Cyber sécurité en entreprise versus Cyber sécurité à la maison

AMUSEC 2021

Yves Jehanno

Contexte

- La crise sanitaire majeure que traverse les pays du globe oblige à une refonte de nos manières de travailler.
- Le salarié doit partager son activité sur plusieurs points géographiques distincts et ne disposant pas des mêmes niveaux de sécurité
- Le tout en respectant les gestes barrières de la cyber sécurité

Le principal bouleversement

- La mise en œuvre du télétravail
  - Avec quels moyens ?
  - Avec quel niveau de responsabilité ?
  - Avec quel niveau de sécurité ?

- Question : Qu'elles sont les informations utilisables en dehors de l'entreprise ?

Conséquence de l'explosion du télé travail

- Dans sa dernière étude sur la "productivité du travail et l'équilibre entre vie professionnelle et vie privée", EAE Business School souligne que la crise du Covid-19 a fait augmenter le télétravail en Espagne de 88% dans les entreprises contre 4% avant la crise. Mais cette explosion du télétravail s'est accompagnée d'une forte augmentation des cyberattaques

Principales cyber menaces

- Phishing : Il s’agit de se faire passer pour une personne ou une entreprise de confiance pour demander généralement de cliquer sur un lien ou un fichier et d'obtenir ainsi des informations sensibles.
- Ransomware : Le cybercriminel prend le contrôle et "kidnappe" l'information en la cryptant. Pour pouvoir la récupérer, il faut alors payer une rançon.
- Attaques sur le Cloud : Par le biais de ces attaques sur le nuage, les cybercriminels recherchent le vol de nos données et ainsi pouvoir accéder à des informations sensibles personnelles ou professionnelles.
- Cryptojacking : Dans ce cas, l'attaque consiste à utiliser les ressources de notre ordinateur. Le cybercriminel peut prendre le contrôle de notre ordinateur pour effectuer ces opérations d'extraction, consommant ainsi nos ressources, qui seront ensuite facturées.

Méthode pour une 1ère évaluation

- Identifier ce qu'on doit protéger
- Lister les risques potentiels
- Lister les mesures de protection en place
- Améliorer celles qui semblent insuffisantes
- Vérifier l'efficacité des mesures
- Adopter un comportement responsable
  - 80% des problèmes de la cyber sécurité se situent entre la chaise et le clavier…

Que protéger ?

- Une information dont la perte / vol porte préjudice à l'entreprise ou à soi même
  - Information militaire / stratégique /industrielle / juridique etc..
- Une information régit par des textes de loi et soumis à une ou plusieurs réglementations
  - Données personnelles, données bancaires, etc..
- Une information dont la perte/vol nous affecte directement
- Un moyen de production, une chaîne de fabrication…

Quels sont les risques ?

- En matière cyber sécurité, on pense naturellement au vilain pirate qui va attaquer notre environnement informatique pour voler nos données, les revendre ou encore faire du chantage financier après demande de rançon
- On oublie souvent que tout cela est possible à cause de notre cyber négligence

La cyber négligence ?

- Utiliser un système obsolète (OS, antivirus, pare-feu)
- Ne pas tenir compte des alertes de sécurité
- Ne pas chiffrer les informations sensibles
- Renseigner les attaquants grâce aux réseaux sociaux
- Modifier les paramètres de sécurité car notre machine est « trop lente »
- Avoir un comportement à risque en allant sur des sites potentiellement dangereux
- Avoir un mot de passe trop simple ou identique pour toutes nos applications, l'écrire en clair sur un post-it,
- Se connecter sur un réseau dont on ignore le niveau de sécurité
- Connecter un périphérique sur son environnement sans être certain qu'il est sans danger
- Mélanger les moyens informatiques de l'entreprise avec les moyens personnels
- Etc..

La cyber transgression

- Selon la société de cyber sécurité Tessian, 52 % des employés pensent qu'ils peuvent s'en tirer avec des comportements plus risqués lorsqu'ils travaillent à domicile, comme le partage de fichiers confidentiels par courrier électronique
- Les principales raisons de cette modification comportementale est le fait de travailler à partir de leur appareil personnel et qu'ils ne sont pas surveillés par les services IT de l'entreprise.
- A cela s'ajoutent les « distractions » accessibles au domicile et qui n'existent pas au bureau

- La vigilance naturelle est réduite. Le télétravailleur devient une nouvelle cible plus accessible pour atteindre les entreprises.

Comment se protéger ?

- Diviser
  - Diviser notre infrastructure en appliquant le principe du droit d'en connaître
- Mettre à jour
  - Faire une veille sécurité et se mettre à jour en permanence
- Renforcer les dispositifs d'authentification
  - Privilégier authentification à double facteur
- Surveiller et traiter les alertes de sécurité remontées par les systèmes
- Chiffrer les données pour les rendre inaccessibles

9 règles simples

- **1. Fermer sa porte**
  - Il ne vous viendrait jamais à l'idée de laisser ouverte en permanence la porte de votre domicile. Pour votre entreprise, c'est pareil. Il faut même utilisez une porte blindée pour réduire les risques de cambriolage :
  - Installez des antivirus et antimalwares.
  - Mettez à jour les logiciels pour éviter qu'ils ne servent aux criminels à rentrer chez vous.
  - Bloquez ou régulez les ports USB.
  - Protégez et sécurisez votre site internet.
  - Enfin sécurisez les accès physiques à vos locaux et à vos serveurs.
- **2. Ne pas laisser traîner ses clefs**
  - Dans l'entreprise, « laisser traîner ses clefs », c'est avoir une gestion laxiste des mots de passe
- **3. Cacher les bijoux de famille**
  - En sécurisant vos serveurs, en sauvegardant vos données et en en contrôlant leur accès, vous rendrez difficilement accessible ce qui fait la valeur de votre entreprise, même si un voleur réussit à entrer chez vous.

9 règles simples

- **4. Ne pas laisser entrer un inconnu**
  - Ne téléchargez pas de logiciels inconnus, porteurs potentiels de virus.
  - N'ouvrez pas de pièces jointes provenant d'une personne inconnue, ou du moins prenez le temps de faire une analyse du message, ne vous précipitez pas : les rançongiciels entrent fréquemment par ce biais dans les réseaux informatiques.
  - Méfiez-vous des appels et des courriels imitant ceux d'un organisme officiel et qui demandent, par exemple, de transmettre des coordonnées bancaires.
- **5. Prendre une bonne assurance**
  - Votre activité vous appartient, protégez-la des cyberattaques en souscrivant une cyber-assurance. La mise en place de celle-ci est déjà, en soi, une démarche de sécurisation poussée puisque l'assureur peut imposer un audit, des procédures claires pour chaque risque, et l'installation de produits et services de sécurité
- **6. Prendre vos précautions lors de vos déplacements**
  - Votre ordinateur et votre téléphone doivent être sécurisés et vos écrans masqués. Vous ne devez emporter que le minimum de données sensibles. Il vous faut fuir les WiFi public… La cybersécurité de l'entreprise se joue en effet aussi hors de l'entreprise.

9 règles simples

- **7. Pour vivre heureux, vivons cachés**
  - Dans l'entreprise, affichez une discrétion indispensable sur les réseaux sociaux. Ces derniers représentent en effet une mine d'informations pour les cybercriminels dans la préparation de leurs attaques.
- **8. Rester vigilants**
  - Sensibilisez et formez vos collaborateurs : la cyber sécurité est l'affaire de tous ! Aidez-les à comprendre les cyber menaces et à signaler les comportements suspects.
  - Surveillez les menaces, faites de la veille
  - Soyez informé des nouvelles solutions de cyber sécurité qui pourraient utilement protéger votre activité
- **9. En cas de problème, appeler les voisins à l'aide**
  - Trop souvent, les entreprises subissant une attaque se défendent seules, font profil bas, voire ne portent pas plainte, de peur que cet événement ne ternisse leur image auprès de leurs clients. L'entreprise doit utiliser tous les leviers à sa disposition pour gérer la cyber-crise. Outre le dépôt de plainte, rendez-vous sur Cybermalveillance.gouv.fr pour vous faire guider.

Conclusion

- En matière de cyber sécurité que l'on soit dans l'entreprise ou à la maison, on s'aperçoit qu'il n'est pas nécessaire d'être un spécialiste pour appliquer les règles du bon sens.
- Il est également important de changer notre attitude face aux risques cyber dont l'une des principales armes des cyber criminels est de réussir à isoler la victime qui n'ose pas demander de l'aide.

- L'adage « Diviser pour mieux régner » constituant la force principale des cyber-attaquants, il devient nécessaire que nous partagions nos expériences pour progresser vers un monde plus résilient.