Lire cet article en ligne

Coronavirus Covid-19 et télétravail : Aspects relatifs à la protection des données

La pandémie du coronavirus (Covid-19) a incité de nombreuses entreprises à mettre en place des solutions de télétravail. La mise en place de ce type de dispositif exige de suivre des règles pour garantir la sécurité des systèmes d'information et des données traitées.

La CNIL a publié des recommandations pour aider à la bonne sécurisation des données personnelles dans ce contexte.

La crise sanitaire mondiale du coronavirus Covid-19 a nécessité la mise en place de mesures de confinement et de stricte limitation des déplacements aux seuls motifs indispensables. Les entreprises, associations, administrations ou collectivités qui en avaient la possibilité ont dû mettre en place le télétravail pour préserver au moins les activités essentielles que ce mode de fonctionnement peut permettre.

Certaines étaient déjà préparées au télétravail, mais pas pour y faire face de manière aussi massive et en s'inscrivant autant dans la durée. D'autres ont dû le mettre en place dans l'urgence, peut-être même « à distance ». Dans certains cas, et faute d'avoir pu déployer les moyens nécessaires, le télétravail s'opère même depuis les équipements personnels des collaborateurs (dans le cadre du BYOD, ou *Bring your own device*), dont le niveau de sécurité ne peut pas être évalué et encore moins garanti et au sein duquel la frontière entre vie privée et vie professionnelle est plus délicate à tracer.

Parallèlement, on peut observer une intensification des activités de cybercriminels qui, comme dans toute situation exceptionnelle, cherchent à en profiter.

L'employeur est responsable de la sécurité des données personnelles de son entreprise, y compris lorsqu'elles sont stockées sur des terminaux dont il n'a pas la maîtrise physique ou juridique, mais dont il a autorisé l'utilisation pour accéder aux ressources informatiques de l'entreprise.

Les risques contre lesquels il est indispensable de se prémunir vont de l'atteinte ponctuelle à la disponibilité, l'intégrité et la confidentialité des données, à la compromission générale du système d'information de

l'entreprise (intrusion, virus, chevaux de Troie, etc.).

Comment les réduire ?

Cet article revient sur les bonnes pratiques à suivre pour mettre en place et gérer le télétravail.

Sécuriser le système d'information

L'ouverture vers l'extérieur du système d'information de l'entreprise peut engendrer des risques sérieux de sécurité qui pourraient la mettre à mal, voire engager sa survie en cas de cyberattaque. Il est primordial de sécuriser le système d'information sur lequel elle repose, en mettant en œuvre les recommandations suivantes :

- Éditer une charte de sécurité dans le cadre du télétravail ou, dans le contexte actuel, au moins un socle de règles minimales à respecter, et communiquer ce document à vos collaborateurs suivant le règlement intérieur. Privilégier autant que possible pour le télétravail l'utilisation de moyens mis à disposition, sécurisés et maîtrisés par l'entreprise. Lorsque ce n'est pas possible, donner des directives d'utilisation et de sécurisation claires aux employés en ayant conscience que leurs équipements personnels ne pourront jamais avoir un niveau de sécurité vérifiable ;
- Si cela est nécessaire, modifier les règles de gestion du système d'information pour permettre le télétravail (changement des règles d'habilitation, accès des administrateurs à distance, etc.), mesurer les risques encourus et, si besoin, prendre les mesures nécessaires. En particulier, limiter l'ouverture des accès extérieurs ou distants (RDP) aux seules personnes et services indispensables, et filtrer strictement ces accès sur le pare-feu. Cloisonner les systèmes pour lesquels un accès à distance n'est pas nécessaire pour les préserver, surtout s'ils revêtent un caractère sensible pour l'activité de l'entreprise ;
- Équiper tous les postes de travail des salariés au minimum d'un pare-feu, d'un antivirus et d'un outil de blocage de l'accès aux sites malveillants ;
- Mettre en place un VPN (*Virtual Private Network* ou réseau privé virtuel) pour éviter l'exposition directe des services sur internet, dès que cela est possible, en activant si possible l'authentification du VPN à deux facteurs. Outre le chiffrement des connexions extérieures, ce dispositif permet également de renforcer la sécurité des accès distants en les limitant aux seuls équipements authentifiés.

Services sur internet

Pour internet, il est recommandé de :

- Utiliser des protocoles garantissant la confidentialité et l'authentification du serveur destinataire, par exemple *HTTPS* pour les sites web et *SFTP* pour le transfert de fichiers, en utilisant les versions les plus récentes de ces protocoles ;

- Appliquer les derniers correctifs de sécurité aux équipements et logiciels utilisés (VPN, solution de bureau distant, messagerie, vidéoconférence etc.), et consulter régulièrement le bulletin d'actualité CERT-FR[1] pour être prévenu des dernières vulnérabilités sur les logiciels et des moyens pour s'en prémunir ;
- Mettre en œuvre des mécanismes d'authentification à double facteur sur les services accessibles à distance pour limiter les risques d'intrusions ;
- Consulter régulièrement les journaux d'accès aux services accessibles à distance pour détecter des comportements suspects ;
- Ne pas rendre directement accessibles les interfaces de serveurs non sécurisées. De manière générale, limiter le nombre de services mis à disposition au strict minimum pour réduire les risques d'attaques.

---

[1] https://www.cert.ssi.gouv.fr/actualite/