Parc d'Activités Schweitzer
26 rue du Bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

FICHE CONSEILS

TELE-TRAVAIL

TELETRAVAIL – ATTENTION !!

Challans,

Le 15/03/2020

Madame, Monsieur,

Par ce message, je souhaiterais vous faire part de ma préoccupation grandissante devant l'augmentation très significative des attaques informatiques qui ont eu lieu durant ces toutes dernières semaines en parallèle avec la prolifération du COVID-19. Vous êtes extrêmement nombreux à nous demander de mettre en place le Télé Travail. En période normal la mise en place de télétravailleurs demande réflexion et mini audit. Nous sommes en situation d'urgence, cependant il ne faut pas confondre vitesse et précipitations. Nous vous conseillons vivement de lire les lignes suivantes écrite en collaboration avec notre expert en Cyber Sécurité, notre directeur technique et Microsoft (pour certains points).

- **Mettre en place un Firewall performant avec adhésion aux mises à jour de service de sécurité**. Ce firewall, (pare-feu) permettra d'éviter les intrusions et les connexions à distance non autorisées. Attention aux Boxs avec des identifiants MDP d'origines ou trop simples !!
- **Equiper correctement les télétravailleurs.** L'ANSSI (Agence National pour la Sécurité de Systèmes d'Informations) déconseille très fortement l'utilisation de matériels personnels. En effet, l'entreprise ne maitrise pas l'outil. Celui-ci a pu être utilisé pour accéder à des sites non sécurisés ou illégaux, les anti-virus peuvent être périmés ou inexistants, les jeux et autres téléchargements de films sont très souvent porteurs de Virus, Malware et autres Vers. La connexion de ce type d'appareil au système d'informations de l'entreprise peut être dévastatrice. Nous sommes tout à fait d'accord avec l'ANSSI.
- **Connecté un télétravailleur n'est pas bénin.** Il existe plusieurs solutions pour connecter un télétravailleur, la 1ere consiste à ouvrir un port du routeur/firewall (porte ouverte sur le S.I.) (nous bannissons cette solution). Une autre solution consiste (si vous êtes équipé d'un firewall Sonicwall) d'installer une licence Global VPN pour être sécurisé (ceci ne dispense pas de se connecter avec un ordinateur sain (Bannir les ordinateurs familiaux). Il est bien entendu, proscrit de se connecter avec un ordinateur en W7 et inférieur. D'autres solutions plus ou moins sécurisées existent, nos ingénieurs avant-ventes sont là pour vous aider à adopter la meilleure solution sur mesure.

- **Encadrement administratif**. Nous vous conseillons vivement, de notifier sur un tableau la liste des connexions distantes (Ordinateurs, Mobiles) ainsi que les accès à la messagerie d'entreprise. L'idéal étant de faire signer aux collaborateurs un engagement de confidentialité et de protection du mot de passe (ne pas enregistrer le MDP sur l'ordinateur), ne pas laisser les enfants et autres personnes accéder à l'appareil. La tenue d'un inventaire permet de ne pas oublier de supprimer les accès après le besoin ou au départ du collaborateur. Rien de pire que de laisser un accès distant possible à Vitam Aeternam. La mise en place de votre Charte Informatique est primordiale.
- **Protection du poste**, vous devez vous assurer que le poste est équipé d'un anti-virus et que celui-ci soit le même que celui de l'entreprise afin d'éviter des incompatibilités engendrant des bugs (Très courant). Interdisez l'enregistrement des fichiers sur le poste distant (pas de sauvegarde, problème éventuel de confidentialité). Je répète le poste ne doit être utilisé que par le collaborateur.

- **Gérer les identités et leur cycle de vie au sein de votre système d'information** ; en effet, selon le statistiques Microsoft, 81% des attaques découlent du vol d'un mot de passe, 73% de ceux-ci étant dupliqués. En particulier, nous vous conseillons de limiter au maximum les comptes bénéficiant de droits spécifiques qui sont des cibles privilégiées des attaquants qui souhaitent obtenir un accès le plus large possible au système d'information ; ces comptes doivent donc faire l'objet d'une attention toute particulière. Nous vous conseillons également, dans la mesure du possible, de mettre en place une authentification multi-facteur en lieu et place du mot de passe traditionnel ; en effet, la mise en place d'une telle approche réduit ce type de compromissions de plus de 99%.
- **Mettre à jour systématiquement et en continu vos systèmes d'exploitation, vos applications, vos pilotes de périphériques et vos firmwares** ; trop d'attaques restent en effet possibles en raison d'une mise à jour trop tardive ou manquante. A ce titre, nous vous rappelons que le support de Microsoft Windows 7 a pris définitivement fin le **14 janvier 2020** et le support de Microsoft Office 2010 prendra définitivement fin **le 13 octobre 2020**. Pour Office, nous vous recommandons vivement de migrer vers une version pleinement supportée avant le 13 octobre 2020. Votre Firewall doit faire l'objet d'un contrat de mise à jour.
- **Mettre en place des dispositifs anti-phishing et former tous vos collaborateurs à reconnaitre ce type d'attaque** ; en effet, le phishing reste l'un des moyens préférés des attaquants pour pénétrer au sein des systèmes d'information. Cependant, depuis le début d'année nous constatons une

recrudescence des piratages exploitant les failles de W7 et l'accès des pirates via des ports ouverts de la Box ou du Routeur/Firewall.

Je suis désolé de rajouter de mornes informations au marasme actuel. Cependant nous estimons qu'il est de notre devoir de vous aider à éviter des erreurs fatales pour votre S.I.

- **Bonne nouvelle.** En tant que partenaire Microsoft, nous sommes autorisés à vous fournir l'accès à la brique "Teams" de Microsoft Office 365 gratuitement pendant une période de 6 mois que vous soyez ou non abonnés à Office 365. Seul un forfait de 45€ht/utilisateur vous sera facturé pour la mise en place du portail et la configuration des utilisateurs. Microsoft met à votre disposition des didacticiels et Tuto pour vous aider à démarrer.

Je vous prie d'agréer Madame, Monsieur, l'expression de mes sincères salutations.

Yann BELZ

Espace Technologie

Notre Expert cyber Sécurité
Espace Technologie

Plus d'informations sur nos prestations contactez-nous :

ESPACE TECHNOLOGIE
Parc d'Activités Schweitzer
26 rue du Bois Fossé - BP 147
85301 CHALLANS Cedex
Tél. 02 51 49 31 31

www.espace-technologie.com
contact@espace-technologie.com