Mission 10 - 11:

Compte - Rendu : Cyber-sécurité

Table des matières :

Module n°1 :

Unité 1 :

Un système d'information est un mot générique désignant tout ce qui sert à faire transiter et à traiter de l'information. Internet est comparable à une sorte d'autoroute mondiale dédiée au transport des informations qui permet de relier un très grand nombre de personnes, d'entreprises du monde entier. Cependant, cela nécessite d'avoir accès à un Internet via un ordinateur entre autres, ce qui n'est pas le cas partout dans le monde en particulier dans les pays défavorisés.

Aucun équipement n’est protégé des cyberattaques à partir du moment où il est connecté (par exemple, cyberattaque sur une Tesla lors de l'événement des Blacks Hats aux États-Unis en 2023).
Ainsi, le Cloud, bien que très utile puisqu’il permet de partager facilement des données entre plusieurs ordinateurs, n’est pas épargné et stocké des données sensibles dessus peut représenter un danger, notamment en cas de fuite de données.

Les auteurs des cyberattaques sont très difficiles à identifier puisqu’il peut s’agir d’une personne ou un groupe de personnes, une entreprise ou un gouvernement. De plus, l’auteur d’une attaque peut virtuellement usurper l’identité d’un tiers rendant son identification d’autant plus compliqué.
Les cibles de ces attaques sont souvent des points névralgiques de la nation, comme un centre de traitement de l’eau ou encore un hôpital, afin de causer le plus de dommages possible.

Le Cyber-espace est un endroit sans frontières géographiques, néanmoins les serveurs sont construits dans certains pays et les lois de celui-ci peuvent influer sur le contenu hébergé. Il y a donc une notion de territorialité.
On peut noter par exemple que les données personnelles sont plus protégées par la loi lorsqu’elles sont hébergées en France qu’aux États-Unis. En effet, en France de nombreuses règles sont mises en place afin de contrôler et réguler l’utilisation des données.

Unité 2 :

Il existe deux types de cyber-attaques : Les attaques ciblées où un attaquant utilise l’ensemble des informations de l’entreprise visée trouvées pour en faire une cartographie précise, et les attaques de masse où l’attaquant parcourent et scannent Internet pour trouver des objets non sécurisés pour en prendre le contrôle facilement et les utiliser dans des attaques.

Les objectifs des pirates lors de ces attaques sont la déstabilisation, la revendication politique ou idéologique, la vengeance (en cas de licenciement d’un employé par exemple), la revente de données, l’espionnage et le défi technique.

Plusieurs méthodes sont disponibles par les attaquants en fonction du résultat attendu. Parmis celles-ci il existe la méthode du Botnet qui consiste à se créer un réseau de machines zombies contrôlées par un attaquant, un Adware/Publiciel qui consiste à envahir l’ordinateur de la victime de publicitées plus ou moins ciblées ou encore le Cheval de Troie qui consiste à cacher un programme malveillant dans un logiciel légitime pour permettre à un attaquant de prendre le contrôle d’un ordinateur en particulier.

Les cyber-attaques peuvent avoir plusieurs conséquences de la perte de disponibilité à la perte financière en passant par un impact sur l'image de l'entreprise.

Afin de s'en protéger, il est conseillé d'utiliser des mots de passes sécurisés, de garder votre système à jour, de ne pas diffuser d'informations confidentielles sur Internet qui pourraient être utilisées lors d'une attaque, de ne pas exécuter d'instructions venant d'un inconnu et de détruire les messages non-sollicités sans y répondre.
Il est également important de sauvegarder régulièrement ses données, de vérifier les expéditeurs d'emails, de ne pas ouvrir de pièces jointes au moindre doute et dans le cadre d'une entreprise, de demander conseil à l'équipe sécurité ou à défaut aux administrateurs du SI (Système d'Information).

Unité 3 :

Les OIV (Opérateurs d'Importance Vitale) sont des acteurs privés indispensables au bon fonctionnement de la Nation (exemple : barrages, circulation routière, station de traitement de l'eau). Dans le cadre d'un salarié d'un établissement considéré comme OIV, celui-ci est soumis à davantage de contraintes de sécurité puisque si une cyber-attaque survient, les impacts sont plus importants.

L'acronyme OCLCTIC désigne l'Office Central de Lutte contre la Criminalité lié aux Technologies de l'Information et de la Communication. Il appartient à la Direction Centrale de la Police Judiciaire (DCPJ)

L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) à plusieurs missions comme qualifier des services et des produits, informer le public sur les bonnes pratiques, détecter les attaques potentielles et anticiper les menaces à venir. Le Livre Blanc pour la Défence et la Sécurité Nationale à été rédigé pour structurer une vision commune ed la défense, et plus particulièrement de la cyber-sécurité en France. Celui-ci à été commandité par le président de la république en 2013.

Des acteurs locaux tels que la Brigade d'Enquête sur les Fraudes aux Technologies de l'Information (BEFTI) agissent pour protéger les citoyens des infractions sur Internet.

La gendarmerie nationale dans le domaine de la sécurité informatique occupe une place importante sur l'ensemble du territoire, ses actions se déclinent sur trois axes : l'anticipation, la prévention et la répression.

La CNIL (Commission Nationale Informatique et Libertés) n'opère pas principalement dans la cyber-sécurité, cependant celle-ci possède une action très liée à la thématique de la sécurité des systèmes d'information.

Unité 4 :

Dans le cadre d'une entreprise, il est interdit d'installer quoique ce soit sur son téléphone professionnel sans avoir l'accord au préalable de son service informatique puisque ceux-ci peuvent contenir des virus qui seraient susceptibles d'infecter tout le réseau de l'entreprise.
D'autre part, les protections mises en place par l'entreprise ne suffisent généralement pas à assurer une sécurité totale, il est important de rester vigilant et de faire preuve de bon sens au quotidien (exemple : ne pas utiliser les Wi-Fi publics facilement espionnables par des attaquants potentiels).

La défense en profondeur est un terme emprunté à une technique militaire destinée à retarder l'ennemi. Dans le cadre de la cyber-sécurité, elle consiste à exploiter plusieurs mesures de sécurité partiellement ou complètement redondantes afin de retarder l'avancée d'un attaquant.

Pour des raisons de sécurité évidentes et de bon sens, il est nécessaire d'effectuer toutes les mises à jour, d'utiliser des mots de passe variés et robustes, et de ne surtout pas laisser un moyen à un attaquant de trouver facilement votre mot de passe aussi bien virtuellement que physiquement.

Avant d'effectuer un paiement en ligne, il est nécessaire de procéder à quelques vérifications sur le site concerné afin de limiter le risque d'attaques. Les vérifications à suivre sont :

- La mention "https://" au début de l'adresse du site internet
- La légitimité du site internet en prenant garde aux fautes d'orthographes
- Le nom du site dans la barre d'adresse afin de s'assurer de ne pas être sur un site de phishing
- La présence d'un cadenas vert dans la barre d'adresse de votre navigateur

Unité 5 :

Le patrimoine informationnel d'une entreprise est la richesse de celle-ci au quotidien et son capital de développement futur. (Catalogue, codes sources des logiciels développés par l'entreprise, portefeuilles des clients…)
En tant que salarié d'une entreprise, il est de votre devoir de protéger son patrimoine informationnel, sa réputation et son image. Ainsi, il est de votre devoir d'éviter tout vol d'informations.

Pour cela, il est conseillé d'être discret lors de vos déplacements, de verrouiller votre session lors de votre pause et à la fin de votre journée de travail, d'accompagner les visiteurs dans leurs déplacements et de maintenir votre matériel à jour.

Une donnée est une information qui peut se présenter sous différentes formes, aussi bien physiques que virtuelles. Celle-ci est caractérisée par l'acronyme DIC (Disponibilité, Intégrité, Confidentialité)
La perte d'intégrité d'une donnée consiste à la modification non-autorisée de celle-ci qui à pour conséquence d'avoir des données erronées au sein de l'entreprise.
La perte de disponibilité d'une donnée consiste à l'incapacité d'avoir accès à l'information voulue, notamment lors d'une attaque DDoS.
Celles-ci sont souvent classées sous différents niveaux de classifications. Ainsi, ces niveaux de classifications des données permettent de déterminer leurs conditions de stockage, d'échange et de destruction.
Afin de stocker de manière sécurisé les données il faut créer des dossiers avec des droits d'accès limités aux personnes autorisées uniquement, et de chiffrer son disque dur.

Module n°2 :

Unité 1 :

La méthode qui permet de prouver son identité afin de se connecter à un service sont les facteurs d'authentification. On les regroupe en trois catégorie :

- Facteurs Biométriques, c'est-à-dire qui on est (Empreinte Digitale)
- Facteurs de possession, c'est-à-dire ce que l'on possède (Badge/Clé)
- Facteur de connaissance, c'est-à-dire ce que l'on sait (Mot de Passe).

La catégorie la plus couramment utilisée est la méthode du mot de passe.

L'utilisation cumulée de plusieurs de ces méthodes permet d'obtenir une authentification plus forte qu'une seule de ces méthodes, cependant elles ne garantissent pas une sécurité absolue.

Le principe d'autorisation quant à lui permet de définir ce à quoi vous avez accès.

Unité 2 :

Les cyber-attaques sont regroupées en deux types d'attaques :

- Les attaques directes : Ce sont des attaquants qui essayent d'obtenir vos identifiants/mots de passe de façon moins subtile (BruteForce, attaque par permutation..)
- Les attaques indirectes : Ce sont des attaquent qui utilisent la ruse pour obtenir vos identifiants/mots de passe (attaque de proximité)

Afin de renforcer l'authentification par mot de passe, il est possible d'y ajouter une méthode complémentaire telle que l'envoie d'un SMS, une question secrète "Quel était le nom de votre mère ?". Cependant il est simple pour un attaquant de se renseigner sur l'identité de sa cible avant d'effectuer son attaque et donc avoir la réponse à cette question. Voilà pourquoi la méthode la plus sûre est l'envoi d'un SMS sur le téléphone portable de l'utilisateur.

Unité 3 :

Comme vu précédemment, il est important de créer un mot de passe suffisamment sécurisé sur chacune des plateformes. Pour cela, quatre facteurs entrent alors en jeu :

- La *longueur*, c'est à dire le nombre de caractère saisis (≠ ako)

- Le ***dictionnaire***, c'est à dire le nombre de caractères différents saisis (alphabétiques, alphanumériques, caractères spéciaux) (≠ aezioka)
- Le ***hasard***, c'est à dire une suite de caractères qui n'ont aucun point commun et qui ensemble ne forment aucun mot. (≠ Ma_Chienne_S'appelle_Tova)
- ***L'unicité***, c'est à dire de saisir un mot de passe différent sur chaque plateforme afin de se protéger en cas de fuite de données. (≠ mdp1, mdp2…)

Il est également possible d'utiliser un système de gestionnaire de mot de passe (coffre-fort) pour que celui-ci puisse générer des mots de passe plus aléatoire et plus robuste que ce qu'aurait pu imaginer un utilisateur classique, et pour que le coffre-fort puisse mémoriser tous les mots de passe afin d'éviter à l'utilisateur de tous les retenir.

A défaut, il est conseillé de générer des mots de passe complexes mais néanmoins faciles à retenir comme "7éT_Gu:2Kd0" grâce à diverses méthodes mémo-techniques (méthode phonétique dans ce cas, "cet été j'ai eu deux cadeaux"). Ce mot de passe est plus robuste que la phrase réelle puisqu'il comporte des lettres minuscules et majuscules, des chiffres, des caractères spéciaux, ne forme pas une phrase en l'état et à une longueur suffisante (11 caractères)

Unité 4 :

Pour se connecter à différents services, il est également possible d'utiliser un seul point d'authentification unique et centralisé, relié à tous les autres services comme Gmail par exemple. Cela peut être plus rapide pour l'utilisateur puisqu'il n'y à plus besoin de créer / mémoriser différents mots de passe ni de les saisir manuellement. Cependant, cela est dangereux car si un attaquant accède à avoir possession de ce point d'authentification centralisé (Gmail dans notre exemple) il peut accéder à tous les services qui y sont rattachés sans besoin d'obtenir le mot de passe.
De plus, le service mère (ici Gmail) peut avoir accès à toute votre activité sur les différents services qui y sont reliés.

Dans un cadre local, il est également dangereux d'utiliser au quotidien une session administrateur. Dans le cas ou votre ordinateur est infecté par un virus depuis une session administrateur, l'attaquant accède directement aux privilèges les plus élevés et devient ainsi plus dangereux car il peut effectuer un plus grand nombre d'actions malveillantes, ce qui n'aurait pas été le cas dans une session utilisateur où tous les privilèges ne sont pas accordés.
C'est pourquoi il est fortement déconseillé d'utiliser un compte administrateur au quotidien, ou à défaut de ne pas naviguer sur internet, ne pas installer un nouveau logiciel ni d'utiliser une messagerie avec puisque ce sont des points d'entrées pour de multiples malwares.

Unité 5 :

Les informations qui transitent d'un terminal à un autre peuvent être chiffrées afin de garantir l'intégrité des données. Le message avant le chiffrement est appelé "message clair", celui après est appelé "message chiffré" et ce qui permet de déchiffrer le message est appelé la "clé". Il existe plusieurs méthodes de chiffrement comme le chiffrement par la clé de César qui consiste à décaler chaque lettre du message clair d'un certain nombre défini par la clé, afin d'obtenir le message chiffré et inversement. Par exemple, le message chiffré "WMXH NB EWZTVP" avec la clé "1423 21 251421" permet d'obtenir le message "Vive la crypto.

Le fait de chiffrer les informations est utile afin qu'un attaquant ne puisse pas réaliser une attaque par écoute, c'est-à-dire de regarder les informations qui transitent et ainsi regarder les informations échangées.

Nous comprenons donc assez rapidement que le message chiffré sans la clé de chiffrement est inutile. Ainsi, selon le principe de Kerchoffs la sécurité du chiffrement réside exclusivement sur la protection de la clé de chiffrement.
Il existe trois types de chiffrement :

- *Chiffrement symétrique* : une seule clé est utilisée de chaque côté du message pour chiffrer et déchiffrer le message. (la clé est alors appelée "bi-clé")
- *Chiffrement asymétrique* : plusieurs clés sont utilisées pour chiffrer et déchiffrer le message. (cette méthode garantit l'authenticité et la non-répudiation des données)
- *Chiffrement hybride* : c'est une méthode qui tire avantage des deux autres méthodes, le chiffrement asymétrique est utilisé pour échanger une clé secrète qui sera ensuite utilisée pour échanger à l'aide d'une opération de chiffrement symétrique

Il existe également les certificats électroniques et la signature numérique qui permettent de garantir l'authenticité d'un expéditeur afin de prouver l'intégrité de la donnée et la preuve de sa provenance

Module n°3 :

Unité 1 :

Afin d'assurer l'envoie de données entre l'émetteur et le récepteur, les données sont divisées sous forme de paquets. Le protocole utilisé pour la navigation web est le protocole HTTP ou HTTPS. Le protocole IP est utilisé pour l'acheminement des paquets et le protocole FTP est utilisé pour l'envoi de fichier. La navigation web repose sur une architecture client/server.

Il existe différents types d'attaques :

- Les *RansomWares* (Chiffrement des données de l'ordinateur ciblé puis une demande de rançon afin de déchiffrer les données)
- L'*Espionnage* (Utilisation du micro, de la caméra afin de récolter des données à caractère personnel.
- *DDoS* (Distributed Denial of Service), (Utilisation de plusieurs terminaux (ordinateurs, téléphones…), afin d'envoyer un nombre de requête inhabituel et trop important à un même server afin de le surcharger et de rendre son utilisation impossible.)

Les CyberAttaques peuvent être visées ou non, les victimes peuvent être des particuliers ou des entreprises voire des nations entières selon les motivations. Pour pouvoir correctement viser une personne en particulier, les attaquants cible l'attaque sur l'adresse IP d'un ordinateur (comparable à une adresse postale d'une maison).

Les réseaux sociaux peuvent être utilisés à plusieurs fins malveillantes. Parmi celles-ci, on peut noter la diffusion de virus, la fuite d'information, l'ingénierie sociale, l'atteinte à l'e-réputation (qui peut mener à du harcèlement) et la récupération de données et in fine l'exploitation de celles-ci, ce qui va à l'encontre des lois fixées par la CNIL.

Unité 2 :

Les logiciels malveillants utilisent souvent des failles de sécurité pour se diffuser, c'est pourquoi il faut respecter certaines pratiques afin de les limiter. Par exemple, l'installation d'un anti-virus, effectuer les dernières mises-à-jour proposées par les éditeurs de logiciels, faire attention lors du téléchargement sur internet, toujours privilégier le téléchargement de fichiers ou de logiciels depuis le site des éditeurs officiels.

Les attaquants peuvent facilement changer l'extension d'un fichier afin de dissimuler un programme malveillant exécutable aux yeux de l'utilisateur. Ainsi, les logiciels malveillants peuvent être contenus dans un fichier exécutable, dans un fichier texte, dans un document PDF et même dans une feuille de calcul Excel.

Si jamais on s'aperçoit que notre terminal est infecté par un quelconque programme malveillant, il faut débrancher le câble réseau de l'ordinateur afin de limiter sa propagation, alertez son entourage, les personnes avec qui nous avons eu des intéractions récemment et ses supérieurs dans une entreprise, et enfin porter plainte.

Il est parfois possible de récupérer les données de l'ordinateur infecté, y compris dans le cas d'un RansomWare qui chiffre les données, en récupérant la clé de chiffrement qui à été utilisée (si jamais le pirate la communique à la police par exemple).

Unité 3 :

Les sites web récoltent et utilisent parfois certaines données des utilisateurs via les cookies. Les cookies sont des outils nécessaires au bon fonctionnement de nombreux sites, cependant ils peuvent également contenir les données de navigations qui sont susceptibles d'être exploitées à des fins commerciales et publicitaires.
C'est pourquoi cette pratique est encadrée par la loi, s'applique à tous les sites web et a pour but de préserver la vie privée des internautes.

L'adresse d'un site doit correctement être orthographié afin de s'assurer d'être renvoyé sur la bonne page internet, et d'éviter un site similaire malveillant (phishing) parfaitement identique visuellement, notamment via l'utilisation du typosquatting (utilisation de la même police que le site original afin de tromper l'utilisateur). Par exemple, www.ssi.gouv.fr n'est pas le même que www.ssi.gov.fr ni même que www.ssi.gouv.com. Afin d'éviter toute confusion, certaines entreprises précisent en détail l'orthographe du site recherché à ses clients, comme CarGlass par exemple.
Il est également recommandé de privilégier les sites affichant le sigle HTTPS avant l'URL plutôt que HTTP. Le protocole HTTPS est le même que le protocole HTTP, mais celui-ci étant sécurisé (Il existe toujours un risque, mais plus faible grâce au chiffrement des données).

Lors de la navigation sur web, il existe la possibilité d'activer la navigation privée sur les navigateurs qui permet d'effacer toute trace de ses données sur le web, mais cela n'exclut en aucun cas la possibilité de se faire infecter par un virus ni par des sites malveillants. Il existe des extensions présentes sur les navigateurs afin de permettre l'ajout de certaines fonctionnalités comme la suppression de pubs

(Adblock par exemple). Cependant il existe deux familles d'extensions, celles approuvées par les navigateurs ce qui offre une certification par rapport à leur contenu, et celles qui ne le sont pas et qui peuvent ainsi contenir du code malveillant. Les pop-up présentes lors de la navigation sur le web peuvent aussi contenir des virus, c'est pourquoi il est conseillé de ne pas cliquer dessus ou à défaut d'être prudent.

Unité 4 :

L'échange de mails comporte plusieurs avantages par rapport au courrier postal :

- Les mails sont gratuits, il suffit juste de se créer un compte sur le service de messagerie de son choix (ex:Gmail) comparé au courrier qui nécessite un timbre, celui-ci étant payant.
- Les mails sont instantanés et plus faciles à diffuser, les messages envoyés sont instantanément reçu par le/les destinataire(s); et ceux-ci peuvent être nombreux comparé au courrier postal qui ne peut être adressé à qu'une seule personne à la fois
- Chaque adresse mail est unique, ce qui permet de s'assurer de l'identité du destinataire

Cependant, celui-ci peut aussi représenter plusieurs menaces aux yeux des utilisateurs.
Tout d'abord, les mails peuvent véhiculer des programmes malveillants qui s'exécutent au chargement du mail, ou un lien frauduleux afin de renvoyer la cible vers un site malveillant, comme un site de phishing. Pour cela, ceux-ci ré-utilisent les codes des sites officiels (Charte graphique identique, typosquatting…)
Afin de s'en prémunir, il est conseillé d'adopter certaines bonnes pratiques comme vérifier l'expéditeur du mail, vérifier le contenu, l'orthographe, vérifier les différents liens et la demande du mail.
Utiliser différentes adresses mails en fonction de leur utilisation peut être utile afin de limiter des demandes saugrenues, et inadaptées. Ces différentes adresses agissent comme un filtre. Ne pas répondre aux communications électroniques non sollicitées peut s'avérer utile pour limiter le risque de marketing agressif, tentative d'escroquerie, ingénierie sociale… Ces communications peuvent aussi êtres appelées "Pourriel" qui provient de la contraction des mots Poubelle et Courriel. Ceux-ci sont souvent représentés dans la catégorie "Spam" sur la plupart des systèmes de messagerie moderne.
De plus, le choix de son mot de passe est très important. La longueur du mot de passe, le nombre de caractères différents et le hasard entre les différents caractères sont des facteurs qui peuvent limiter l'attaquant lorsque celui-ci tente de pirater votre boîte mail.
Il est également de bien prendre en compte que, si le chiffrement de client à client

(chiffrement de bout en bout) n'est pas mis en place, des informations transmises via la messagerie instantanée peuvent être interceptées par un attaquant.

Enfin, lorsque nous envoyons un mail, l'unité qui joue le rôle du facteur est le client de messagerie et le protocole utilisé par le serveur de messagerie est le protocole SMTP (Simple Mail Transfert Protocol)

Unité 5 :

Pour établir une connexion avec d'autres équipements sur Internet, votre ordinateur est connecté à une box, elle même connectée au réseau de votre fournisseur d'accès à Internet. Ce dernier est enfin connecté à d'autres entités formant ainsi le réseau Internet.
Le principal équipement chargé d'acheminer les paquets sur Internet est le routeur. Une fois l'adresse IP obtenue, le navigateur peut envoyer une requête HTTP à destination du serveur pour obtenir le contenu de la page web. L'affichage de cette page peut correspondre à une, plusieurs dizaines voir centaines de requêtes HTTP. Le protocole HTTPS cité précédemment est indispensable lors de la consultation de divers sites comme les réseaux sociaux, les messageries électroniques via un webmail, les sites marchands, les comptes en banque et plus généralement tous les services avec un mot de passe et que les informations qui transitent sont sensibles. Ainsi, il est fortement déconseillé et même dangereux de procéder à des paiements sur des sites en HTTP et non en HTTPS.

Un fichier HTML peut contenir beaucoup de ressources comme des liens, vidéos, sons, textes, images, et scripts (JavaScript).

Afin de garantir l'authenticité d'un site internet, un certificat peut être nécessaire à l'intérieur duquel on retrouve une clé publique associée au serveur, la signature d'une autorité de certification et l'identité du serveur que le client souhaite visiter.

Module n°4 :

Unité 1 :

Dans la cybersécurité, il existe plusieurs types de personnes regroupées sous trois catégories :

- Les *Whites Hats* : Ce sont des chercheurs qui ont pour mission, avec l'accord des parties prenantes, de chercher des vulnérabilités dans un système. S'ils en trouvent, ils ont pour mission d'en informer les éditeurs de ces logiciels
- Les *Grey Hats* :
- Les *Blacks Hats* : Ce sont des individus avec des intentions purement malveillantes, qui n'ont pour but uniquement de détruire ou détériorer des systèmes d'informations souvent à des fins politiques ou économiques.

Une vulnérabilité est une défaillance dans la sécurité du système. Une fois qu'une d'entre elle est trouvée et corrigée, elle est souvent communiquée publiquement par les éditeurs via des notes de mises à jour, via des bases de données publiées en ligne (entre autres par des *CERT, Computer Emergency Response Team*, ou *CSIRT, Computer Security Incident Response Team*) , via des chercheurs sur des sites accessibles publiquement.

Le fait de les communiquer à pour but d'informer les utilisateurs n'ayant pas effectué les dernières mises à jour (qui ont pour but de les corriger) l'existence de ces failles et l'importance d'installer les MàJ. Cependant, cela à aussi pour effet d'informer les personnes malveillantes des failles, et celles-ci peuvent donc tenter d'attaquer des personnes n'ayant pas encore tenu à jour leur système.

Les failles sont caractérisées dans le milieu des attaquants comme les failles dites "0-day", ce sont des failles qui ne sont pas encore découvertes et corrigées par les éditeurs, et donc exploitables. Ce terme vient de l'anglais qui signifie "0-jour". Cela fait référence à des failles qui dans un monde "idéal" pour les attaquants auraient été découvertes le jour même et donc pas encore corrigées.

Afin de naviguer en sécurité, il est conseillé de désactiver les plugins inutiles, bloquer les sites suspects et effectuer les mises à jour de votre navigateur et de tous les logiciels utilisés. De manière plus générale, il vaut mieux installer le moins de logiciels possibles afin de limiter le risque de potentiels virus dissimulés au sein de ces programmes.

Unité 2 :

Pour protéger correctement son matériel, il est important de mettre en place certaines bonnes pratiques. Parmis celles-ci, on peut noter le fait d'installer un anti-virus (qui analyse les fichiers présents sur l'ordinateur mais aussi sur les stockages externes connectés à l'ordinateur comme les clés USB), paramétrer

correctement son terminal (si on est habilité à le faire) , activer l'option de mises-à-jour automatiques,

En cas de vol ou perte de celui-ci, il est possible d'avoir au préalable mis en place un nombre maximal de tentatives de connexion, ce qui entrave fortement la progression des attaquants (notamment en cas de BruteForce, attaque qui consiste à tester toutes les combinaisons jusqu'à trouver la combinaison correcte). Le chiffrement de ses données les protège contre un accès illégitime.

Il est important de noter que, lors de l'installation d'un logiciel, il peut vous être proposé d'installer des programmes complémentaires (en cas de partenaires commerciaux par exemple) et il faut donc rester vigilant à n'installer uniquement ce qui est nécessaire.

Dans une entreprise, la sécurité des équipements est assurée par le service informatique, il est nécessaire de s'y conformer, sous peine de graves sanctions. Les terminaux sont configurés par l'administrateur réseau afin de garantir une protection maximale contre les programmes malveillants, et certaines sont mises en place à travers la charte informatique à destination des employés.

Unité 3 :

L'administrateur réseau peut configurer un ordinateur ou un réseau d'ordinateurs avec des sessions qui ont pour objectif d'identifier les utilisateurs (et donc retracer les activités) et de définir les privilèges de chaque utilisateur.

- Les sessions "*administrateur*" sont celles avec le plus de privilèges, elles ont les pleins pouvoirs sur un ordinateur et sont uniquement réservées aux administrateurs réseau.
- Les sessions "*utilisateur*" sont des sessions pour les employés avec des droits limités, principalement utilisées par les salariés afin d'exécuter des logiciels par exemple. Chaque employé à sa propre session et ne peut effectuer que certaines actions délimitées par l'administrateur réseau (ne peut pas installer de nouveaux logiciels par exemple).
- Les sessions "*invités*" sont les comptes avec le moins de privilèges et ne permettent souvent que de naviguer sur internet sans pouvoir conserver ses informations d'une session à une autre.

Utiliser un compte administrateur pour travailler au quotidien présente plusieurs risques puisque ses privilèges permettent d'installer des programmes malveillants ou répandre une contamination sur le réseau interne de l'entreprise, ce qui n'est pas le cas avec un compte utilisateur étant donné que ceux-ci sont dans un

réseau segmenté, et ne peuvent ainsi pas contaminer certaines sections de l'entreprise.

Afin d'éviter l'usurpation d'identité via l'usage de votre session, il est conseillé de définir un verrouillage automatique après un temps défini pour éviter toute mauvaise utilisation d'un appareil déverrouillé. Il ne faut pas que les identifiants et mots de passe de n'importe quelle session soient divulgués à qui que ce soit. Ceux-ci doivent rester propres à chaque utilisateur, propriétaire de sa session.

Pour garantir une sauvegarde des données efficace, celle-ci doit être réalisée fréquemment, conservée ailleurs qu'à l'endroit où les données sont utilisées habituellement, et stockée sur des supports uniquement pour les besoins de la sauvegarde avec le minimum d'accès à l'extérieur.

Unité 4 :

Les périphériques de stockage externes (Clé USB par exemple), se divisent en trois catégories : Les Disques Optiques, Les Disques Mécaniques à Plateaux, et Les Disques à Mémoire Flash, et sont très utiles puisqu'ils permettent de transporter facilement un grand volume d'information, et permettent également le transport de ces données.

Cependant, ceux-ci ont également plusieurs points faibles d'un point de vue sécurité des données mais aussi de l'ordinateur sur lequel le périphérique est branché.

Les données sur une clé USB peuvent être compromises, volées (vol du périphérique), perdues (perte du périphérique), divulguées ou encore détruites (destruction physique de la clé). En cas de vol du périphérique, il est cependant possible de chiffrer les données afin qu'un utilisateur autre que vous n'y ait pas accès. Il peut être intéressant de le faire si les données stockées sont à caractère sensible ou personnelles.

Il est important que même après la suppression des données sur un composant de stockage, les données restent stockées dessus et uniquement le chemin d'accès est supprimé. Ainsi, des utilisateurs malveillants peuvent parfois avoir accès à ces données grâce à certains outils, même si vous avez réenregistrer une quelconque information par dessus.

De plus, il est également dangereux pour votre ordinateur d'y brancher une clé USB car celles-ci peuvent être facilement piégées. Lorsque l'on branche un périphérique à un ordinateur, celui-ci reconnaît automatiquement de quel périphérique il s'agit puis le configure automatiquement avec les droits correspondants afin d'éviter à l'utilisateur de le faire manuellement (droit de taper sur des touches pour un clavier). Cependant, certains périphériques à l'allure de clé USB paraissent comme des claviers aux yeux de l'ordinateur et ainsi peuvent taper

du texte. In fine, le soi-disant clavier tape du texte malveillant afin de permettre à un attaquant de prendre possession de votre ordinateur entre autres.

C'est pourquoi il est très fortement déconseillé (voir interdit en entreprise) de brancher des périphériques externes car ceux-ci peuvent facilement être piégés en allant de "clés USB" à des "Cigarettes éléctroniques". Il est conseillé d'utiliser le chargeur secteur fourni pour recharger votre matériel comme un téléphone, cigarette électronique…
Cette faille est difficile à prévenir car elle relève de l'erreur humaine, et les programmes malveillants présents sur un périphérique ne sont pas toujours détectés par l'anti-virus de l'utilisateur (ils peuvent néanmoins être détectés en cas de scan du périphérique par exemple).

Unité 5 :

Afin de limiter la propagation et la compromission d'un virus au sein du SI de l'entreprise, ou même dans le cadre personnel, il est conseillé de séparer les différents comptes ou sessions en fonction des usages. Cela consiste à cloisonner les univers personnels et professionnels en utilisant par exemple des mots de passe différents pour chaque site ou application, on encore différents comptes selon les besoins, en utilisant des comptes avec des droits différents, ou en utilisant des différents comptes de messagerie électroniques. Cela va avec la même démarche que de ne pas utiliser un compte administrateur au quotidien afin de limiter les droits de l'attaquant en cas d'infection par un virus.

Un VPN (Virtual Private Network) permet d'accéder au réseau interne de l'entreprise depuis l'extérieur et d'assurer la confidentialité des données échangées en chiffrant les communications. En revanche, il ne protège pas le système d'information (SI) de l'entreprise contre la propagation d'éventuels virus lors du raccordement de votre poste.

Le BYOD (Bring Your Own Device) ou AVEC (Apportez Votre Equipement personnel de Communication) consiste à travailler avec son ordinateur personnel et doit être proscrit par l'entreprise, car cette façon de travailler ouvre les portes à diverses failles de sécurité (notamment en cas d'infection par un virus sur votre ordinateur lié à un usage personnel et qui pourrait se transmettre au SI de l'entreprise).

Pour travailler en sécurité, il est nécessaire de suivre les consignes de la charte de l'entreprise. L'utilisateur du SI s'engage à la respecter en la signant en même temps que son contrat de travail. Celle-ci recommande entre autres de séparer les usages, de mettre à jour son matériel, mais aussi d'utiliser des outils de chiffrement et des comptes sans privilèges.
Il est également recommandé d'interdire l'utilisation de son équipement professionnel à des personnes extérieures à l'entreprise et de ne pas héberger de

données professionnelles sur son équipement personnel et inversement. Celle-ci peut également vous interdire d'utiliser votre poste personnel pour travailler (cf. BYOD)