Les outils pour assurer la sécurité des applications et des données

SOMMAIRES

1. Introduction
2. Une sécurisation de l’entreprise.
3. Une sécurisation des employés
4. Conclusion
5. Webographie et Glossaire

Introduction

Le régime juridique du télétravail est inscrit dans le Code du travail, qui définit le statut et les droits du télétravailleur ainsi que les conditions de mise en place du télétravail dans une entreprise.

La crise du Covid a été l'occasion d'appliquer l'article L.1222-11 du Code du travail et de généraliser le recours au télétravail sans possibilité de refus du salarié. Cet article de loi prévoit en effet qu'en cas de menace d'épidémie « la mise en œuvre du télétravail peut être considérée comme un aménagement du poste de travail rendu nécessaire pour permettre la continuité de l'activité de l'entreprise et garantir la protection des salariés ». Aucun avenant au contrat de travail n'est nécessaire : un salarié peut donc passer en télétravail sans formalisme particulier.

Mais cela pose beaucoup de problèmes sur divers aspects, mais surtout sur la sécurité du travail et de l’espace de travail de l’entreprise, dans un réseau interne donc dans l’entreprise, sécurisée les données internes est plutôt simple même s'il faut quand même faire attention, mais lorsqu’il s’agit de travail à distance et encore plus si celui-ci n’est pas préparée comme ce qui est arrivée lors du premier confinement pour beaucoup d’entreprises, les conséquences peuvent être catastrophiques .

Car en cas de problème de sécurité celle-ci peuvent subir diverses attaques comme DDOS, vol de données, ransomwares, keyloggers ce qui peut venir grandement gêner le travail de l’entreprise voir même le stopper et ici, c’est donc la pérennité de l’entreprise qui est mise en jeu et il est donc important de sécuriser le télétravail du côté des employés comme de l’entreprise.

Une sécurisation de l’entreprise.

- Une entreprise doit donc ouvrir son réseau vers l’extérieur lors de la mise en place d’un cadre de télétravail, pour commencer pour reprendre l’exemple de la vague massive de mise en place du télétravail lors du premier confinement, les entreprises forcer de faire du télétravail, ont du ouvrir leur Firewall pour beaucoup car elle ne pouvait et n’avait pas pour beaucoup le temps de sécuriser leurs réseaux pour l’extérieur ce qui a donner lieu a une porte ouverte vers ces réseaux pour les hackers, une augmentation accrue des cyberattaque donc lors de ce changement de masse, dans une époque ou les cyberattaques se multiplient (+569 % selon Interpol et +600 % selon l’ONU pour le premier confinement) il est important de bien sécuriser son réseau d’entreprises et cela par diverses méthodes :
- Fournir les outils de sécurité (Ex : un bon antivirus) pour assurer la sécurité des applications et

des données, si possible fournir un ordinateur professionnel qui serait utilisable a but purement professionnel en limitant les activités et possibilité sur celui-ci afin d'éviter des failles de sécurités venant ici de l'employer.

- L'entreprise peut mettre en place une méthode avec une approches comme le Zero Trust Network Access qui mets en place plusieurs couches de protections et d'identifications et en limitant les accès sur le serveur que au documents nécessaires par les employées pour leur travail afin de limiter les accès sur le serveurs ainsi que d'éparpiller les accès à des endroits non-nécessaire par ceux-ci et donc limiter les risques d'intrusion sur le réseau de l'entreprise.
- Utiliser des outils de cloud/drive de manière sécurisé, maintenir les outils de sécurités du/et le réseau à jours afin de résoudre et d'éviter d'éventuelles faille de sécurités.
- Réalisées des sauvegardes seront parfois le seul moyen pour l'entreprise de recouvrer ses données suite à une cyberattaque. Les sauvegardes doivent être réalisées et testées régulièrement pour s'assurer qu'elles fonctionnent ainsi aussi, il faut que les données sauvegardées soient cryptées afin d'avoir un risque minimum.

Une sécurisation des employés

Il est aussi essentiel afin d'assurer une bonne sécurité en cas de télétravail, que la sécurité viennent aussi des première personne que cela concernent, les employés. Pour cela voici diverses méthodes afin de bien sécuriser les applications et données manipulées par les employés.

- Il faut avoir une politique stricte de déploiement des mises à jour de sécurité. Mettre ses outils connectés à jours afin de garder une sécurité optimum, car celle-ci corrige les divers failles de sécurité trouver récemment et/ou améliore leurs sécurités cela inclus les outils application et sécurité interne a ses outils, comme un antivirus sur tous les appareils afin de garantir une bonne sécurité de votre espace de travail et du réseau interne de l'entreprise, ainsi qu'un bon antivirus que l'entreprise devrait fournir si possible.
- Renforcez la sécurité des mots de passe et modifiez les souvent sur les postes de travail que vous utilisez sur votre lieu de travail à distances ou utilisez des outils de cryptage des mots de de passes (comme BitLocker ou BitWarden) afin de minimiser les risques de hacking ou d'intrusion dans le réseau de l'entreprise car en télétravail celle-ci s'effectue ici a distance et donc il est beaucoup plus facile pour un hacker de s'infiltrer dans un réseau a distance et faire ce qu'il lui plaît dans les limites du possible.
- Se connecter sur un réseau wifi sécurisé en permanence lorsque vient le travail, une connexion wifi sécurisé est primordial surtout lorsqu'il s'agit de la vôtre et non celle de l'entreprise et sauvegarder son travail en crypté sur un autre support sécurisé comme un drive afin d'éviter une perte en cas de suppression des données, mais limitées l'utilisation de périphériques externes.
- Et aussi faire en sorte que même en dehors de l'entreprise, les règles de la charte informatiques soit respecter, un employé ne doit pas faire en télétravail ce qu'il ne ferait pas au bureau.

Conclusion

Dans un contexte de télétravail, la sécurité des applications et des données est essentiel afin de

pouvoir garantir la continuité du travail de l'entreprise dans de bonnes conditions et sans problèmes.

Mais cette sécurisation doit venir des deux parties, entreprise comme employé doivent-être complémentaire afin de garder une sécurité optimum et garder l'activité de l'entreprise à flot et pérennisé son activité même a distance.

Sources

- https://teletravail.fr/connexions-et-securite/
- https://www.journaldunet.com/solutions/dsi/1496419-teletravail-comment-proteger-les-entreprises-contre-la-recrudescence-des-cyberattaques/
- https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail
- https://www.stormshield.com/fr/actus/teletravail-et-cybersecurite-comment-allier-mobilite-et-securite-informatique/
- https://www.silicon.fr/avis-expert/teletravail-la-flambee-dattaques-dans-le-cloud-montre-que-les-entreprises-netaient-pas-pretes
- https://www.itforbusiness.fr/teletravail-et-rgpd-comment-eviter-la-faille-de-securite-19128

par Dorian.K et Matteo.G