Compte rendu :

Panorama de la SSI :

Les systèmes d'information sont aujourd'hui présents partout, à la maison et au travail, sous des formes différentes. On pense naturellement aux ordinateurs et aux équipements réseaux (tels que le modem ADSL téléphonique, la fibre…), mais il faut également compter les ordiphones (smartphones en anglais), les imprimantes et photocopieurs, les télévisions et montres connectées, pour ne citer que des exemples classiques. Cette hyperconnectivité se manifeste au travers de réseaux, au premier rang desquels on trouve Internet, l'agrégation mondiale des réseaux d'opérateurs. On peut également citer les réseaux téléphoniques mobiles, aujourd'hui complètement interconnectés à Internet. Du point de vue local, d'autres technologies permettent de transférer des données sur de faibles distances telles que les technologies Wi-Fi et Bluetooth, qui sont beaucoup utilisées dans la domotique ou sur le marché des vêtements intelligents. Un bracelet connecté, par exemple, n'est jamais très loin du téléphone auquel il transfère ses données. Aujourd'hui, de nombreux sites internet vous proposent de communiquer ou d'héberger vos données au travers d'espaces en ligne appelés « cloud ».Le « cloud » c'est-à-dire le « nuage », consiste en la mutualisation des ressources de calcul et de stockage distribuées dans des datacenters répartis dans le monde entier. Il n'est donc pas nécessaire de stocker les données sur un poste de travail ou d'être connecté à un réseau local pour consulter ses documents de travail ou ses photos de vacances. L'ensemble des réseaux qui relient ces objets crée le cyberespace. Par conséquent, les attaques informatiques utilisent ce territoire pour atteindre les cibles. Or, celui-ci possède des propriétés particulières qui font qu'il est nécessaire de repenser le modèle habituel. En effet, le cyberespace est un espace sans frontières concrètes. Mais ces propos sont à nuancer, car les réseaux reposent sur des infrastructures techniques physiques qui se trouvent sur un territoire bien déterminé : il y a donc une dimension de territorialité. Par exemple, dans certains pays, il est interdit de posséder ou de faire transiter une donnée qui serait chiffrée sans permission. Le cyberespace possède une double dimension : Il s'agit à la fois d'un espace social de partage de biens immatériels et de connaissances, mais aussi d'un support pour les nombreux services critiques comme la gestion à distance des usines. Cet espace possède des caractéristiques propres comme une quasi-instantanéité, des espaces contractés, des mouvements et extensions perpétuels .Chaque individu a la possibilité de créer de nombreux espaces dans ce monde immatériel .Ces caractéristiques donnent un avantage certain aux attaquants, car l'impact peut être quasi-immédiat. L'attaquant bénéficie d'un effet de surprise très avantageux. Ainsi la défense doit faire preuve d'une forte réactivité . Contrairement à ce que l'on pourrait penser, ce cyberespace n'est pas totalement libre et désordonné. Cependant, la nature décentralisée d'Internet fait de lui un espace « contrôlé » par plusieurs organismes, états ou entreprises. À tous les échelons, de nombreux organismes exercent ou peuvent exercer un contrôle ou une censure sur les informations qui y circulent. Notons tout d'abord que pour fonctionner, le réseau est tributaire de câbles ou de satellites : en l'absence de « tuyaux » suffisamment grands, le trafic peut être très fortement ralenti. Aujourd'hui, de nombreux pays sont dépendants, pour leur accès au réseau, d'un ou deux câbles sous-marins ou souterrains. En Afrique par exemple, des pays entiers voient leur accès tributaire des décisions des pays voisins ou des choix des entreprises privées. Notons également que certains pays disposent techniquement de la capacité de bloquer ou de censurer tout ou partie d'Internet. Durant les manifestations qui ont précédé la chute de Hosni Moubarak, par exemple, l'Égypte a pu couper quasi-instantanément l'accès au réseau en faisant pression sur les fournisseurs d'accès à Internet (FAI). Sans aller jusqu'à ces extrémités, de nombreux pays exercent aussi un contrôle très fort sur le réseau. Des contenus contraires aux lois nationales sont ainsi bloqués dans la plupart des pays autoritaires, mais aussi dans des démocraties : en France, la loi sur les jeux d'argent en ligne permet d'ordonner le filtrage des sites qui n'ont pas reçu un agrément.

Un monde à haut risques :

Il existe plusieurs types de pirates ayant des motifs d'attaques différents : du hacker isolé agissant par vengeance ou démonstration de compétence, au groupe de hackers organisé ayant pour objectif de revendre ses services pour déstabiliser des entreprises, ou de revendre des informations subtilisées dans des bases de données non-sécurisées comme des informations bancaires ou des données nominatives. Des groupes organisés tels que le réseau Anonymous quant à eux procèdent par exemple à des actions de défacements, de piratage de sites web, ou de divulgation d'informations pour revendiquer des actions auprès d'entreprises réputées ou pour procéder à des opérations punitives. Les attaques de masse sont aujourd'hui très courantes, car leur coût est très faible pour l'attaquant et les revenus générés peuvent rapidement devenir intéressants. Les attaques de masse scannent ou balayent Internet pour trouver des objets non-sécurisés comme les caméras que nous avions citées en introduction pour en prendre le contrôle facilement si le mot de passe n'a pas été changé. Les attaquants arrivent ainsi à se constituer un réseau d'objets connectés pour en faire un « botnet », c'est-à-dire un réseau de machines compromises, autrement dit un groupe d'ordinateurs infectés et contrôlés par un pirate à distance. Ce réseau servira par la suite à commettre une attaque sur une cible prédéfinie par l'intermédiaire des objets connectés des entreprises ou des logements personnels sans que personne ne le sache. En parallèle des attaques massives que nous venons de voir, les entreprises ou les personnes peuvent être victimes d'attaques ciblées. A contrario des attaques de masse, les attaques ciblées sont moins courantes. En effet, les modes opératoires sont plus complexes et demandent des compétences spécifiques ou une connaissance particulière de l'entreprise. Concrètement, cela veut dire que l'attaquant connaît sa victime et qu'il met en œuvre tout un procédé pour l'atteindre. Il s'agit principalement de cas d'espionnage pour obtenir une information qui n'est pas publique : espionnage économique ou industriel, atteinte à la propriété intellectuelle, ou encore pour des raisons politiques. Pour les entreprises et les particuliers, les conséquences des cyber-attaques peuvent être de plusieurs natures mais la conséquence la plus couramment rencontrée est la perte financière engendrée par la fraude. La fraude est un acte commis dans l'intention de nuire et d'en tirer un profit illicite. Plusieurs conséquences sont alors possibles : les « pirates » peuvent se connecter aux systèmes dans le but de détruire des données, ou au contraire d'accumuler les données pour mieux connaitre leur « proie » et parvenir à détourner de l'argent. Ce dernier cas est illustré par la « fraude au président » qui consiste à obtenir un virement vers un compte à l'étranger, sur ordre supposé d'un dirigeant ou d'un fournisseur, derrière lequel se cache en réalité un internaute malveillant. En effet, la fraude est assez facile à mettre en œuvre avec les nouveaux modes de communication puisqu'il est assez simple de récupérer des données d'une entreprise en comparaison du gain financier qui peut être important .On peut également retrouver la fraude dans des cas plus précis et plus techniques comme les attaques sur les systèmes d'information des bourses et notamment les systèmes de HFT (« High Frequency Trading ») où il y a un risque d'effacement de millions de transactions et de détournement d'investissements associés. Dans ce cas, des sommes importantes d'investissement peuvent être perdues et donc léser l'entreprise. Au-delà de l'aspect financier, les attaques informatiques peuvent jouer sur l'avenir des dirigeants. Par exemple, lors du piratage d'un site de rencontres extraconjugales, le PDG de la société propriétaire du site a décidé de démissionner suite à la publication de 30 Go de données du site contenant les noms, les comptes utilisateurs, les courriels et les adresses ainsi que les historiques de navigation de ses clients. Malheureusement cette expérience a démontré que cela pouvait aller tragiquement plus loin puisque certaines personnes se sont suicidées suite aux révélations du site. Il s'agit là d'un aperçu des conséquences sociales que peut avoir un piratage. Le cyberespace est un monde à hauts risques qu'il est important d'identifier afin de mettre en place les mesures de protection adaptées pour protéger les systèmes d'information visés par les attaquants. Si malgré toutes vos précautions vous êtes la cible d'une cyber-attaque, quelques recommandations s'imposent. En tant que salarié, il est tout d'abord recommandé de débrancher son ordinateur du réseau et de couper son wifi. Ensuite il est important de signaler l'attaque à votre service informatique dans les plus brefs délais afin qu'il puisse intervenir pour évaluer les dommages et limiter les conséquences. D'autre part, la plateforme cybermalveillance.gouv.fr mise en place par l'ANSSI a pour objectif de venir en aide aux victimes d'actes de cybermalveillance. La plateforme s'adresse aux particuliers et également à toutes les entreprises et collectivités territoriales (hors OIV). Elle a pour objectifs. La mise en relation des victimes via une plateforme numérique avec des prestataires de proximité susceptibles de les assister techniquement .La mise en place de campagnes de prévention et de sensibilisation à la sécurité du numérique, sur le modèle de la sécurité routière .La création d'un observatoire du risque numérique permettant de l'anticiper.

Sécurité sur Internet :

Internet ne repose pas sur de la magie et nous allons voir en détail comment il rend toutes ces activités possibles. La navigation sur Internet repose sur une architecture appelée client/serveur. Il s'agit du mode de fonctionnement le plus courant en informatique de nos jours. Les clients envoient leurs demandes au serveur qui envoie à son tour une réponse à ces demandes. Ils sont tour à tour émetteurs et récepteurs de messages. Notez que votre ordinateur est capable d'interroger simultanément de nombreux serveurs. C'est ce qui se passe lorsque vous êtes connecté sur le web et que vous consultez simultanément Skype ou votre messagerie qui sont des services hébergés sur Internet. En effet, sur Internet différents services vous sont proposés dont le World Wide Web qui permet de naviguer de site en site. Pour assurer le transit des données entre l'émetteur et le récepteur, celles-ci sont découpées en paquets. Ces paquets se composent d'une partie de la donnée que l'émetteur souhaite transmettre, à laquelle sont ajoutées des informations relatives à son transport, telles que l'adresse IP du destinataire (numéro d'identification de son ordinateur sur un réseau). Pour illustrer ce fonctionnement, prenons l'exemple de l'affichage d'une page web, et comparons-là au transport d'un courrier postal sur un réseau routier. Le point de départ est la box ADSL du domicile, et le point d'arrivée est le serveur hébergeant les éléments du site à afficher. Lors d'un clic sur le lien hypertexte menant à la page web, une requête est envoyée sur le réseau, sous la forme de paquets.ZwAMpPfySGLjdm4x_mrTpsi7Qjg28SAb3-_NOPROCESS_timeline_1.png. Cette requête part de la box vers le réseau de l'opérateur, et circule à travers de nombreux routeurs appartenant à différents opérateurs. Les routeurs se basent sur l'adresse IP du serveur web, comparable à une adresse postale, pour acheminer les paquets jusqu'au lieu physique où est hébergé le serveur de destination. Restez prudent sur vos téléchargements et surtout sur l'ouverture des fichiers en provenance d'Internet ou de supports externes tel les clés USB ou les disques durs externes, que vous soyez à l'initiative du téléchargement ou qu'un expéditeur vous l'adresse en pièce jointe par messagerie. De très nombreuses affaires de cyber-attaque démarrent par un double-clic innocent, sur un simple fichier de tableur par exemple ! Installez un antivirus (lui-même obtenu sur un site d'éditeur de confiance !) pour assurer un scan ponctuel des fichiers téléchargés. De plus un scan régulier de l'ensemble du disque est indispensable pour s'assurer qu'une propagation n'est pas en cours sur votre poste ou y remédier le cas échéant. En contexte professionnel, ces manipulations sont du ressort des équipes de Direction des Systèmes d'Information s'il y en a une. Le module 4 de ce MOOC sera consacré à la sécurisation du poste de travail. En attendant, nous allons revenir plus en détails sur les bonnes pratiques à adopter lorsque vous naviguez sur Internet ou utilisez votre messagerie électronique. Chaque site web accessible sur Internet dispose d'une adresse compréhensible (et si possible mémorisable !) par l'homme. Prenons l'exemple de l'adresse du site de l'ANSSI « www.ssi.gouv.fr ». Différents niveaux composent cette URL. Étudions sa composition de droite à gauche. Le « .fr » est géré par une association nommée AFNIC (Association française pour le nommage Internet en coopération). Le « .gouv » est un sous-domaine réservé à l'État français. Le « ssi » est le terme choisi par l'État français pour référencer tous les noms de domaines qui relèvent de l'ANSSI. Le « www » est un sous-domaine faisant référence par convention au World Wide Web. Il est traditionnellement destiné à héberger un site web. Tout comme une erreur dans un chiffre d'un numéro de téléphone, une seule erreur de caractère dans l'adresse d'un site vous entraîne vers un site web totalement différent.Soyez vigilant avec l'écriture de ces adresses puisqu'en théorie n'importe qui peut demander à un prestataire spécialisé (appelé registraire), l'enregistrement d'un nom vers une adresse IP si celui-ci n'est pas déjà réservé. L'objectif du « typosquatting » est de réserver un nom dont la typographie est proche d'un site officiel pour tromper l'utilisateur ou nuire à l'entité. C'est pour cela que les équipes web d'une entité réservent généralement plusieurs adresses similaires d'un point de vue typographique, avec un maximum d'extensions possibles (.fr, .com, .org, etc.) pour éviter que leurs visiteurs ne tombent sur un site malveillant ou qui nuit à l'image de l'entité.Exemple d'impact : Pour illustrer ce concept, prenons l'un des exemples les plus marquants de l'histoire du typosquatting qui est celui d'un site réservé aux adultes qui se nommait www.whitehouse.com qui a pour un temps été confondu avec le site institutionnel de la Maison Blanche www.whitehouse.gov.Aujourd'hui encore un site satirique contre la Maison Blanche est hébergé sous l'adresse www.whitehouse.org. Pour résumer le typosquatting, faites attention aux fautes de frappe lorsque vous saisissez une URL dans la barre d'adresse de votre navigateur. Une fois que vous avez accédé au site, vérifiez qu'il correspond à ce que vous attendez et pour éviter toute erreur de saisie ultérieure, enregistrez-le dans vos favoris ! Les messageries électroniques sont l'objet de nombreuses menaces déjà présentées dans l'unité 1 de ce module : logiciels malveillants, marketing agressif, rançongiciel et autres techniques d'ingénierie sociale, etc. Généralement, les courriels malveillants sont envoyés à destination d'un grand nombre de cibles, ils ne sont pas (ou peu) personnalisés. Si un courrier vous paraît trop vague ou vraiment impersonnel, il y a de grandes chances qu'il s'agisse d'un pourriel. Ce que nous avons vu dans cette unité, avant d'afficher une page web, le navigateur doit connaître l'adresse du serveur web correspondant à l'aide d'un ou plusieurs serveurs DNS. Lorsque l'adresse IP est obtenue, le navigateur demande une page du site au serveur web. L'utilisation d'un serveur mandataire (ou proxy) peut vous permettre d'optimiser l'ouverture de pages web déjà consultées, d'améliorer la sécurité de vos navigations et d'empêcher une éventuelle infection.

Sécurité du poste de travail et nomadisme :

Pour commencer ce cours, intéressons-nous tout d'abord à la notion de vulnérabilité.En effet, les personnes cherchant à mieux connaître les systèmes informatiques que nous utilisons tous les jours sont nombreuses. Il peut s'agir de criminels, d'organisations mafieuses, de services de renseignement mais aussi de chercheurs du domaine privé ou universitaire. Quel que soit le profil de la personne qui travaille sur cette recherche, une fois qu'une défaillance est détectée dans la sécurité du système, on parle de vulnérabilité. Dans le cas d'organisations criminelles, cette vulnérabilité est plutôt utilisée pour attaquer le système concerné, tandis que dans le cas des chercheurs, cela conduit plutôt à la corriger. L'une des premières méthodes utilisées en sécurité a été la sécurité par l'obscurité. Celle-ci consiste à maintenir un attaquant potentiel dans l'ignorance du fonctionnement interne du système auquel il s'attaque. En informatique et en électronique, cela consiste à ne pas diffuser le code qui fait fonctionner les logiciels, les spécifications des circuits et à limiter la documentation à comment « faire fonctionner » le système, sans expliquer « comment il fonctionne ». rappelez-vous qu'il est essentiel de respecter un certain nombre de paramètres de base pour assurer la sécurité de vos appareils. Veillez à adopter une utilisation « responsable ».Maintenez à jour votre système et ses logiciels.Activez votre pare-feu. Installez éventuellement des logiciels supplémentaires qui peuvent participer à l'amélioration du niveau de sécurité, en ayant conscience de leurs conditions d'utilisation (respect de la confidentialité et de la vie privée), ainsi que des risques associés.Soyez vigilant sur l'installation de logiciels tiers.Enfin, rappelez-vous que le chiffrement est essentiel pour protéger les données de vos appareils mobiles tels que téléphones, tablettes et ordinateurs portables. Aujourd'hui les équipements modernes disposent de nombreux outils et interfaces de communication : Bluetooth, Wi-Fi, NFC, Micro, Caméra, etc. auxquels peuvent accéder le système et les applications. Notons que ces interfaces peuvent présenter des risques. En effet, certaines peuvent être utilisées à votre insu et présentent une surface d'attaque supplémentaire pour votre équipement ou des vecteurs supplémentaires d'atteinte à la confidentialité. Pour conclure ce module, rappelez-vous de ne pas connecter à votre ordinateur un périphérique amovible provenant de source douteuse. Chiffrez les données des périphériques amovibles dont la perte ou le vol pourrait vous être préjudiciable. Rappelez-vous que tous les supports de stockage ont une durée de vie plus ou moins limitée, il est donc nécessaire de faire au minimum deux copies de sauvegarde (sur des supports de stockage différents) des données que vous ne voudriez pas perdre, et de choisir des supports de stockage adaptés à la durée de conservation souhaitée. Nous avons vu que cette cohabitation des usages (dans un sens ou dans l'autre) pose des problèmes en matière de sécurité des données (perte ou vol des appareils, intrusions, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ d'un collaborateur, etc.). En effet, les usages et les mesures de sécurité associés aux environnements professionnels et personnels sont différents, c'est pourquoi il est fortement conseillé de séparer le matériel utilisé. Pour bien comprendre les enjeux de cette séparation des usages, arrêtons-nous quelques instants sur une pratique de plus en plus répandue de nos jours.En effet, on constate qu'aujourd'hui la frontière entre le monde professionnel et le monde personnel s'estompe. L'illustration la plus connue est certainement celle qui consiste à travailler en environnement professionnel avec son équipement personnel (ordinateur, ordiphone, tablette, etc.).Cette pratique, connue sous le nom de BYOD (Bring Your Own Device) ou sous le nom francisé AVEC (Apportez Votre Equipement personnel de Communication), est à proscrire.K1B9QvoNCkDGLqHD_uDtrWvVoDi_sxeDu-_NOPROCESS_timeline_2.pngEn effet, on pense souvent à tort que puisqu'on utilise son ordinateur personnel tous les jours, il n'y a aucun risque à l'utiliser pour son activité professionnelle. En fait, n'importe quel système informatique peut contenir des programmes malveillants. Le BYOD est une solution parfois utilisée dans des entreprises de toutes tailles et tous secteurs d'activité confondus.Cependant, cette pratique doit être proscrite car elle pose des problèmes en matière de sécurité des données pour les entreprises (vol ou perte des appareils, intrusions, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur).

DEFINITION :

L'extension, c'est le suffixe du nom du fichier, qui lui est renseigné par le créateur du fichier (exemple : logo-anssi.jpg pour une image représentant le logo de l'ANSSI).

Dans un navigateur, on rencontre principalement deux protocoles :

- « http » est le moyen non-sécurisé d'accéder à des ressources,
- « https » est la variante sécurisée de ce protocole.

Un cookie est un objet associé à un site web stocké sur l'ordinateur, qui permet à ce site de stocker des informations relatives au client et de récupérer ces informations lors d'une visite ultérieure du client

Serveurs DNS traduisent des demandes de noms en adresses IP, en contrôlant à quel serveur un utilisateur final va se connecter quand il tapera un nom de domaine dans son navigateur

Une adresse IP (Internet Protocol address) est une suite de chiffres attribuée à chaque appareil connecté à un réseau informatique ou à Internet.

Un proxy (aussi appelé serveur mandataire en français) est un programme qui joue le rôle d'intermédiaire entre un ordinateur et un réseau. Il transfère la demande de votre ordinateur vers le site cible en utilisant sa propre adresse IP (et non celle de votre ordinateur).

La cybersécurité est un « sous-ensemble » de la sécurité informatique. Elle vise à protéger les ressources du piratage ou des cyberattaques, c'est-à-dire des menaces provenant d'Internet ou survenant via Internet.

LE COMCYBER est un commandement opérationnel, qui rassemble l'ensemble des forces de cyberdéfense du ministère sous une autorité interarmées.

LE CNIL est le régulateur des données personnelles. Elle accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits

OIV Les opérateurs d'importance vitale sont désignés par le ministre coordonnateur du secteur qui les sélectionne parmi ceux qui exploitent ou utilisent des installations indispensables à la vie de la Nation.

LE CHIFFREMENT HYBRIDE Le chiffrement hybride consiste à : Créer une clef de session aléatoire. Chiffrer de façon symétrique avec la clef de session. Chiffrer la clef de session avec la clef publique du destinataire.

HAMEÇONNAGE Technique de fraude sur Internet visant à obtenir des renseignements confidentiels (mot de passe, informations bancaires…) afin d'usurper l'identité de la victime

-Botnet : réseau de terminaux infectés par un/des malwares , souvent à utilisation malveillante.

-Rançonnement : attaque malveillante à but de nuire au bon fonctionnement de leur terminaux afin de couper leur activité. Les pirates demandent alors une rançon en contrepartie d'un arrêt de l'attaque. Pour effectuer cette attaque, les pirates utilisent un rançongiciel.

-La défiguration de site (aussi parfois vu sous le terme « défacement » par anglicisme) consiste à modifier une partie d'un site web, affichant alors des éléments choisis par le pirate.

-MALVERTISING : le pirate intégrera du contenu malveillant sur des fausses publicités en ligne pour essayer de piéger les visiteurs de sites web sans passer par le propriétaire du site en question.

-l'ingénierie sociale (plus connue sous son nom anglais « social engineering ») désigne l'ensemble des attaques informatiques mettant l'accent sur les vulnérabilités humaines.Elle est souvent utilisée par les pirates pour arriver à leurs fins en parallèle d'attaques plus techniques. Ils ont recours à de nombreuses ruses qu'il convient de savoir déjouer autant que possible.

-L'hameçonnage ou le phishing consiste à obtenir du destinataire d'un courriel, d'apparence légitime, qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion à des services financiers, afin de lui dérober de l'argent.

-Un fichier n'est fondamentalement qu'une suite de 0 et de 1 compréhensibles par l'ordinateur.

-L'extension, c'est le suffixe du nom du fichier, La convention veut que l'extension du fichier corresponde à son format, cela permet non seulement d'identifier rapidement le format du fichier mais aussi de lui associer un logiciel par défaut (c'est-à-dire le logiciel automatiquement choisi pour l'ouvrir).

-Internet désigne le réseau informatique qui relie par le biais du protocole de communication IP (Internet Protocol) des millions d'ordinateurs à l'échelle mondiale.

-Le World Wide Web ou Web désigne une des utilisations possibles d'Internet. Il a été inventé plusieurs années après Internet et désigne un système hypertexte public qui fonctionne sur Internet et permet de consulter des pages web et de naviguer entre elles via des hyperliens.

-Un nom de site est associée à une adresse IP sur laquelle du contenu est hébergé.

-L'objectif du « typosquatting » est de réserver un nom dont la typographie est proche d'un site officiel pour tromper l'utilisateur ou nuire à l'entité.

-Un cookie est un objet associé à un site web stocké sur l'ordinateur, qui permet à ce site de

stocker des informations relatives au client et de récupérer ces informations lors d'une visite ultérieure du client.

-Navigation privée permet de limiter les traces de navigation laissées sur l'équipement lors de notre passage, mais attention elle ne préserve pas des menaces et on est encore loin de l'accès totalement anonyme sur le grand réseau Internet !C'est d'ailleurs généralement rappelé lors de l'activation de ce mode : votre fournisseur d'accès ou votre entreprise dispose toujours de traces des sites auxquels vous accédez.

-Un pourriel est une communication électronique non sollicitée.

-Le DNS (Domain Name System) est le nom d’un service hiérarchique distribué jouant le rôle d’annuaire pour Internet.

-vulnérabilité: une faille dans la conception, l’exécution ou la gestion d'un système informatique

-Les « black hats » qui cherchent des failles pour les exploiter à des fins de malveillances ou de profits.

-Les « white hats » qui cherchent des failles pour les remonter aux éditeurs et fabricants afin qu’ils améliorent leurs outils.

-pare-feu : blocage des connexions entrantes et sortantes du réseau.