STORMSHIELD

TÉLÉTRAVAIL ET CYBERSÉCURITÉ

COMMENT ALLIER MOBILITÉ ET SÉCURITÉ INFORMATIQUE ?

Julien Paffumi
Product Management Leader, Stormshield

Pratiqué par de plus en plus d'entreprises et prisé par les salariés, le télétravail est en plein essor. Une tendance forte, voire forcée, qui nécessite toutefois quelques précautions de la part des entreprises et des administrations, pour ne pas avoir de mauvaises surprises en matière de protection des données. Si les entreprises et administrations disposent des solutions technologiques et du cadre juridique nécessaires pour développer le télétravail, elles ont encore malgré tout de bonnes raisons de s'inquiéter pour leurs conditions de sécurité.

TÉLÉTRAVAIL : UNE PRATIQUE QUI SÉDUIT, MAIS PAS SANS RISQUES INFORMATIQUES

Selon une étude menée en France par Stormshield et l'Usine Digitale auprès de 200 responsables informatiques, 62% des personnes interrogées estimaient fin 2018 que le télétravail était déjà la principale question de sécurité à résoudre pour les entreprises. Un chiffre qui a fortement dû grandir avec la généralisation forcée de cette pratique, suite aux grèves dans les transports fin 2019 et surtout au confirment de début 2020. Désormais, la sécurité de l'entreprise doit aussi se penser en dehors de ses murs.

Trois types de risques doivent particulièrement être anticipés :

- l'impossibilité, pour le salarié, d'accéder aux ressources dont il a besoin pour travailler,
- la contamination du système de l'entreprise par le biais d'une faille de sécurité de l'appareil de l'employé (et réciproquement),
- la fuite ou la perte de données.

Selon une autre étude réalisée par un acteur de la cybersécurité, près de 9 employés sur 10 utilisent leur matériel informatique personnel à des fins professionnelles, et 42% d'entre eux déclarent ne pas mettre à jour régulièrement leur système de sécurité. De quoi donner des sueurs froides aux DSI pour garantir la sécurité des informations sensibles de l'entreprise.

L'ENJEU DE SÉCURISER LES ACCÈS DISTANTS

C'est un élément de la transformation numérique où l'entreprise s'expose : les terminaux du salarié et l'accès à ses données multiplient les brèches potentielles. La mobilité, le digital workplace (le fait de retrouver son espace de travail partout, quels que soient la connexion ou le terminal utilisés) ainsi que l'internet des objets offrent autant de possibilités nouvelles de transformation que de possibilités d'attaques et de préjudices. Le salarié devient certes plus autonome et plus performant, l'entreprise va plus vite – **mais comment faire pour que ce ne soit pas au détriment de la sécurité ?**

Les entreprises qui veulent ainsi ouvrir leur système d'information vers le travail hors des murs doivent prendre des précautions élémentaires, notamment pour :

- authentifier les utilisateurs et définir les politiques d'accès ;
- assurer l'accès aux applications et services internes à distance ;
- sécuriser les communications.

Pour répondre à cet enjeu, selon cette même étude menée par Stormshield et l'Usine Digitale, 76% des personnes interrogées ont mis en place un système d'accès distant via VPN (Virtual Private Network) dans le cadre de leur transformation numérique.

L'ENJEU DE PROTÉGER LES DONNÉES DES TERMINAUX

En complément de la mise en place de réseaux privés virtuels, les données présentes sur les terminaux (ordinateurs, smartphones, tablettes) doivent également être protégées. En effet, 42% des DSI estiment qu'il faudrait mieux sécuriser les terminaux dont les utilisateurs se servent lorsqu'ils sont en situation de mobilité ou en télétravail.

Pour répondre à cette demande, le contenu du disque dur de l'appareil client doit alors être chiffré, de sorte qu'un malfaiteur qui se retrouverait en sa possession ne puisse pas l'examiner. Les fichiers sont alors placés dans un container, avec un chiffrement supplémentaire. Il peut prendre la forme d'un navigateur alternatif au système qui permet, une fois que l'utilisateur s'est authentifié, de manipuler les fichiers contenus sur le terminal comme ceux hébergés sur un service de stockage cloud.

SYSTÈMES D'IDENTIFICATION ET SOLUTIONS CLOUD AU CŒUR DE LA PROTECTION

Pour les entreprises, limiter les risques informatiques liés au télétravail passe ainsi par des mesures concrètes et des solutions techniques.

1. **Profiler les télétravailleurs.** Pour l'entreprise, il est essentiel de définir en amont des profils de télétravailleurs en fonction de leurs attributions et des informations sensibles auxquelles ils doivent ou non avoir accès. Entre les télétravailleurs occasionnels du week-end, ceux à temps partiel ou à plein temps, les mécanismes de sécurité ne sont pas les mêmes.

2. **Authentifier les accès à distance.** Le premier moyen d'éviter une intrusion étrangère dans le système de l'entreprise est d'instaurer un système d'identification du télétravailleur lorsqu'il s'y connecte (identifiant, mot de passe, code à usage unique…).

3. **Dissocier et protéger les appareils.** Au-delà d'un système de protection anti-virus, le moyen le plus simple d'éviter les risques de contamination entre le matériel de l'employé et le système informatique de l'entreprise est encore de réduire les droits d'administration au maximum sur la machine. Et donc d'attribuer au télétravailleur un PC à usage strictement professionnel, régulièrement mis à jour – au niveau sécuritaire – par le service informatique.

4. **Sécuriser l'accès aux données**. Afin de sécuriser les flux d'informations entre le poste du salarié et le réseau de l'entreprise, il est également possible d'utiliser un VPN (Virtual Private Network). Avec le développement du cloud, certaines entreprises mettent également en place des plateformes de bureau virtuel, qui permettent d'accéder n'importe où et sur n'importe quel appareil aux données sensibles de l'entreprise, sans y être directement physiquement connecté. La solution du cloud permet de décorréler l'authentification pour l'utilisation du poste, toujours difficile à protéger, de l'authentification pour l'accès à l'information sensible. Au final ce qui compte, c'est la sécurisation de la donnée stockée qui va transiter.

SENSIBILISER LES COLLABORATEURS AUX RISQUES INFORMATIQUES DU TÉLÉTRAVAIL

Mais toutes ces technologies ne seraient rien sans des précautions de base à prendre par le collaborateur nomade, moins soumis aux procédures de contrôle de l'entreprise, à savoir :

- la mise à jour de ses terminaux, aussi utile en dehors du périmètre de l'entreprise qu'à l'intérieur ;
- la dissociation des messageries personnelles et professionnelles ;
- la limitation de l'usage de périphériques externes (clés USB, disques durs…) pour transférer des données d'un ordinateur à l'autre ;
- l'activation de son VPN en déplacement (hôtel, lieu de restauration ou en transit) ;
- le verrouillage de son poste, dans des espaces de coworking comme à domicile.

En réunissant ces conditions, le collaborateur en télétravail s'implique dans la sécurité du système d'information, comme s'il était au bureau. Il économise du temps et devient plus réactif, plus performant, tout en restant protégé, en ne donnant aucune prise aux failles de sécurité. Pour réussir ces nouveaux défis de transformation numérique, l'entreprise doit donc l'accompagner dans l'adhésion et la systématisation des bonnes pratiques via des sensibilisations régulières aux enjeux de sécurité informatique liés au télétravail.

Cependant, si cette sensibilisation est indispensable, elle ne suffit pas. Il n'est pas réaliste aujourd'hui d'imposer de trop fortes contraintes aux utilisateurs, et la sécurité informatique des entreprises ne peut pas reposer uniquement sur ce genre de mesures, qui restent de l'ordre de la prévention. Les solutions de sécurité déployées doivent donc ainsi répondre en parallèle à des exigences d'ergonomie, de fluidité et de simplicité. Être *cybersecurity-by-design* en somme.
