau wi-fi "guest" réservé aux terminaux de vos salariés et des personnes extérieures à la société. Il est aussi possible de mettre en place un portail dont l'accès de chaque utilisateur est sécurisé (identifiant, mot de passe…) et paramétré selon des niveaux d'autorisation différents. Autre option, établir un contrôle à distance, par exemple bloquer l'accès au SI à certaines heures de la journée ou en cas de vol ou de perte du terminal. «*Avant d'initier quoi que ce soit, intéressez-vous d'abord au type d'usage professionnel que vos salariés font de leurs terminaux personnels*, préconise Arnaud Cassagne, directeur technique chez Nomios, intégrateur réseau et sécurité. *Le BYOD n'est finalement pas tant un projet technique qu'une problématique managériale.*»

« La majeure partie des attaques d'un système informatique en entreprise est due à la négligence des utilisateurs. »
Arnaud Cassagne,
directeur technique, Nomios

4 Impliquer ses collaborateurs

Pour que ces règles et ces mesures soient efficaces, encore faut-il sensibiliser vos salariés régulièrement. «*La majeure partie des attaques d'un système d'informatique en entreprise est due à la négligence des utilisateurs*, constate Arnaud Cassagne (Nomios). *Ainsi, n'hésitez pas à rappeler plusieurs fois par an à vos salariés de ne pas laisser leurs terminaux sans surveillance, de choisir des mots de passe sécurisés, de signaler systématiquement toute perte ou tout vol de matériel, ou encore de sauvegarder régulièrement les fichiers qu'ils utilisent.*»
Cela peut se faire dans le cadre d'ateliers de groupes, par l'envoi d'e-mails de rappel réguliers ou bien via l'élaboration d'un document didactique… L'idée étant d'expliquer simplement, exemples concrets à l'appui, l'intérêt d'une telle démarche pour l'entreprise comme pour le salarié. En la matière, mieux vaut toujours prévenir que guérir.

MARION PERROUD
→ mperroud@chefdentreprise.com

→ CE QU'IL FAUT **RETENIR**

- Le BYOD (utilisation de terminaux personnels à des fins professionnelles) fait peser des risques sur la sécurité de votre système informatique.
- Mieux vaut initier une réflexion globale sur la question plutôt que de proscrire cette pratique.
- Mettez en place des solutions techniques et managériales.
- La sensibilisation et l'implication de vos équipes restent les clés d'une stratégie réussie.