UNIDEES
IT & Security Compliance

Guide de cyber sécurité du télétravail

Avec la pandémie mondiale de coronavirus (COVID-19) annoncée par l'OMS et les recommandations, incitations et même parfois les obligations légales, de nombreuses entreprises et organismes prennent des mesures rapides pour en limiter la propagation. Le télétravail est au cœur de ces efforts. Bien que les mécanismes de travail à distance puissent être efficaces pour ralentir la propagation du COVID-19 d'une personne à l'autre, ils présentent des défis de cyber sécurité qui sont différents du travail sur site.

Vous trouverez dans ce guide des conseils pour préparer la mise en application du télé travail et les 10 recommandations pour aider les entreprises à relever le défis de sa cyber sécurité.

” Politique ”

Passez en revue votre sécurité actuelle des informations et d'autres politiques similaires pour déterminer s'il existe des directives de sécurité établies pour le travail à distance et l'accès à distance aux systèmes d'information de l'entreprise. Certaines organisations peuvent avoir des politiques spécifiquement conçues pour le travail à distance, tandis que d'autres peuvent prévoir des éventualités dans les plans de reprise après sinistre, les politiques BYOD (apportez votre propre appareil) et d'autres plans et politiques similaires.

Si aucun plan ou politique pertinent n'est en place, c'est le bon moment pour établir au moins quelques directives de base pour aborder l'accès à distance aux systèmes d'information de l'entreprise et l'utilisation par les employés d'appareils personnels pour les affaires de l'entreprise.

Il est recommandé de proscrire l’utilisation d’appareil personnel pour tout accès à distance au système d’information. Si cette mesure n’est pas possible compte tenu de l’urgence de donner accès aux employés pour assurer la continuité de l’activité et la non disponibilité en quantité suffisante d’appareil professionnel (laptop) il est de mise de procéder à quelques mesures d’hygiènes (récapituler à la fin de ce document).

” Communication ”

Tous les managers de l’entreprise doivent être familiarisés avec les directives, plans et politiques de sécurité applicables et veiller à ce que les informations pertinentes soient transmises à leurs équipes et dans l'ensemble de l'organisation. Il est essentiel que l'organisation soit alignée de haut en bas. N'oubliez pas que la plupart des employés n’ont aucune connaissance en sécurité et que certains n'ont peut-être jamais travaillé à distance auparavant. Il est donc essentiel de fournir des conseils et un cadre précis de travail à distance sécurisé à tous les employés pour leur permettre de continuer à travailler et à assurer leur mission.

Les situations d’urgence étant inévitables, les entreprises élaborent des plans de continuité d’activité.

Mettez à profit cette opportunité pour valider et adapter les hypothèses relatives au télétravail. Assurez-vous que votre VPN et votre stratégie de sécurité en général couvrent toutes les applications dont votre personnel a besoin pour accomplir son travail, où que ces applications soient hébergées. En suivant ces conseils, vous pouvez faire beaucoup pour assurer la sécurité de votre entreprise sans compromettre la productivité de vos employés.

“ Préparation ”

Les entreprises doivent examiner les plans de violation des données et de réponse aux incidents pour s'assurer que leur organisation est prête à répondre à une violation des données ou à un incident de sécurité. Mettez à jour les plans si nécessaire pour les informations de contact de l'équipe de réponse aux incidents à distance et des conseillers externes. Le risque de sécurité accru du travail à distance renforce la nécessité de mettre en place un plan en cas de problème.

Avec une quantité grandissante d’employés travaillant à domicile au milieu de l'épidémie de Covid-19, les serveurs VPN des entreprises sont désormais devenus primordiaux pour la dorsale d'une entreprise et leur sécurité et leur disponibilité doivent être au centre des préoccupations des équipes informatiques. **Il est très important que les services VPN soient corrigés et à jour car il y a beaucoup plus de tentative d’attaque contre ces services.**

Gardez les ressources informatiques en bonne santé et bien dotées en personnel. Lorsque plus d'employés que la normale travaillent à distance ou que le travail à distance est nouveau pour une organisation, les ressources informatiques peuvent être limitées et l'assistance informatique requise peut augmenter.

“Top 10 pour la cyber sécurité du télétravail“

1

Rappelez aux employés les types d'informations qu'ils doivent protéger. Cela comprend souvent des informations telles que des secrets commerciaux, la propriété intellectuelle de l’entreprise, les informations sur les clients, les informations sur les employés et d'autres informations personnelles (informations qui identifient une personne physique). Ces données qui sont stockées sur ou envoyées vers ou depuis des appareils distants doivent être cryptées lors de leur mouvement et au repos sur l'appareil et sur les supports amovibles utilisés par l'appareil.

Sensibilisez les employés sur la façon de détecter et de gérer les attaques de phishing et d'autres formes d'ingénierie sociale impliquant des appareils distants et l'accès à distance aux systèmes d'information de l'entreprise.

Il y a un nombre croissant d'e-mails de phishing basés sur le coronavirus qui circulent s'attaquant aux problèmes de santé du public.

2

3

Appliquer une hygiène irréprochable et obligatoires sur les postes nomades : antivirus (avec fonction firewall et IPS) installé et à jour (moteur & définition, systèmes et applications avec les derniers correctifs de sécurité, logiciel de connexion à distance (VPN client par exemple) dans sa dernière version stable et mise à jour, ….

4

Bloquez le partage d'ordinateurs de travail et d'autres appareils. Lorsque les employés ramènent des appareils de travail à la maison, ces appareils ne doivent pas être partagés avec ou utilisés par quiconque à la maison. Cela réduit le risque d'accès non autorisé ou par inadvertance aux informations protégées de l'entreprise.

Assurez-vous d'utiliser exclusivement des accès à distance chiffrés Les outils d'accès à distance de tous les employés doivent garantirent que le trafic Internet est crypté. Assurez-vous que les employés utilisent par exemple un VPN lorsqu'ils travaillent et lorsqu'ils accèdent à distance aux systèmes d'information de l'entreprise. Ceci est valable pour les employés de la DSI et les prestataires qui seraient amenés à effectuer des accès à distance pour des travaux de maintenance. N'oubliez pas que les accès à privilège sont particulièrement ciblés par les cyber criminel. Il faudra privilégiez des solutions de type PAM (Privileged Access Management) pour cette dernière population).

5

.

6

Mettez à jour vos systèmes, tous vos systèmes. Les systèmes qui sont ou seront exposés sur internet pour le travail à distance, même à travers un VPN, doivent être immédiatement à jour des derniers correctifs.

7

Faites des sauvegardes et conservez les hors ligne. La bonne pratique pour atténuer les conséquences d'une attaque est de vous assurer que votre entreprise dispose de sauvegardes à jour des données importantes (base de donnée, messagerie, serveur de fichier, …) . Vous devez vous assurer qu'une sauvegarde est conservée séparément du réseau - hors ligne - ou dans un service en nuage conçu à cet effet.

Limitez l'accès des employés aux informations protégées à la portée et à la durée minimales nécessaires à l'exercice de leurs fonctions. Ne pas permettre d'accès 24/7 mais uniquement aux mêmes horaires nécessaires que lors d'un accès sur site.

8

.

9

Envisagez la gestion des appareils mobiles (MDM) et la gestion des applications mobiles (MAM). Ces solutions peuvent aider à gérer et à sécuriser les appareils et applications mobiles. Ces outils peuvent également permettre aux organisations de mettre en œuvre à distance un certain nombre de mesures de sécurité, notamment le chiffrement des données, les analyses de logiciels malveillants et l'effacement des données sur les appareils volés.

Implémentez et appliquez l'authentification à deux facteurs ou à facteurs multiples (MFA). Si vous n'avez pas encore activé MFA, c'est le moment de le faire..

10

” Utilisation d’un dispositif personnel “

Même si cela n’est pas du tout recommandé, il sera difficile pour une entreprise de fournir un dispositif portable pour tous les employés dans ce contexte de pandémie Covid-19. Les dispositifs personnels pour le télétravail risque donc vraisemblablement de se généraliser et nous vous recommandons de prendre quelques mesures d’hygiènes.

→ C’est le moment parfait pour mettre en place une politique BYOD et ainsi gérer les données professionnelles conservées sur ces appareils personnels.

→ Ces dispositifs personnels ne pourraient se connecter à vos systèmes qu’après que vous ayez vérifié l’existence de mises à jour d’un logiciel antivirus (même gratuit) du système d’exploitation et des applications.

→ Les informations sur l'entreprise ne doivent jamais être téléchargées ou enregistrées sur les appareils personnels ou les services cloud des employés, y compris les ordinateurs des employés, les clés USB ou leurs comptes Google Drive ou Dropbox personnels.

→ Les fonctions «Mémoriser le mot de passe» doivent toujours être désactivées lorsque les employés se connectent aux systèmes d'information et aux applications de l'entreprise à partir de leurs appareils personnels.

N'oubliez pas, que les lois de lutte contre la fraude numérique et la protection des données à caractère personnel s'appliquent toujours pendant le coronavirus (#LOI0904DZ, #LOI1807DZ #RGPD).

Restez vigilant – la Cyber Sécurité n'est pas à l'abri du COVID-19 !