MySUSI

Sensibilisation des Utilisateurs à la Sécurité Informatique

Ci-dessous une description détaillée du programme de cette session de sensibilisation à la sécurité informatique
Le contenu s'adresse **à toute personne** dans l'entreprise et permet de prendre conscience de ce qu'est la sécurité informatique, les risques, menaces et enjeux. Cela permet aussi de transposer ces informations pour l'Internet à domicile qui est désormais toujours connecté avec de plus en plus d'équipements. Aujourd'hui tous les collaborateurs participent à la sécurité de leur entreprise.

La session est basée sur une **présentation** Microsoft Powerpoint **en français**. Les quelques démonstrations seront faites sur un ordinateur.

MySUSI embarque la présentation dans une application Windows autonome. Cela permet aux clients de disposer en interne du support complet de la session et des composantes externes (vidéos, documentations, démonstrations...). Ainsi la gestion des agendas et du temps interne à la société est beaucoup plus libre.

MySUSI nécessite à une personne de l'entreprise à minima de suivre le module "train the trainer", pour lui permettre de reproduire au plus proche l'interactivité avec les candidats durant la session.

Ce module est dispensé par AF software pour être le plus proche des messages d'origine. La personne suivant ce module doit avoir une expérience de 2-3 ans dans les réseaux et sécurité informatique.

Certains chapitres sont animés de vidéos explicatives et ludiques. En complément divers documents sont distribués durant la session.

Un **maximum** de **12 personnes par session** est recommandé.

- La sensibilisation à la sécurité informatique : Pourquoi ?
  - L'entreprise
  - Les utilisateurs
  - Les hackers
  - Les réglementations (PCI-DSS, ISO 27001, GDPR, OTAN SSI, etc...)
  - Statistiques
  - ROI

- Les objectifs

- Le Système d'Information (SI)
  - Le SI c'est quoi ?
  - Confidentialité
  - Intégrité
  - Disponibilité
  - Non répudiation
  - Importance dans l'entreprise

- Les bases & fondamentaux
  - Internet c'est quoi ?
  - Activité

- La sécurité informatique
  - Qu'est ce qu'est la sécurité informatique ?
  - La sécurité physique
  - La sécurité de l'exploitation
  - La sécurité logique
  - La sécurité applicative
  - Sécurité Entreprise vs Domicile
  - Qui s'en occupe
  - Vocabulaire

- L'analyse des risques
  - Les risques
  - A retenir
  - Statistiques
  - Evolution

- Les défauts de la sécurité informatique

- Les vulnérabilités
  - Définition
  - Détecter les failles
  - Cycle de vie d'une vulnérabilité

- Les risques & menaces
  - Définir les risques
  - Origine des risques
  - Chiffres
  - Objectifs & fondamentaux
  - Les 5 Objectifs
  - USB & CD

- Les enjeux
  - Financiers
  - Responsabilité Civile & Pénale
  - Opérationnels

- Le profil des attaquants
  - Définition du cybercriminel
  - Principales motivations du cybercriminel
  - Amateurs
  - Professionnels

- Les différent types d'attaques & méthodes
  - Les types d'attaques
  - A retenir
  - Méthodologie d'intrusion
  - Les outils
  - Etapes d'un ransomware
  - Temps réel

- La politique de sécurité
  - Analyse de la situation
  - Analyse des risques
  - Politique de sécurité
  - Mesures de sécurité
  - Implémentation
  - Validation

- Comment se protéger
  - Quoi protéger ?
  - Comment protéger ?
  - Les outils
  - Quelques réflexes
  - Réflexes en HTTP

- RGPD / GDPR (Module uniquement disponible pour des projets sur le sujet)
  - Comprendre
  - Généralités
  - Pour l'entreprise
  - Pour le collaborateur
  - Liens utiles

- Les smartphones & tablettes
  - Prévisions
  - Utilisation quotidienne
  - Statistiques
  - Attention
  - Les bons réflexes

- Les statistiques 2015 - 2016
  - Social Engineering
  - Malwares
  - Ransomwares
  - Failles par mois
  - Top des attaques
  - Top par éditeur
  - En résumé
  - Top du Phishing
  - Phishing activité
  - 2016 Ransomware « Locky »

- Les statistiques 2016 -> 2019
  - Evolution des ransomwares
  - Backdoors, Trojans, RAT's
  - Evolution des backdoors, Trojans, RATS's
  - NotPetya 3 mois après
  - Malwares sur Mac
  - Top 10 des cyberattaques

- Les menaces de demain

- Des exemples & coûts
  - St Gobain / Fedex / Merck
  - Comptes volés
  - Exemple de site Web « defaced »
  - Car Hacking
  - Evolution

- Le Darknet
  - C'est quoi ?
  - On trouve quoi ?
  - Paiement ?
  - Bitcoin, comment cela fonctionne ?

- Les démonstrations
  - Microsoft Word et macro malveillante
  - Prise de possession d'un ordinateur via un cheval de Troie

- Recherche de mot de passe via Brute Force
- Faire sauter le mot de passe administrateur (<20s)
- Prise en main d'une session Windows (sans le mot de passe)
- Attaque typosquatting et homograph
- USB Capture
- Un petit tour sur le Darknet !!! (sur demande + Internet)
- Attaque Social Engineering via Facebook (sur demande + Internet)
- Configuration et utilisation d'un ransomware (sur demande)

Cette session de sensibilisation à la sécurité informatique aborde le sujet sous deux aspects : technique et organisationnel.

Le volet technique reste au niveau de la présentation des risques et des menaces pour l'entreprise au quotidien et le volet organisationnel s'attache à donner aux participants des bons réflexes et des bonnes pratiques en parallèle des éléments techniques présentés. Il s'agit donc d'impliquer les participants dans la sécurité du système d'information en étant acteur et non simple spectateur.

Concrètement pour les participants il s'agira de :

- Etre sensibilisés de manière interactive et créative aux menaces informatiques auxquelles ils peuvent être directement confrontés dans leur activité professionnelle et privée

- Comprendre les problématiques liées à la sécurité informatique

- Comprendre pourquoi la prévention est nécessaire

- Prendre conscience du rôle qu'ils ont à jouer

- Adopter les bonnes attitudes et réflexes

Les bases théoriques ne seront dispensées que dans la mesure où elles permettent de toucher du doigt, concrètement, un concept important, un risque, ou tout simplement une meilleure compréhension des procédures générales préconisées dans une entreprise (charte). Il s'agit de montrer par des exemples ou des anecdotes vivantes (virus propagé de différentes manières, attaques diverses, écran de veille et mot de passe, mauvaise stratégie de mot de passe, etc.) la légitimité des précautions à prendre en matière de sécurité, tout en disposant des bases techniques pour comprendre les points d'entrée des failles potentielles de sécurité. Les exemples sont

suffisamment concrets et réalistes pour d'une part capter l'attention de l'auditoire mais aussi et surtout bien faire passer le message « ça n'arrive pas qu'aux autres ».

Enfin, pour se situer dans une approche dynamique et non passive, pour chaque exemple la conclusion sera « qu'aurait fallu-t-il faire pour l'éviter ? ».