TOSA

La sécurité au travail

2.1 La sécurité du poste de travail

2.2 L'ingénierie sociale

2.1 La sécurité du poste de travail

A. Sécurisation matérielle

Les atteintes à la sécurité physique du poste de travail peuvent provenir d'événements naturels comme la foudre ou encore une inondation mais aussi d'incidents tels qu'une surcharge de tension du circuit électrique ou encore, un incendie.

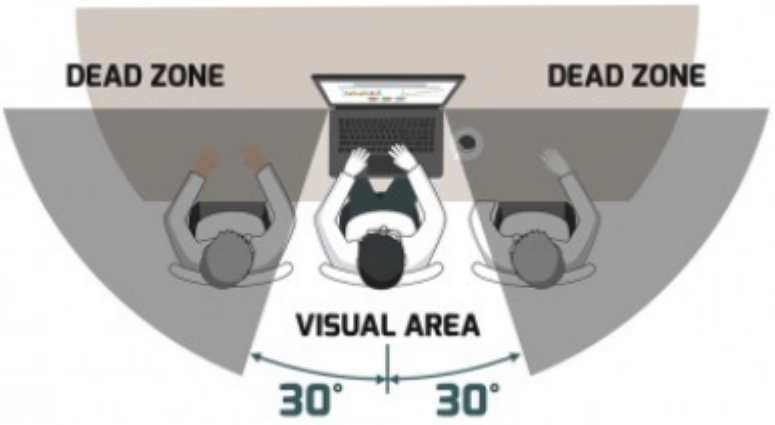
Aucun système informatique n'est à l'abri d'une panne de sorte que l'ensemble des dispositions visant à protéger le poste de travail des menaces d'une telle nature seront préventives et exclusivement du ressort de l'entreprise.

Ces mesures peuvent être de différents ordres. Par exemple, l'installation de détecteurs de fumée, l'utilisateur de dispositifs de protection électrique comme les onduleurs qui en cas de coupure prennent le relais de l'alimentation électrique grâce à leur batterie intégrée ou encore, une disposition spatiale des infrastructures de bureau qui permette de limiter les conséquences d'une inondation (matériel informatique situé dans une pièce en hauteur par exemple).

Des actions malveillantes, voire criminelles, peuvent également mettre en péril la sécurité du poste de travail tel le vol ou la destruction de matériel. À ce niveau d'intervention, l'entreprise devra s'assurer de la protection du cadre de travail en termes d'accès physique et interdire ce dernier à toute personne étrangère et/ou ne disposant pas des droits d'accès au service mais il sera également du ressort de l'employé, à veiller à la sécurisation de son poste de travail en restant vigilant, en mettant hors d'accès tout terminal professionnel et en signalant tout comportement suspect.

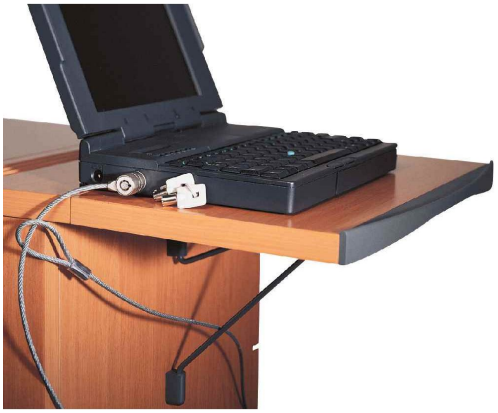
Enfin, il existe toute une série d'accessoires visant la protection physique du poste de travail et des données. En effet, dans le cas où il n'est pas possible de tenir hors de vue des données inhérentes au poste de travail qui s'afficheront sur un écran d'ordinateur par exemple, il est possible de mettre en place des filtres de confidentialité et des protecteurs d'écran qui empêchent la lecture de celles-ci.

Le filtre de confidentialité consiste en un film sombre doté d'un système de fixation qui réduit le champ de vision d'un écran à l'instar de la figure ci-après.



En termes de support mobile de données, notamment ceux qui permettent le transfert et le stockage d'informations, l'utilisation de clefs USB non cryptées lorsqu'il s'agit de contenir des données jugées sensibles sera à limiter voire proscrire puisque les risques de pertes ou de vol sont accrus. Enfin, il paraît évident que l'emploi d'un smartphone ou d'une tablette utilisé dans le cadre professionnel ne devrait pas faire l'objet d'un usage personnel.

En conclusion, il existe également, pour empêcher les vols, des câbles spécifiques munis de part et d'autre d'un verrou ou d'un cadenas doté d'un mécanisme de verrouillage numérique permettant que le matériel soit fixé en un endroit. En effet, au vu de l'expansion du travail en espace partagé (open space), cet outil s'avère particulièrement nécessaire lorsque le cadre de travail accueille différents secteurs d'activité, que des données sensibles sont manipulées dans le cadre de l'activité professionnelle et que du public soit susceptible d'être accueilli par certaines entreprises.



Pour finir, dans le cadre de la certification TOSA, le candidat devra surtout comprendre les différentes situations à risques susceptibles, à son niveau d'implication, de causer un préjudice à son entreprise par défaut de précaution. Ces situations sont, par exemple, celles qui placent les terminaux professionnels dans un contexte propice à la perte, le vol ou la détérioration de données à la suite d'une intervention physique. Des gestes simples basés soit sur des dispositifs fournis par l'entreprise comme le filtre de confidentialité ou le verrouillage mécanique de son pc en cas d'absence, soit encore sur des actions de prévention que le candidat devra être en mesure d'envisager pour éviter toute atteinte à la sécurité physique de son poste de travail.

B. Sécurisation logicielle

A. L'erreur humaine : principale source des cyber incidents

Selon l'indice relatif à la veille stratégique en matière de sécurité d'IBM, l'erreur humaine est impliquée dans plus de 90 % des incidents de sécurité (clic sur un lien de phishing, consultation d'un site Web suspect, activation de virus ou autres menaces persistantes avancées).

B. Sensibilisation efficace à la sécurité informatique

La formation du personnel est essentielle pour générer une prise de conscience des salariés et pour les motiver à être plus attentifs aux cybermenaces et aux contre mesures, même s'ils estiment que cela ne fait pas partie des responsabilités liées à leur poste.

C. Comment sécuriser votre poste de travail:

- Installer systématiquement, de préférence automatiquement, les mises à jour du système d'exploitation
- Utiliser le pare-feu (firewall)
- Installer l'antivirus institutionnel TRAPS
- Installer un anti-espions (s'il existe pour votre système)
- Chiffrer l'intégralité du contenu de votre ordinateur (si cela est possible sur votre système)

D. Ce qu'il ne faut pas faire

- Utiliser des systèmes d'exploitation obsolètes
- Donner des droits administrateurs aux utilisateurs n'ayant pas de compétences en sécurité informatique.

E. Les dangers potentiels

- Les virus
- Les chevaux de troie
- Les espiogiciels (spyware)
- Le spam
- Les canulars

F. Les modes de contamination

- Les supports amovibles ou tout support qui a besoin d'être connecté ou introduit dans un ordinateur est un danger potentiel.
- Le réseau informatique où la plus grande partie des infections est réalisée aujourd'hui par les réseaux.

G. Les dommages

- Destruction de fichiers
- Corruption de fichiers
- Destruction matérielle
- Instabilité du système
- Dégradation des ressources du système

H. Pour aller plus loin:

- Interdire l'exécution d'applications téléchargées ne provenant pas de sources sûres.
- En cas de compromission d'un poste, rechercher la source ainsi que toute trace d'intrusion dans le système d'information de l'organisme
- Effectuer une veille de sécurité sur les logiciels et matériels utilisés dans le système d'information de l'organisme.
- Mettre à jour les applications lorsque des failles critiques ont été identifiées et corrigées
- Installer les mises à jour critiques des systèmes d'exploitation sans délai en programmant une vérification automatique hebdomadaire.
- Diffuser à tous les utilisateurs la conduite à tenir et la liste des personnes à contacter en cas d'incident de sécurité ou de survenance d'un événement inhabituel touchant aux systèmes d'information et de communication de l'organisme.

2.2 L'ingénierie sociale

A. Définitions et étapes

C'est un type d'attaque psychologique qui exploite le comportement humain et ses biais cognitifs (c'est-à-dire ses failles de raisonnement). Elle consiste généralement à manipuler la victime afin de la pousser à révéler des données sensibles pouvant être utilisées à des fins de piratage. Elle peut également consister à pousser la victime à réaliser des actions nuisibles à l'entreprise en toute bonne foi.

Cette méthode comporte quatre étapes.

Recherche

La première étape consiste à récolter des informations. Le but est de rassembler des informations sur la victime au moyen par exemple de l'OSINT. Le hackeur devra en outre être en mesure de répondre correctement à toutes les questions de la victime si elle doit se faire passer pour une source légitime. Pour cela, il se renseignera également sur l'entreprise ou sur certains corps de métier.

Prétexte

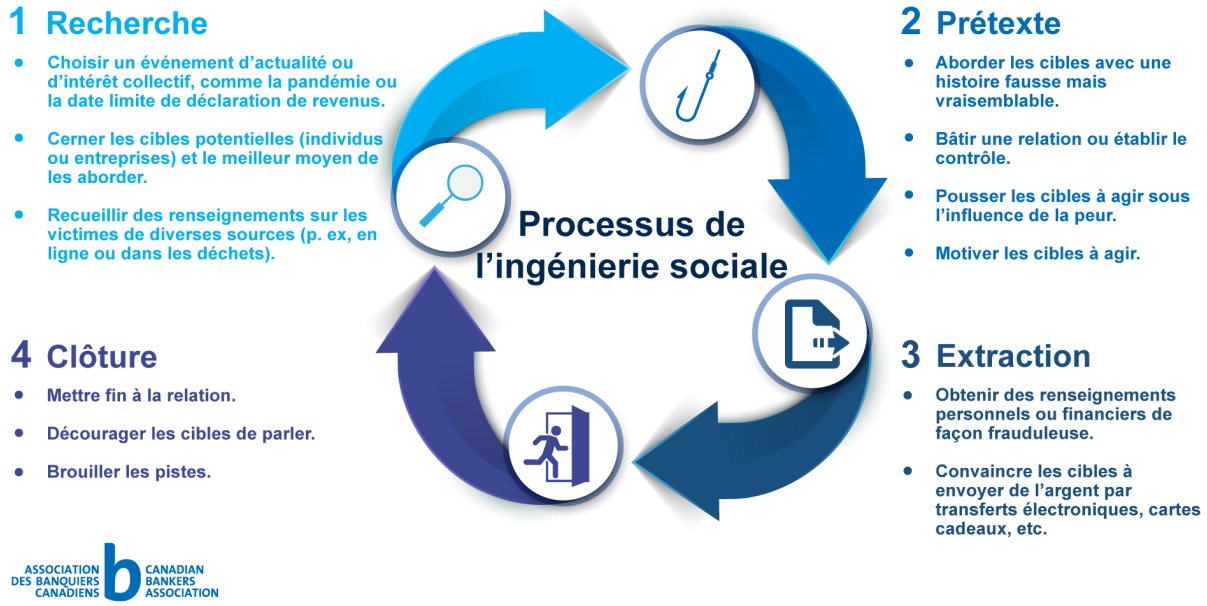
La seconde étape est le prétexte. C'est à cette étape qu'il choisit son angle d'attaque. Après avoir récolté assez d'information il est temps pour l'attaquant de faire un scénario fiable vis-à-vis de la victime. Le but est d'installer une relation de confiance avec la future victime

Extraction

Une fois ce lien établi et le pirate **perçu comme étant fiable**, il peut exploiter sa cible. La troisième étape va donc être d'utiliser le prétexte mis en place pour mener la victime à exécuter certaines actions ou à divulguer des informations confidentielles sur l'entreprise.

Clôture

Lors de la dernière étape, le pirate **brise le lien et disparaît**. Il s'attellera à ne laisser aucune information qui pourrait remonter à sa réelle identité. Il menacera peut-être également la victime pour la dissuader de parler.



B. Techniques les plus courantes

1. **Hameçonnage** : courriels, sites web ou textos trompeurs pour voler de l'information.

2. **Harponnage** (fraude du PDG) : courriels ciblés visant des personnes ou des entreprises.

3. **Appâtage** : attaque qui promet à la victime une récompense ou un cadeau.

4. **Maliciel** : attaque qui fait croire qu'un maliciel a été installé sur l'ordinateur de la victime en lui offrant de payer pour le faire supprimer.

5. **Faux-semblant** : fausse identité pour tromper les victimes et soutirer de l'information.

6. **Quid pro quo** : attaque utilisant un échange d'information ou de service pour convaincre la victime d'agir.

7. Talonnage : s'appuie sur la confiance humaine pour donner au criminel l'accès physique à un édifice ou une zone sécurisée.

8. Hameçonnage vocal : message ou appel téléphonique qui semble urgent pour convaincre les victimes d'agir prestement pour éviter une arrestation ou d'autres risques.

9. Attaque par point d'eau : attaque d'ingénierie sociale sophistiquée qui infecte, par un logiciel malveillant, à la fois un site web et les internautes qui le visitent.

C. Exemples

- L'attaquant se renseigne sur une entreprise, il s'informe sur le fonctionnement de l'entreprise, sa hiérarchie, les modèles utilisés pour les adresses e-mails ainsi que sur les projets en cours et quelques logiciels qui sont utilisés dans l'entreprise. Ensuite, il va s'informer sur un collaborateur en particulier de l'entreprise. Il s'informe sur le déroulement d'une journée classique pour lui et il peut également chercher ses hobbys via les réseaux sociaux.

Une fois les informations récoltées, l'attaquant prépare un scénario.
L'attaquant se fait passer pour un employé du département informatique. Il prépare un email avec le même modèle qu'utilise l'entreprise cible. Il demande à la victime si elle peut télécharger et installer un correctif d'un logiciel utilisé quotidiennement car il n'a pas réussi à le déployer à distance. L'attaquant demande en quelque sorte une faveur, qui dans des circonstances normales pourrait être totalement plausible.
Malheureusement, si le collaborateur télécharge et installe le logiciel, il se retrouve piégé et il sera fautif d'avoir fait entrer le ransomware dans l'entreprise. Tout cela est possible car le collaborateur a été naïf et a voulu être serviable. Pour lui, il venait simplement en aide à un collègue.

L'appât du gain

Les pirates profitent du fait que nous connaissons bien certaines offres légitimes et proposent par exemple 100 euros pour remplir un sondage qui demande (comme par hasard) de créer un compte (vous devez donc introduire un identifiant et un mot de passe). Dans cet exemple, les pirates espèrent que vous allez réutiliser les mêmes informations d'identification que celles que vous utilisez ailleurs et qu'ils pourront ainsi s'en servir pour accéder à vos comptes bancaires ou à d'autres comptes.

❖ La peur

Un message vocal vous dit que vous êtes sous enquête pour fraude fiscale et que vous devez appeler immédiatement pour éviter une arrestation et une enquête criminelle. Cette attaque d'ingénierie sociale survient en période de déclaration d'impôts, où les gens sont déjà stressés au sujet de leurs impôts. Les cybercriminels misent sur le stress et l'anxiété générés par la déclaration de revenus et utilisent ces sentiments de crainte pour inciter les gens à suivre les directives du message vocal.

❖ La curiosité

Les cybercriminels surveillent les événements très médiatisés pour profiter de la curiosité humaine en tendant des pièges d'ingénierie sociale incitant à l'action. Après le deuxième écrasement d'un Boeing MAX8, les cyberfraudeurs ont envoyé des courriels avec des fichiers joints contenant prétendument des fuites d'information au sujet de l'écrasement. En fait, le fichier joint installait une version du virus Hworm RAT dans l'ordinateur des victimes.

❖ La bienveillance

Les humains sont enclins à se faire confiance et à s'aider mutuellement. Après une recherche sur une entreprise, les cybercriminels ciblent deux ou trois employés avec un courriel semblant provenir de leur gestionnaire. Le courriel leur demande d'envoyer à leur gestionnaire le mot de passe de la base de données comptable, prétextant que le gestionnaire en a besoin pour que la paie soit faite à temps. Le ton du courriel est urgent et sous-entend qu'ils aideront leur gestionnaire en agissant rapidement.

❖ L'urgence

Vous recevez un courriel du service à la clientèle du site web de magasinage où vous achetez fréquemment. Vous devez confirmer l'information de votre carte de crédit pour protéger votre compte. Le langage utilisé dans le courriel vous presse de répondre sans délai pour éviter que l'information de votre carte de crédit soit volée par des criminels. Sans y penser deux fois, et parce que vous avez confiance en ce commerce en ligne, vous envoyez non seulement l'information de votre carte de crédit, mais également votre adresse courriel et numéro de téléphone. Quelques jours plus tard, votre compagnie de carte de crédit vous appelle pour vous dire que votre carte a été volée et qu'elle a servi pour des achats frauduleux de plusieurs milliers d'euros.

D. Comment s'en prémunir?

Nous le savons tous, la plus grande faille en informatique reste l'humain derrière la machine. L'ingénierie sociale s'appuie sur ce principe. Par conséquent, il sera essentiel de faire comprendre aux membres du personnel qu'ils sont la principale cible de ces attaques.

Leur expliquer des cas concrets ou prévoir un test de mise en situation réelle pourrait par exemple leur faire prendre conscience de leur propre vulnérabilité.

C’est seulement en tombant dans un piège d’hameçonnage ou d’une autre approche d’ingénierie sociale que les gens comprennent comment elle fonctionne. Avec une formation en sensibilisation à la sécurité centrée sur les personnes qui utilise les simulations d’hameçonnage, offrant un contenu engageant et pertinent qui tient compte de la nature humaine, vous pouvez demeurer protégé de l’ingénierie sociale.

E. Comment réagir face à une attaque?

Si toutefois cela ne suffisait pas et qu’un cyberincident avait lieu. Le membre du personnel qui détecte ou identifie une menace, doit être capable d’effectuer un signalement. L'idéal étant d'avoir une personne de contact prévue à cet effet.

Cela sera utile le jour où on découvre un logiciel suspect sur un ou plusieurs appareils, un site web altéré sans sans rendre de compte, des données modifiées ou qui semblent avoir disparues ou voir des machines ne fonctionnent plus normalement, machines bloquées, etc.

Étapes suivant la détection d’un incident

Premièrement, éviter que l'incident se propage (confiner). Il faut déconnecter du réseau toutes les machines et les disques durs externes mais ne pas les éteindre car on risquerait de perdre des données essentielles pour enquêter.

Une fois que l'on sait tout ça, on va se demander comment se prémunir de ses menaces ou ce qu'on appelle aussi cyberincident.

On va chercher à les détecter et ça, ça commence avec le personnel de l'organisation qui est souvent considéré comme le maillon faible mais c'est pourtant lui qui offre le meilleur potentiel en matière de cybersécurité.

Avec l’OSINT, il faut faire prendre conscience à l'individu qu'il est une potentielle porte d'entrée pour un attaquant. Leur expliquer avec des cas concrets, voir un test de mise en situation réelle pourrait par exemple leur faire prendre conscience de leur propre vulnérabilité.

C'est pour ça que des organisations utilisent l'OSINT aussi pour trouver des failles.

Pour se mettre à la place de l’usager, au moindre doute, que ce soit pour un mail, une demande d’information ou même le fait de douter de la véritable identité d’un interlocuteur, il faut agir immédiatement :

- Faire valider la demande d’information : en discuter avec les collègues ou ses supérieurs. La procédure est bien suivie….

- Demander à la personne de vous contacter par d’autres moyens et différents canaux pour vérifier l’identité de la personne.

- Jouer avec les détails: poser des questions pour repérer les incohérences, leur demander des choses qu’ils doivent connaître ou encore donner de fausse information pour jauger leurs réactions.

- Travailler en collaboration avec le département IT : même si on ne peut rien faire contre l'arnaqueur, c’est après au service IT de mettre en place les mesures nécessaires et notamment en informer tous les collaborateurs de ces menaces et nouvelles menaces.

- Le dernier point qui peut paraître un peu forcé, mais quand on est dans une zone avec un accès restreint, c’est de demander par exemple un badge de visiteurs à la personne voir carrément appeler la sécurité.

Série de recommandations :

- Détruire les documents et équipements IT qui ne sont plus utiles
- Verrouiller l’accès à vos données sensibles et protéger par mots de passes
- Être sûr de l’identité de la personne avec qui on échange
- Ne pas se laisser charmer ou intimider
- Restreindre l’accès aux matériels, équipements et les bâtiments
- Être à jour au niveau des protocols de sécurité de son organisation
- Le dernier qui paraît évident, mais ça reste compliqué selon la situation, c’est de ne pas croire une personne sur parole

Sources:

- https://www.youtube.com/playlist?list=PLn1l55Gza9px_uDleaG5xBqI81yYQ24MZ
- https://ccb.belgium.be/sites/default/files/cybersecurity-incident-management-guide-FR.pdf
- https://www.restena.lu/files/inline-images/FICHE_SocialEngineering_EN_2021.pdf
- https://www.legroupenova.com/blog/securite-postes-travail/
- https://www.reseaucerta.org/sites/default/files/comm_securite.pdf
- https://www.ponemon.org/news-updates/news-press-releases.html
- https://www.inforisque.info/actualite-du-risque/documents/7632-ebook-olfeo-facteur-humain-prochain-maillon-fort-cybersecurite.pdf
- https://terranovasecurity.com/fr/9-exemples-ingenierie-sociale/
- https://www.itweapons.com/fr/social-engineering-attacks-blog-2/
- https://www.oppens.fr/quest-ce-que-lingenierie-sociale-et-comment-sen-premunir/
- https://digitalsecurityguide.eset.com/fr/ingenierie-sociale-pieges
- https://cutt.ly/3Za6y48
- https://cutt.ly/SZa6asS
- https://cutt.ly/GZa60sj
- https://cutt.ly/oZswFde
- https://cutt.ly/MZsrrYs
- https://cutt.ly/tZaHxBi
- liste systèmes et logiciels obsolètes: https://www.cert.ssi.gouv.fr/information/CERTFR-2005-INF-003/