Théo Fréret, Alerig Cuvillier, Louis Beghin, Marc Tahon-Dujardin

Hygiène informatique et cybersécurité

Groupe 4

20/09/21

Volet 1 : Énumération des risques

Les risques				
■ (Probabilité qu'un risque se produise)	Très faible	Faible	Probable	Très probable
● (Impact des risques)	Négligeable	Mineur	Important	Critique
Hameçonnage				● ■
Matériel défectueux ou ancien			● ■	
Machines extérieures (BYOD)		■	●	
Envoi non sécurisé de fichier		● ■		
Accès à la salle de serveur	■		●	
Réseau local et/ou internet non sécurisé			■	●
Mots de passe mal organisés/sécurisés			●	■
Session impersonnelle et non sécurisée		■	●	
Risques d'incendie	■			●
Perte de données		■		●

Comme vous le voyez, rien n'est négligeable. Chaque risque se doit d'être pris au sérieux.

Volet 2 : Mesures à mettre en place

Les risques	Solutions apportées
Hameçonnage	Séminaire informatif sur l'hameçonnage.
Matériel défectueux ou obsolète.	Réparer et/ou remplacer le matériel.
Machine extérieure (BYOD)	Configurer un tunnel (VPN/tunnelisation) qui redirige sur les serveurs de l'entreprise afin de sécuriser les machines extérieures au réseau de l'entreprise (Exemple : OpenVPN).
Envoi non-sécurisé de fichier	Choisir un cloud, drive ou logiciel de transfert de données attitré à l'entreprise.
Accès à la salle de serveur	Mettre un déverrouillage électronique.
Réseau local et/ou internet non sécurisé	Borne Wi-Fi 6 sécurisé et WPA3 pour l'open-space ; Matériel à jour ; Antivirus sur chaque machine connectée.
Mots de passe mal organisés/sécurisés	Utilisation de gestionnaires de mot de passe tel que Keepass.
Session commune et non sécurisée	Mise en place de sessions pour chaque employé sécurisé par un mot de passe et possibilité de verrouillage.
Risque d'incendie	Climatisation de la salle des serveurs et achat d'un extincteur CO2
Perte de données	Mise en place d'un backup des serveurs une fois tous les trois jours. (Le serveur de backup n'a pas besoin d'être récent car il ne communique pas avec internet, mais seulement avec le serveur. Il servira uniquement de base de stockage.)

Volet 3 : Consignes à destination des salariés

Consigne 1 : Hameçonnage

Ne pas ouvrir les courriels douteux et ne procéder à des paiements/redirections que sur des sites recherchés par nous-même. Tout employé devra suivre un séminaire informatif de prévention à l'hameçonnage.

Consigne 2 : Machine extérieur

Hors du télétravail aucune machine ne sera admise au sein des locaux de l'entreprise.

Consigne 3 : Envoi de fichier

Utiliser le service de stockage de l'entreprise et uniquement celui-ci, si et seulement si le fichier transmis appartient à l'entreprise. Pour tout autre cas n'importe quel logiciel est utilisable.

Consigne 4 : Accès à la salle de serveur

La salle de serveur doit rester fermée en tout temps, et seul le personnel autorisé d'accès y est admis. En aucun cas un employé non-autorisé ne doit y entrer.

Consigne 5 : Gestionnaire de mot de passe

Chaque employé se doit d'avoir un gestionnaire de mot de passe (comme Keepass) organisé et à jour.

Consigne 6 : Le télétravail

En cas de télétravail, l'utilisation du VPN de l'entreprise est requis pour sécuriser les connexions entre l'entreprise et l'employé.

Consigne 7 : Sessions

Chaque employé possède une session dédiée et ne doit en aucun cas partager son mot de passe ou son identifiant avec un collègue ou autre.

Consigne 8 : Wifi de l'open-space

Pour garantir l'intégrité et la sécurité du réseau de l'entreprise le mot de passe du wifi de l'open-space ne doit pas être partagé avec des personnes extérieures à l'entreprise.

Volet 4 : Sources, matériels et logiciels

- Réseaux & Télécoms (périodique en ligne)
  www.reseaux-telecoms.net/
  Article : Un point d'accès WI-FI sécurisé pour le télétravail signé Palo Alto Networks
  13/09/2021
  (Wifi sécurisé type entreprise à la maison)

- Linkedin (réseau social professionnel)
  https://www.linkedin.com/
  Post de Loris Viarouge directeur marketing France chez Dell
  09/09/2021
  (Lien vers article de Stephane Huet sur comment se protéger et anticiper une cyber-attaque)

- Intrinec
  https://www.intrinsec.com/
  Blog : Bonnes pratiques - Luttez efficacement contre le phishing
  30/03/2020
  (Information concernant le phishing et les moyens de le contrer)

- Youtube
  https://youtu.be/
  Vidéo de prévention de Dell « Hameçonnage ou phishing : reconnaître un mail ou un faux site »
  29/07/2021
  (S'armer contre le phishing)

- XPR
  https://conseils.xpair.com/
  Article Web : Pourquoi climatiser les salles informatiques ?
  Décembre 2020

Solutions matériel		
Matériels	Prix	Maintenance
Extincteur CO2	~100€	Maintenance à faire une fois par an
Serveur de backup	~400€ - cout de mise en place indéterminé	Maintenance non nécessaire sauf panne et nettoyage (poussière)
OpenVPN	0€ - cout de mise en place indéterminé	Aucune
Antivirus	339,99 €/an	Aucune