ISEIG
Institut Suisse d'Enseignement de l'Informatique de Gestion

Cybercriminalité, les bons réflexes
Cyberattaque = Intervention humaine

Vous et vos collaborateurs connaissez-vous leur environnement de travail et les règles à respecter ? Sensibilisez-les aux bonnes pratiques à adopter au sein de l'entreprise et à la maison.

Exemple 1 - Rançongiciel

Pour une entreprise, quelles sont les conséquences d'une attaque de type rançongiciels (logiciels de rançonnage ou ransomwares), un virus qui encrypte et prend les données en otage ?

Si les sauvegardes sont exécutées régulièrement, on peut supposer que :

- les données créées depuis la dernière sauvegarde sont perdues,
- le système doit être arrêté pour désinfection le jour de l'attaque,
- la dernière sauvegarde est restaurée,
- les données entre l'attaque et la restauration de la dernière sauvegarde doivent être recréées.

Résultat : 3 jours ouvrables sont perdus. Dans le cas d'une entreprise de 200 personnes, cela représente 3 jours multipliés par 200 personnes, soit 600 jours/personne, l'équivalent de 3 salaires annuels moyens.

Exemple 2 - Usurpation d'identité

Selon la police cantonale de Genève, 120 cas d'usurpation d'identité électronique ont été recensés en 2015, dont 12 ont abouti à des vols importants s'élevant à plus de 8 millions de francs. La police donne l'exemple d'une seule société qui a versé plusieurs millions sur des comptes en Europe et en Extrême-Orient. Toutes les entreprises, très diverses de par leur taille ou leur activité, peuvent être la cible de ces escrocs internationaux.

Exemple 3 - Fraude aux paiements

Une fraude aux versements de loyers se répand en Suisse depuis fin 2014. De quoi s'agit-il? Faire payer deux fois les loyers grâce à une astuce incroyable ! Une grande entreprise romande en a fait les frais et a déposé plainte.

La subtilité de cette fraude ? Via un courriel, courrier ou téléphone, les escrocs se font passer pour des avocats, huissiers et autres responsables de la régie. Ils expliquent dans des lettres à l'en-tête piraté, que la régie a changé de banque et que dorénavant, les loyers doivent être versés sur un nouveau compte. Le locataire n'y voit que du feu et paie ainsi son loyer aux escrocs. Lorsqu'arrive le rappel officiel de la véritable régie pour un loyer impayé, le locataire n'y comprend plus rien ! Sauf qu'il devra bel et bien s'acquitter à nouveau de son loyer. Du moins s'il ne veut pas perdre son logement …

Présentation

Le développement d'Internet et des technologies de l'information conduit les utilisateurs à la facilité, en faisant trop confiance à ces outils. Ainsi les escrocs profitent de la naïveté des utilisateurs pour s'introduire dans les systèmes d'information et encrypter des données pour se faire transmettre des sommes d'argent.

Une vulnérabilité est le déclencheur de toutes attaques qui se réalisent. Aujourd'hui, les outils techniques, bloquant les accès et surveillant la propagation de virus ou autres, sont connus et assez bien maîtrisés par les services informatiques.

Par contre, on oublie souvent les comportements humains qui eux sont plus difficilement contrôlables et qui peuvent engendrer des risques importants.

Lors de l'engagement de collaborateurs, il leur est demandé de savoir utiliser ou d'être formés sur des applications informatiques métiers, mais rarement de connaître les principes de base de l'utilisation d'un système d'information et de l'environnement dans lequel ils vont travailler.

Les collaborateurs connaissent bien leur métier et les outils mis à leur disposition. Par contre, les règles de base pour gérer et sauvegarder leurs données sont méconnues. Il en va de même pour l'utilité et la

Suite au verso

composition d'un mot de passe sécurisé, pour la gestion et le contrôle de leurs courriers électroniques et pour plus encore. Tous ces éléments sont dus au manque d'implication ou de connaissance des dirigeants qui négligent la formation et sensibilisation aux bases de la sécurité informatique de leurs équipes.

Cette formation de sensibilisation d'une demi-journée présente les bonnes pratiques et les règles en vigueur pour éviter les désagréments ainsi que les coûts dus à une attaque, une escroquerie ou la perte de données.

La formation, qui **peut être personnalisée et dispensée en entreprise**, démontre que les mesures de sécurité ne doivent plus être une contrainte mais une habitude.

Pour qui :

- toute personne qui utilise le système d'information de son entreprise
- responsable de sécurité souhaitant mettre en place un système de sensibilisation à la sécurité informatique dans son entreprise

Objectifs :

- connaître les règles de base à respecter pour réduire les risques de sécurité dus au comportement humain

Prérequis :

- ---

Programme :

Les thèmes suivants sont développés en plaçant le collaborateur au cœur de la démarche :

- le système d'information et le poste de travail
- la gestion des données
- les mots de passe
- boîte aux lettres électroniques (e-mail)
- Internet
- appareils mobiles
- arnaques et escroqueries
- réseaux sociaux
- famille et enfants

Durée, prix :

Formation	Jour	Prix	Prix/j
Cyber-arnaque, peut-on s'en protéger ?	0.5	220.- *	na

selon conditions générales. Le prix comprend toute la documentation distribuée. Les cours se déroulent de 13:30 à 17:00

* Remise de 5 % aux membres ADI, GRI, aux diplômé(e)s ISEIG CP, titulaires du BFI, DFI ou certifié(e)s MCSA, MCSE, MCSD formé(e)s à l'ISEIG