EFCSE - ECSM – MATRICE DE RISQUE

Prenez le temps nécessaire pour observer les informations qui vous parviennent et les analyser afin de prendre les bonnes décisions.

Nous vous proposons ici un outil pratique et simplifié dans un contexte de cyber-attaque.

EUROPEAN CYBER SECURITY MONTH

Be secure,

Be on your toes

MATRICE DE RISQUES					
Probabilité / Impact	Insignifiant	Mineur	Modéré	Majeur	Critique
Rare	Débrancher accidentellement le cordon d'alimentation électrique du matériel				Connecter un périphérique externe à un système interne
Peu probable	Ancien matériel qui ne fonctionne plus	Coupure de courant entrainant la perte du travail en cours / perturbation du dispositif électronique	Oublier de verrouiller son ordinateur en quittant son poste de travail	Attaque par déni de service [(D)DoS]	Surchauffe de la salle des serveurs
Possible	Matériel défectueux (écran, unité centrale, souris, clavier...)	Oublier son mot de passe	Renverser du liquide sur un appareil électronique	Utiliser un service d'échange non sécurisé ou non adapté	Subir une catastrophe naturelle
Probable			Subir une attaque par outil de dissimilation d'activité [Rootkit]	Perdre une clef USB contenant des informations sur la société	Ouvrir ou télécharger des fichiers infectés
Quasiment certain		Accéder au réseau à distance	Erreur humaine accidentelle	Subir une cyber attaque	Être victime d'une cyber attaque

Avez-vous remarqué que la plupart des risques majeurs et critiques sont dus à des erreurs humaines ?

QUE FAIRE / COMMENT PREVENIR LES RISQUES ?					
Probabilité / Impact	Insignifiant	Mineur	Modéré	Majeur	Critique
Rare	Bien s'organiser pour éviter les problèmes				S'assurer qu'un périphérique inconnu est propre et exempt de toute menace pouvant affecter les périphériques internes
Peu probable	Disposer de matériel performant (neuf ou récent) pour les sauvegardes et les serveurs qui stockent les données	Configurer des sauvegardes automatiques / avoir toujours des sauvegardes	Faire en sorte que les ordinateurs se verrouillent automatiquement après un certain temps de non-activité	Avant : sur provision/ bande passante Pendant : appeler l'hébergeur Après : créer un référentiel d'attaque	Si vous êtes responsable des serveurs / salles des serveurs, assurez-vous qu'ils sont correctement ventilés afin qu'ils ne surchauffent pas.
Possible	S'assurer d'avoir toujours du matériel pour un remplacement de matériel défectueux	Changer les mots de passe avec suffisamment de logique / simplicité pour les mémoriser	Pas de liquide autour des appareils électroniques. Disposer de sauvegardes (juste au cas où...)	Choisir un fournisseur de services approprié	Soyez conscient des catastrophes naturelles pouvant avoir un impact sur vos activités et préparez-vous en conséquence
Probable			Sécuriser le système avec des programmes appropriés	Ne pas stocker des données sensibles sur une clef USB	Ne pas ouvrir ou télécharger des fichiers provenant de sources inconnues
Quasiment certain		Ne pas accéder au réseau de l'entreprise via un canal non sécurisé	Faire en sorte que le personnel/ collaborateurs soient sensibilisés et/ou formés aux bonnes pratiques	Avoir un antivirus performant sur chaque matériel numérique installé	Avoir des procédures en place pour réagir rapidement à l'attaque

EFCSE vous remercie pour votre participation au mois européen de la cybersécurité et vous invite à suivre ses publications au-delà de cet événement d'octobre 2019 dédié à la cybersécurité.