Guide des bonnes pratiques

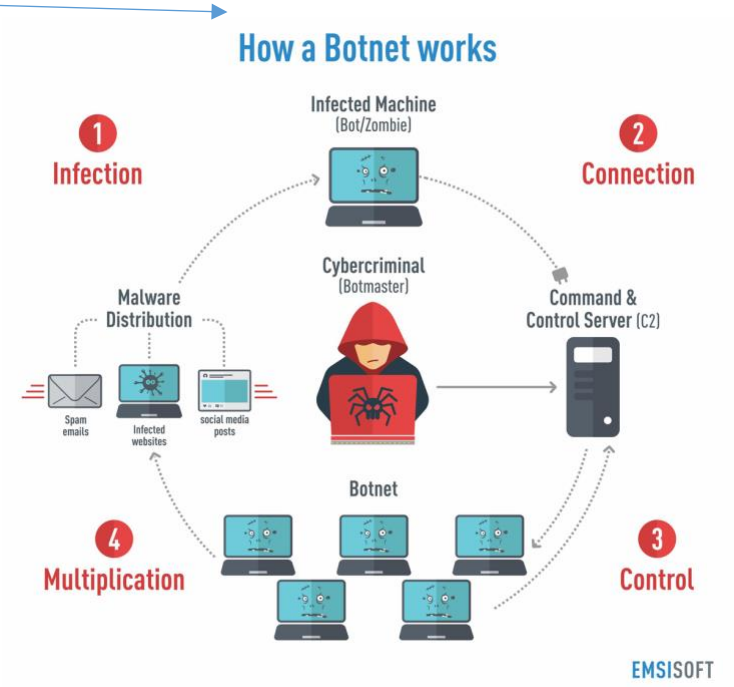
Bonjour, ce document est destiné à tous les membres M2L, actuellement il est composé en deux parties bien distinctes : -réseaux sociaux, danger et bonne pratique
-mobilité et technologies en entreprise.

Partie réseaux sociaux :

La première partie parlera des réseaux sociaux comme son nom l'indique, elle traitera plus particulièrement de son utilisation dans les milieux sensibles (entreprise, défense militaire et personnel).
Le but sera de vous avertir sur les dangers qui plane sur vous et l'entreprise si vous ne respectiez pas consciencieusement ces petites règles du quotidien et de voir les nouveautés en matière de Cybersécurité.

Rappels des menaces basiques (sur les réseaux sociaux) :
-les vers (worm en anglais) : pour rafraîchir la mémoire de tous commençons par un classique, le ver est un programme **qui se reproduit et se déplace à travers un réseau** sans avoir besoin de support physique ou logique (disque dur, programme hôte, fichier, etc.) ; un ver est donc un virus spécialisé dans la propagation réseau.

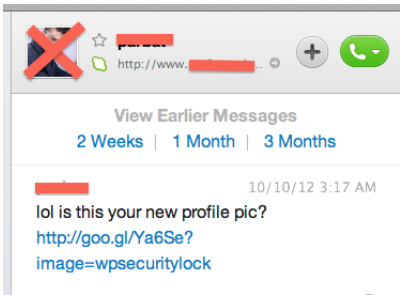
Exemple avec Koobface spécialement conçu pour se propager grâce aux réseau sociaux et utilisant des **Botnet**.



Koobface fut conçu pour se propager à travers les réseaux sociaux, enrôler plusieurs machines avec son botnet, hacker plus de comptes et spammer plus pour enrôler d'autres machines. Pendant ce temps les botnets habituels font de l'argent notamment avec les scareware et autres services de rencontres russes.

Scareware : logiciel malveillant qui trompe les utilisateurs pour les amener à visiter des sites web infestés de programmes malveillants ; **les scarewares peuvent prendre la forme de fenêtres contextuelles**.
Koobface agira sur **facebook** un certain temps, ce qui lui permis potentiellement de toucher pas loin de 200 millions d'utilisateurs (soit pratiquement toute la population du Brésil 2017).

D'autres réseaux sociaux eux aussi ont eu des problèmes, exemple Skype :



Message d'un inconnu (ou pas) Infecté par le vers qui est devenu un Botnet.
Ce dernier essaye de vous faire cliquer sur ce lien qui vous amènera vers le site contenant le vers destiné à vous infecter.

Attentions certains vers peuvent aussi se propager par clef USB.

Conseille : -si vous êtes infecté, le plus souvent c'est un contact qui va vous avertir
-la suppression de cette infection se fera comme tous les programmes malveillants (anti-malware,anti-virus…)
-pour se protéger : avoir un antivirus et pare-feu à jour et actif, vérifier toujours le contenu d'un lien **sans cliquer** et en laissant sa souris dessus ou utiliser un site comme (https://www.virustotal.com/gui/home/upload) et ne jamais mettre de clef USB d'inconnus dans l'ordinateur.

-Cheval de Troie (Trojan en anglais) : un cheval de Troie est un logiciel malveillant – maliciel – qui pourra prendre le contrôle de votre ordinateur ou en perturber le fonctionnement (voler les données bancaires, détruire des données, etc).

Pour être infecté par un Trojan, il faut le télécharger sans le savoir.

Souvent c'est un fichier .rar,.zip,.dll.exe, etc qui se cache dans l'installation d'un programme ou bien d'un jeu.

Sa présence ne peut se déceler que par un comportement anormal de votre ordinateur.

C'est pour cela que je vous déconseille les téléchargements sur des sites non sécurisés (sans le logo cadenas c'est-à-dire sans https) et douteux, pour les mails infectés nous verrons ça dans quelques instants.

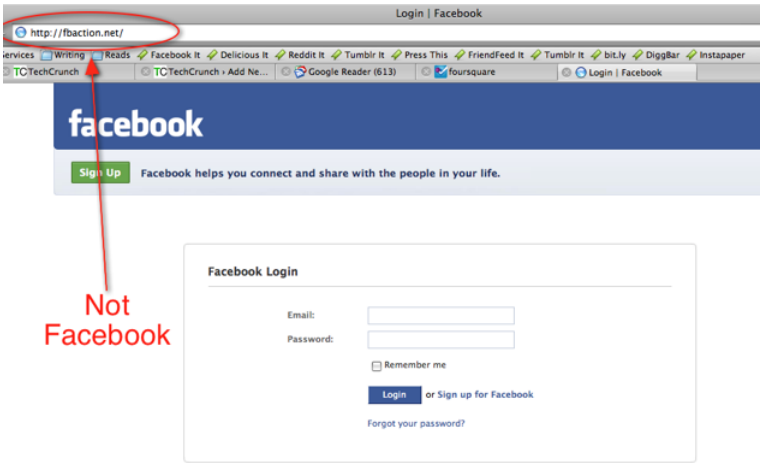
La partie rappels rappel est finis

Bien-sûr,
Je n'ai pas parlé des liens raccourcis piégeait car ils sont présents partout : mail, message sur toutes plateformes et réseaux sociaux.
Et pour l'usurpation d'identité car elle ne peut se faire que par un hack

Comme par l'attitude désinvolte des utilisateurs écrivant leur password et l'accrochant
Sur leur ordinateur par exemple mais c'est rare qu'une entreprise soit touchée.

ATTENTION CETTE PARTIE PARLE AUSSI BIEN DE MENACES DES RESEAUX SOCIAUX QUE DE CELLE DE L'ENTREPRISE.

L'hameçonnage (phishing en anglais) : de nos jours l'hameçonnage est rarement représenté sous cette forme, mais nous devons constamment nous méfier, car de veille méthode peuvent ressortir.



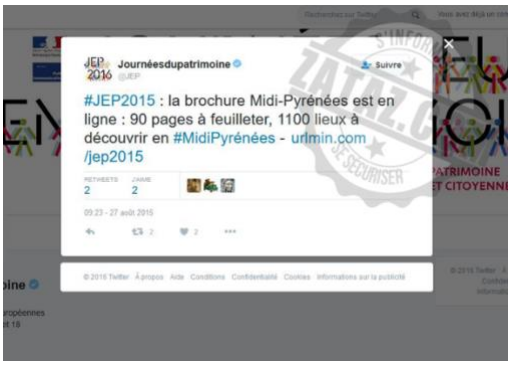
La méthode n'est pas très compliquée à comprendre, le nom de domaine de facebook qui je le rappelle :

n'est pas le bon et donc vous êtes sur un faux site, un copier collé créé dans le but que vous rentriez vos vrai identifiant facebook pour subtiliser votre compte.

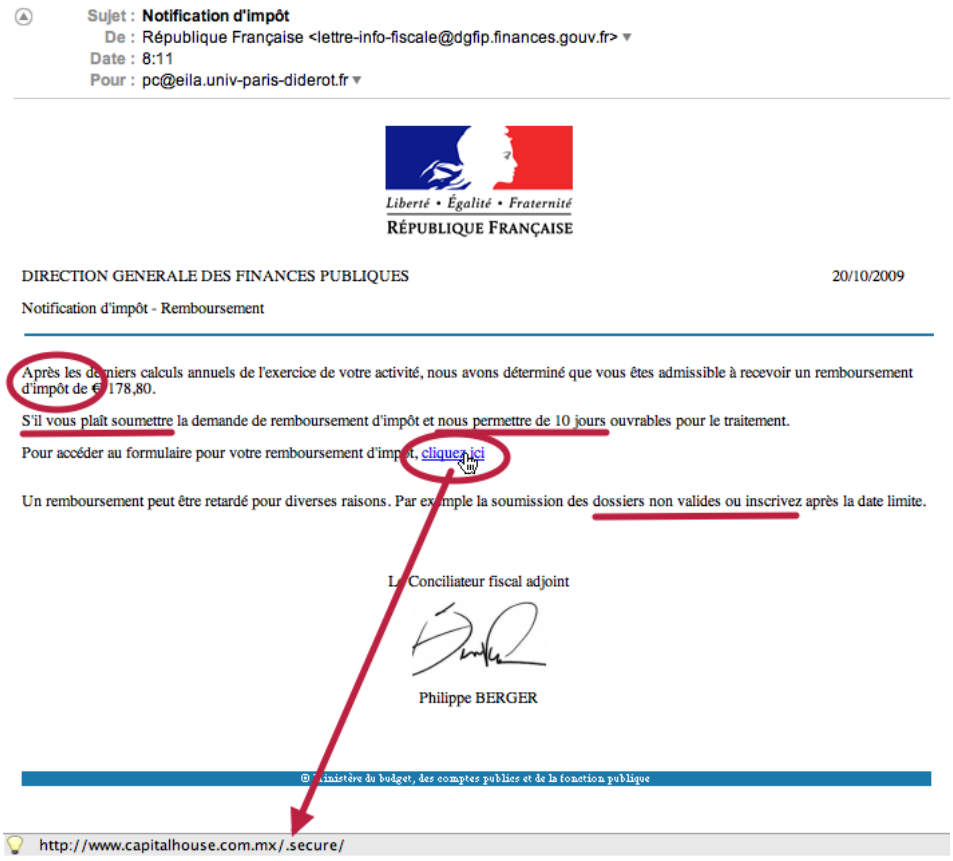
L'hameçonnage est une méthode qui avec le temps ne fait que se peaufiner, les acteurs de la menace phishing innovent sans relâche. Des technologies tels que les passerelles de messagerie sécurisées (SEG Secure Email Gateway en anglais) laissent passer une grande partie des mails phishing.

Les messageries ayant une volonté de ressembler de plus en plus aux réseaux sociaux et en même temps étant très utilisé dans le milieu de l'entreprise je risque de traitait ce sujet dans les deux parties du guide.

Exemple typique sur Twitter de phishing, ici nous voyons un message qui apparait anodin mais qui est en réalité corrompu car le lien qui est noté dans le message ramène sur un site piégé de virus,vers,Trojan etc...



Autre exemple avec un mail, pareil avec une URL piéger cela-dit ceux genres de mail aura plus tendance à vous amener sur une page falsifiée du gouvernement pour vous inciter à donner vos coordonnés bancaires.



Pour se protéger je conseille de faire preuve de logique, car comme dans l'exemple du haut il faut savoir, que le gouvernement ne vous enverra jamais de mail en rapport avec un gain ou perte d'argent à régler.

L'utilisation de logiciels comme Kapersky VirusDesk pour faire vérifier les URL peut être aussi un plus mais n'oubliez pas de le vérifier quand même en laissant votre souris sur le lien MAIS SANS CLIQUER.

Nous avons aussi un danger très sous-estimé et très dangereux des réseaux sociaux, les fuites de données.

La raison d'être des réseaux sociaux est le partage cependant dans une entreprise ou dans la fonction publique (agents de la défense) il vaut mieux garder le silence.

Voici une liste des choses à ne pas partager :

-les produits

-les projets

-les finances

-les changements organisationnels

-les scandales

-des photos de lieux interdits

Avertissez aussi vos proches de ne pas partager ces choses si vous les avez informés.

N'oubliez pas que certaines personnes sont prêtes à tout.

Exemple : en mars 2012, Mohammed Merah abat trois militaires à Toulouse et Montauban, et en blesse un autre grièvement. Ces quatre personnes ont été ciblées du fait de leur statut de militaire.

Les types d'application FacebookLive, Periscope, Snaptchat, etc sont à proscrire car :

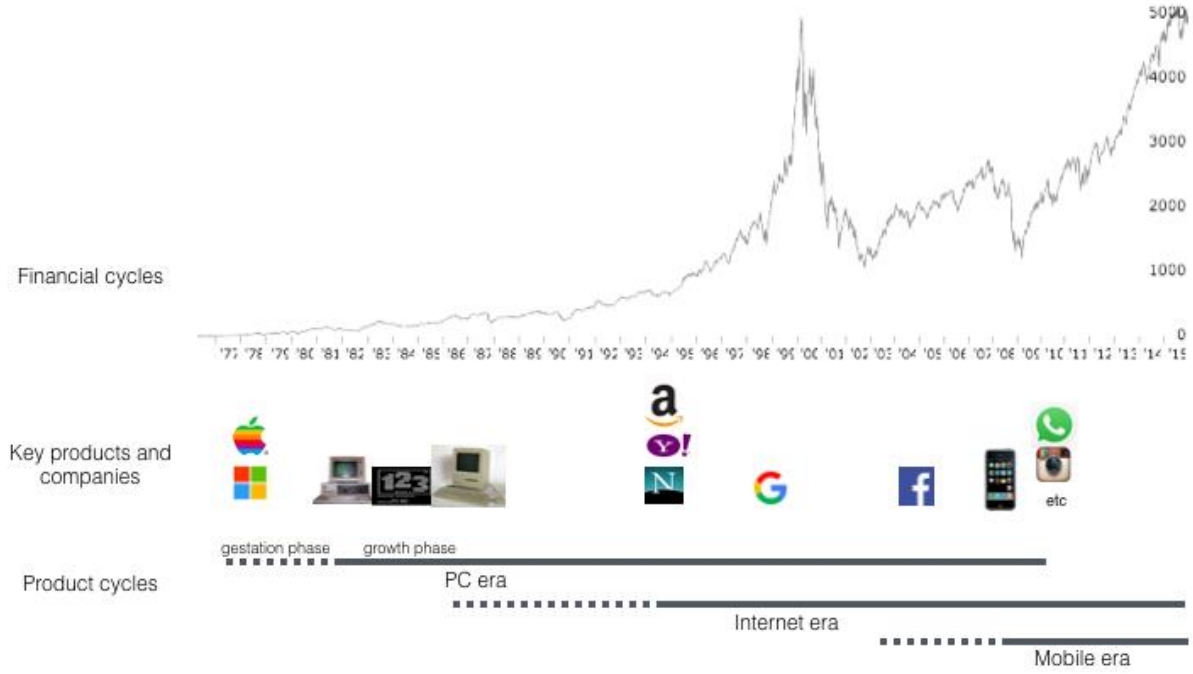
+----------+------+

Partie mobilité :

Les entreprises sont de nos jours en conversion vers le numérique et les nouvelles technologies sans se douter des inconvénients que vont leur procurer ses nouveaux outils (tablette, drone, cloud serveur, etc).

C'est pourquoi ce guide vous sera d'une grande aide mais seulement pour un temps car les technologies sont en constante évolution.

Dans cette partie je commencerai par parler des nouvelles technologies pour finir par ces dangers.



Comme vous pouvez le voir dans l'image ci-dessus nous entrons dans l'ère mobile, le cycle des produits stagne par rapport au cycle financiers.

Il faut comprendre qu'après le physique vient le software ; et le software rapporte beaucoup.

Le PC a permis aux entrepreneurs de créer des traitements de texte, des tableurs et de nombreuses autres applications de bureau. Les moteurs de recherche, le commerce électronique, le courrier électronique et la messagerie, les réseaux sociaux, les applications commerciales SaaS et de

nombreux autres services activés sur Internet. Les smartphones permettent la messagerie mobile, le réseautage social mobile et des services à la demande tels que le covoiturage.

Aujourd'hui, nous sommes au milieu de l'ère mobile et qui dit mobile dit mobilité.

Le cloud : Qui pourrait mieux représenter la mobilité que les nuages ? Le cloud fait partie intégrante de cette nouvelle ère.

Qu'est-ce que le cloud ? C'est une nouvelle façon de stocker vos données (photo,document pdf, logiciel,etc) et sa démocratisation devient de plus en plus présente dans diverses domaines : Jeux vidéo, service entreprise, réduire les coûts de stockage, etc…

Ce petit schéma expliquera une petite partie de ce que peut faire le cloud :

Les avantages principaux :

-moins cher que le stockage physique

-pas besoins de ressources humaines qualifiaient pour gérer les serveurs (pour une entreprise)

-disponibilité garantie par le data center qui contient vos données et maintenance

-plus rapide, fiable et évolutif (variable en fonction du prestataire choisie pareil pour le particulier)

Inconvénient

-fonctionnement par rente

-perte de savoir-faire pour l'entreprise

-la fiabilité du prestataire est variable comme la sécurité de vos données

Certains hébergeurs sont déjà très bien avancés sur ce marché qui ne fait que grandir et propose des services uniques :

OVHCLOUD (on vous héberge cloud) et son IPMI (Intelligent Platform Management Interface) qui permet au client de modifier des paramètres importants notamment avec l'administration du BIOS à distance facilement.

AWS (Amazon web service) avec son kit de développement logiciel AWS Mobile permettant à votre application d'accéder directement à AWS tel que DynamoDB, S3 et Lambda et le kit de développement mobile prend en charge beaucoup IOS.

Bien-sûr les promesses du Cloud sont irrésistibles. Pour montant dérisoire, les clients peuvent monter un serveur. Les sauvegardes s'effectuent en un clic. Plus besoin de se préoccuper d'acheter du matériel ou de maintenir la salle serveurs à la bonne température. Il suffit de se connecter et tout fonctionne.

Cependant, ces gains de praticité se traduisent par une perte de contrôle.

Voici ce qui peut se cacher derrière le voile :

-Les mêmes failles de sécurité s'y retrouvent voir **annexe 1**

-Vous n'avez pas de réelle certitude sur ce que vous obtenez

Pour démarrer une machine dans le Cloud, il vous suffit de cliquer sur un bouton, en choisissant par exemple Ubuntu 18.04 ou FreeBSD. Mais comment être certain qu'il s'agit de la distribution standard ? **un ancien salarié d'un datacenter partagé a raconté que son employeur insérait des comptes secrets dans ses distributions, et modifiait ensuite les routines standard de surveillance des processus d'UNIX, afin de masquer ses activités.**

La confiance envers votre fournisseur de Cloud doit être une évidence. Il faut être absolument convaincu de son incorruptibilité ; malheureusement c'est une tâche très compliquée.

-**Le Cloud ajoute une couche supplémentaire qui échappe à votre contrôle**, les instances Cloud sont généralement fournies avec une couche logicielle supplémentaire sous le système d'exploitation, et celle-ci est complètement hors de votre contrôle, très peu documenter elle pourrait servir à subtiliser, corrompre ou modifier vos données, au moment où celle-ci y transitent.

-**les employés ne travaillent pas pour vous et non pas de compte à rendre et leur avenir n'a pas grand-chose à voir avec vos résultats**

-**Les économies d'échelle ont un effet de bord**

L'un des côtés positifs du Cloud est qu'il s'agit d'un marché de masse. Cela permet d'offrir des tarifs bon marché, car les fournisseurs ont des armoires et des armoires de matériel. Cela permet de maintenir les prix bas, mais cela conduit également à une monoculture, qui facilite la tâche des attaquants. Trouver une faille dans une instance peut ainsi ouvrir l'accès à des milliards d'entre elles **et le risque 0 n'existe pas.**

COMMENT SE PROTEGER ?

Il est compliqué de pouvoir se protéger quand on fait de l'infogérance et il est compliqué pour les entreprises d'attirer de nouveaux clients s'ils n'ont pas confiance.

C'est pour cela qu'est apparu : le Saas,Iaas et le Paas.

Saas(software as a service) = on met à disposition tout(matériels, systèmes d'exploitation, interpréteur) excepté l'application car c'est la vôtre.

Paas(Platform as a service) = choix des services, systèmes d'exploitation en gros tous les choix au niveau de la virtualisation

Iaas(infrastructure as a service)= on monte le cloud de A à Z (sauf câble)

Les Iot

Iot : une étude récente (2020) réalisée aux Etats-Unis par des entités du groupe Palo Alto Networks a montré combien l'IoT est un un nid de failles de sécurité.

L'étude a été réalisée dans deux secteurs gros utilisateurs d'Iot et aux Etats-Unis : la santé et la location de biens.

Rappellons que la plupart des appareils d'imagerie médicale sont des objets connectés et que bon nombre de bien loués sont équipés de traceurs GPS.

L'étude rappelle un chiffre du Cabinet Gartner(*entreprise américaine de conseil et de recherche dans le domaine des techniques avancées, chiffres d'affaires 2,4 milliard et 13000 salarier en 2017*) :

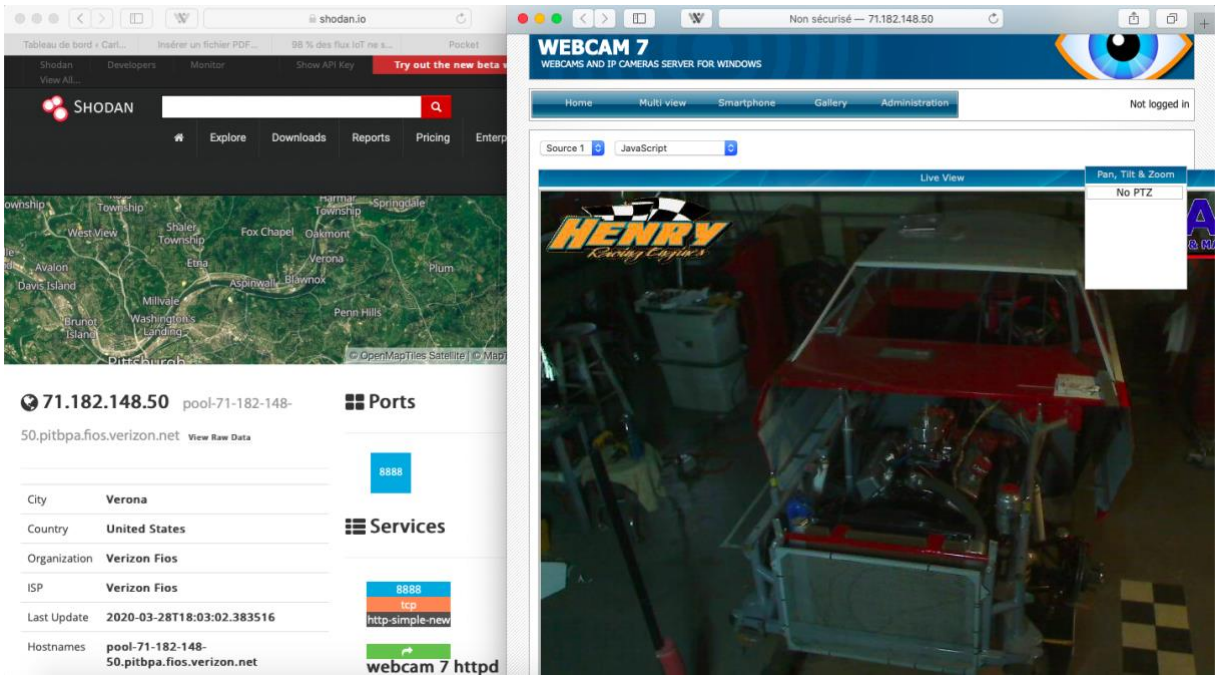
- Il y a 4,8 milliards d'appareils connectés, en progression de 21,5% entre 2018 et 2019.
- Les Iot sont riches en données personnelles
- 98% des flux des Iot ne sont pas chiffrés
- Les logiciels des Iot sont rarement mis à jour, les rendant vulnérable sur des failles bien documentées.
- Changement rare des mots de passe d'administration par défauts.

57% des objets connectés sont concernés par ces attaques de gravité moyenne à élevée.

Dans l'imagerie médicale, 83% des appareils utilisent des environnements qui ne sont plus maintenus (comme des anciennes versions de Windows), créant des failles qui sont par ailleurs comblées dans le SI depuis longtemps.

Des chiffres qui font peur mais pour mieux les visualisés voici une image du site web shodan.io qui exploite le nom changement des mots de passe d'administration par défauts.

Voici l'image d'un garage au états-unis qui n'a pas sécurisé sa caméra.



Voyez comme il est simple d'obtenir des informations sur une entreprise via les Iot.

COMMENT SE PROTEGER ?

- Modifier le mot de passe administrateur
- Regarder si le fabricant fait des mises à jour et si le matériel utilisé dans l'Iot est fiable et sécurisé.
- Éteindre le matériel si possible (sauf si caméra)
- Regarder si l'appareil possède un système de localisation pour le désactiver si possible.

Quand on parle d'Iot , on parle aussi de connectivité.

Nous pouvons affirmer que les Iot (Internet des objets) ont besoin de beaucoup de cette connectivité, c'est pour cela que nous devons faire attention aux nouvelles technologies telles que :

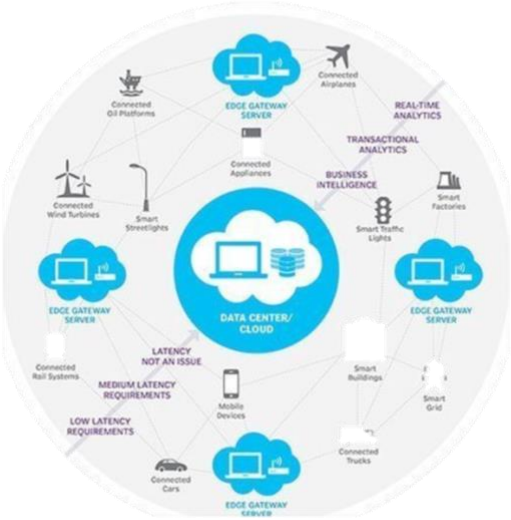
-Wifi 6 ou 802.11ax

-5G

-Edge Computing

D'ailleurs parlons de **l'edge computing**, commençons par une définition simple et compréhensible par tous. "Edge computing" est tout d'abord lié à l'Internet des objets.

L’argument est le suivant : dans certaines conditions d’application, il faut minimiser la latence (c’est-à-dire le temps de transfert réseau et donc, le temps de réponse global) pour garder de bonnes performances. Dans ce cadre, il serait plus logique de traiter localement les données recueillies par les capteurs plutôt que de les expédier directement dans le Cloud. En général, on estime qu’il faut entre 150 et 200 millisecondes pour transmettre les données d’un dispositif IOT à un fournisseur de services cloud et inversement. Alors qu’avec des serveurs déployés à proximité de ces dispositifs (*On the edge* -sur le bord- donc…), ce délai pourrait être de l’ordre de deux à cinq millisecondes. Un gain très intéressant (presque cent fois mieux !) si la performance est un facteur critique. L’edge computing est aussi appelé “mesh computing” (informatique en réseau maillé), “peer-to-peer”, “informatique autonome”, “grid computing”, et par d’autres noms (*fog computing, dew computing*, etc.) qui impliquent tous la gestion informatique décentralisée par opposition au cloud computing qui lui représente le nouveau paradigme de l’informatique centralisée.



Les Iot se multiplient de plus en plus : montre, balance, maison connectée, etc.

Dans quelques années 45% de toutes les données générées par les dispositifs IoT seront stockées, traitées, analysées et utilisées à proximité ou en périphérie du réseau ; d’où l’utilité de l’edge computing.

Avec la décentralisation de l'informatique, les technologies de réseau optimisées pour les flux de trafic croisés et/ou les communications en réseau mesh deviendront de plus en plus importants.

Wifi et hotspot :

Le développement des objets communicants et leur usage quotidien sont aujourd'hui à l'origine de l'omniprésence des réseaux sans-fil Wi-Fi, tant chez les particuliers que dans le monde professionnel.

Les réseaux wifi sont cependant très vulnérables et utilisables par bon nombres de personnes malveillantes qui veulent profiter des failles de la Wifi pour intercepter des données sensibles (informations personnelles, codes de cartes de paiement, données entreprise, etc.)

Par marque de robustesse, les mécanismes cryptographiques intrinsèques aux réseaux Wi-Fi n'apportent parfois qu'une fausse impression de sécurité. Fin 2012, les principaux profils de sécurité sont par ordre d'apparition :

- Le WEP, dont la clé(mot de passe d'accès) est cassable en moins d'une minute
- Le WPA, de robustesse variable en fonction du paramétrage utilisé ;
- Le WPA2, particulièrement robuste ;
- WPS(WPA+aes(méthode de chiffrage)) simplifie l'authentification d'un terminal sur un réseau WPA2 (par code PIN par exemple) mais ré-introduit une vulnérabilité importante qui en réduit fortement le niveau de sécurité
- WPA3 : protection maximale

Néanmoins même en WPA3 on peut intercepter vos données à caractère sensible, cela favorise les attaques du « man of the middle », l'homme du milieu c'est un individu qui va s'immiscer dans une conversation entre deux terminaux pour essayer de falsifier les informations, ou se faire un passer pour un des deux, ou voler les informations.

COMMENT SE PROTEGER :

- Tunnel VPN(ou RPV) : c'est une connexion sécurisé et chiffré créé par un logiciel VPN qui permet d'obtenir une adresse IP anonyme pour voyager sur le web de manière transparente. Différentes versions d'un VPN existent comme IPsec ou SSL.
- Utiliser des clefs privée et publics pour ces communications.
- Aller seulement sur les sites https(TLS/SSL).

Revenons à la Wi-Fi, La technologie Wi-Fi repose sur un lien radio dont les ondes sont par nature sujettes à l'intercep- tion et aux interférences (brouillage des ondes accidentel ou intentionnel). En l'absence de moyens de protection complémentaires conformes à la réglementation, il convient alors de ne pas utiliser de lien Wi-Fi pour faire transiter des données sensibles ou critiques comme, par exemple :

- Des informations classifiées de défense. Leur protection en confidentialité doit impérativement être assurée par des équipements agréés par l'ANSSI
- Des informations sensibles à caractère confidentiel ;
- Des informations non confidentielles mais dont la disponibilité et l'intégrité sont critiques pour des infrastructures industrielles ou d'importance vitale.

Quand on parle de mobilité on parle aussi de voyage c'est pourquoi j'ai créé un guide basé sur l'ANSSI sur les bonnes pratiques.

Guide sur le voyage

Paru en janvier 2013 dans sa première version, le Guide d'hygiène informatique édité par l'ANSSI s'adresse aux entités publiques ou privées dotées d'une direction des systèmes d'information (DSI) ou de professionnels dont la mission est de veiller à leur sécurité. Il est né du constat que si les mesures qui y sont édictées avaient été appliquées par les entités concernées, la majeure partie des attaques informatiques ayant requis une intervention de l'agence aurait pu être évitée.

ANSSI (Agence nationale de la sécurité des systèmes d'information) est un service français à compétence nationale, l'ANSSI a pour mission de protéger les systèmes d'information de l'état mais elle est aussi chargée d'une mission de conseil et de soutien aux administrations et aux opérateurs d'importance vitale.

Commencez par établir un état des lieux pour chacune règle, déterminez si votre organisme atteint le niveau standard et, le cas échéant, le niveau renforcé.

Si vous ne pouvez pas faire cet état des lieux par manque de connaissance de votre système d'information, n'hésitez pas à solliciter l'aide d'un spécialiste pour procéder à un diagnostic et assurer un niveau de sécurité élémentaire.

À partir du constat établi à cette première étape, visez en priorité les règles pour lesquelles vous n'avez pas encore atteint le niveau « standard », pour définir un premier plan d'actions.

Lorsque vous avez atteint partout le niveau « standard », vous pouvez définir un nouveau plan d'actions en visant le niveau « renforcé » pour les règles concernées.

Les équipes opérationnelles, pour être à l'état de l'art de la sécurité des systèmes d'information, doivent suivre - à leur prise de poste puis à intervalles réguliers - des formations sur :

> la législation en vigueur ;
> les principaux risques et menaces ;
> le maintien en condition de sécurité ;
> l'authentification et le contrôle d'accès ;
> le paramétrage fin et le durcissement des systèmes ; > le cloisonnement réseau ;
> et la journalisation.

Attitude générale

Entant qu'utilisateur vous devez suivre un certain nombre de règles en matière de sécurité pour la pérennité de votre travail :

L'un des boulots entant qu'utilisateur est de signaler et les informations sensibles, en indiquant sur quelle poste ils sont ou en les envoyant sur le serveur mais aussi rester en alerte sur l'activation du firewall et de l'antivirus.

Il faudra aussi que vous indiquiez votre heure d'arrivée et de départ et ne pas utiliser le matériel qui n'est pas attribué à votre fonction.

Les droits de l'administrateur réseau ne sont certainement pas les mêmes que les votre c'est pour cela qu'il ne faut pas toucher au ordinateur de vos collègues.

Vos équipements mobiles personnelle devront être déclarer à l'informaticien et laissé pour une inspection si votre organisme tolère de le BYOD.

Vous ne devrez-vous connecté sur le réseau que si votre matériel est sûr d'utilisation. BYOD=bring your own devices

Règle

Suivre les critères rigoureusement de dimensionnement pour les mots de passe exigé par INSSI. Désactiver votre session avant de partir même pour aller manger !!!

Protéger les mots de passe stockés sur les systèmes non pas sur des support physique telle que des mémos ou encore post-it ni des supports numériques telle que des fichiers de mots de passe, envoi par mail à sois même, recours aux boutons « se souvenir du mot de passe ».

Vous serez limitée avec les applications installées et modules optionnels des navigateurs web aux seuls nécessaires

Le pare-feu local et un anti-virus (ceux-ci sont parfois inclus dans le système d'exploitation) ne devra jamais être désactivé.

Règle sur le matériel nomade et sans-fil

Tout périphérique externe devra être montré à un membre de la sécurité informatique.

Il ne faudra pas se connecter à des réseau public ou inconnu et désactiver les interfaces sans-fil(Bluetooth et WiFi)

Entant qu'utilisateur quand vous recevez un message sur votre boite mail il est de votre devoir de vous demander si l'expéditeur est-il connu ? Une information de sa part est-elle attendue ? Le lien proposé est-il cohérent avec le sujet évoqué ? En cas de doute, une vérification de l'authenticité du message par un autre canal (téléphone, SMS, etc.) est nécessaire.

Les terminaux nomades (ordinateurs portables, tablettes, ordiphones) sont, par nature, exposés à la perte et au vol. Ils peuvent contenir localement des informations sensibles pour l'entité et constituer un point d'entrée vers de plus amples ressources du système d'information. Au-delà de l'application au minimum des politiques de sécurité de l'entité, des mesures spécifiques de sécurisation de ces équipements sont donc à prévoir.

Sachez que les cybercafés, les hôtels, les lieux publics et les bureaux de passage n'offrent aucune garantie de confidentialité. Dans de nombreux pays étrangers, quel que soit leur régime politique, les centres d'affaires et les réseaux téléphoniques sont surveillés. Dans certains pays, les chambres d'hôtel peuvent être fouillées sans que vous vous en rendiez compte.

Règle en mission

Utilisez de préférence du matériel dédié aux missions (ordinateurs, ordiphones, supports amovibles tels que les disques durs et clés USB) Ces appareils ne doivent contenir aucune information 3 autre que celles dont vous avez besoin pour la mission.

Sauvegardez les données que vous emportez et laissez la sauvegarde en lieu sûr. Vous récupérerez ainsi vos informations à votre retour en cas de perte, de vol ou de saisie de vos équipements.

Évitez de partir avec des données sensibles.

Utilisez un filtre de protection écran pour votre ordinateur. Cela vous permettra de travailler à vos dossiers pendant vos trajets sans que des curieux puissent lire ou photographier vos documents par-dessus votre épaule.

Marquez vos appareils d'un signe distinctif (comme une pastille de couleur). Cela vous permet de surveiller votre matériel et de vous assurer qu'il n'y a pas eu d'échange, notamment pendant le transport. Pensez à mettre un signe également sur la housse.

Gardez vos appareils, support et fichiers avec vous. Prenez-les en cabine lors de votre voyage. Ne les laissez jamais dans un bureau ou dans la chambre d'hôtel (même dans un coffre).

Utilisez un logiciel de chiffrement pendant le voyage (fournir par un membre de la sécurité informatique de votre organisme). Ne communiquez pas d'information confidentielle en clair par téléphone ou tout autre moyen de transmission de la voix (services de VoIP comme Skype !!!).

Pensez à effacer l'historique de vos appels et de vos navigations

En cas d'inspection ou de saisie par les autorités, informez immédiatement votre organisme.

N'utilisez pas les équipements qui vous sont offerts (clés USB). Ils peuvent contenir des logiciels malveillants.

Désactiver la géolocalisation.

Ne connectez pas vos équipements à des postes ou des périphériques informatiques qui ne sont pas de confiance.

Ne rechargez pas vos équipements sur les bornes électriques libre-service. Certaines de ces bornes peuvent avoir été conçues pour copier les documents à votre insu.

Dernière règle très important ne faite confiance à personne amis, collègue ou autre.
Vos données sensibles sont la priorité (bien-entendus votre vie et celle des autres reste la priorité).

Avant mission

Transférez vos données > sur le réseau de votre organisme à l'aide de votre connexion sécurisée ; > sinon sur une boîte de messagerie en ligne dédiée à recevoir vos fichiers chiffrés (qui seront supprimés dès votre retour).

Puis effacez-les ensuite de votre machine, si possible de façon sécurisée, avec un logiciel prévu à cet effet.

Effacez l'historique de vos appels et de vos navigations Cela concerne aussi bien vos appareils nomades (tablette, téléphone) que votre ordinateur.

Après mission

Changez tous les mots de passe que vous avez utilisés pendant votre voyage. Ils peuvent avoir été interceptés à votre insu

Analysez ou faites analyser vos équipements. Ne connectez pas les appareils à votre réseau avant d'avoir fait ou fait faire au minimum un test anti-virus et anti-espiogiciels.

Annexe 1 :

En 2016 un communiqué de presse se transforme en piège dû à un mauvais choix de partenaire urlmin.com

Communiqué de presse

PRÉFET DE LA RÉGION LANGUEDOC-ROUSSILLON-MIDI-PYRÉNÉES

Toulouse, le 9 septembre 2016

33es Journées européennes du patrimoine
17 et 18 septembre 2016

Patrimoine et citoyenneté

Le thème de cette 33e édition des Journées européennes du patrimoine est consacré aux lieux d'expression de la citoyenneté. Un thème qui nous unit et nous rassemble tous, autour de la République.

Il permettra la découverte ou la redécouverte de lieux symboliques de la naissance de la citoyenneté, de leur historiques de sa constitution et de lieux actuels de pratique et d'exercice quotidiens.

Les 17 et 18 septembre, plus de 1 300 lieux et monuments de notre nouvelle région Languedoc-Roussillon-Midi-Pyrénées accueilleront le public, dont près d'une centaine pour la première fois. La thématique de la citoyenneté sera mise à l'honneur dans de nombreux sites. Un grand nombre d'animations sont proposées, dont la richesse et la diversité permettront au public de découvrir ou redécouvrir les trésors du patrimoine régional ainsi que celles et ceux qui l'étudient, le conservent et le font vivre.

Pour que chacun puisse organiser plus aisément ses *Journées du patrimoine*, la direction régionale des affaires culturelles a élaboré un **guide régional numérique.**

Cette publication, de plus de 140 pages, offre une grande place aux descriptifs des monuments, aux animations qui y sont proposées ainsi qu'aux illustrations. Chaque visiteur a la possibilité, grâce à une large gamme d'outils de recherche et de personnalisation, de préparer plus aisément ses visites.

Contacts Presse

Direction régionale des affaires culturelles (Drac)
Tony Simone
☎ 05 67 73 20 36

Préfecture
Sophie Lesaffre
☎ 05 35 16 38 31
☎ 05 34 45 38 31

Virginie Avizou
☎ 06 85 80 22 14
☎ 05 34 45 38 17

1, place Saint-Étienne
31038 Toulouse Cedex 9
☎ 05 34 45 34 45

Vous pouvez consulter les précédents communiqués de presse à l'adresse suivante :
www.languedoc-roussillon-midi-pyrenees.gouv.fr/communiques

Le guide régional numérique est disponible à l'adresse suivante
http://urlmin.com/jep2016
et sur le site de la Drac
www.culturecommunication.gouv.fr/Regions/Drac-Languedoc-Roussillon-Midi-Pyrenees

Le programme national est consultable sur le site
www.journeesdupatrimoine.culturecommunication.gouv.fr

twitter.com/PrefetLRMP www.languedoc-roussillon-midi-pyrenees.gouv.fr page 1/1

Dans un premier temps, l'agence de communication a préparé, à l'occasion des journées européennes du patrimoine, une plaquette d'informations. Un document lié aux 1300 lieux et monument du Languedoc-Roussillon-Midi-Pyrénées.

Dans un second temps, le programme au format PDF est installé sur la toile. L'adresse électronique (l'URL) est longue, loin d'être pratique pour être communiquée à la presse, aux partenaires…

[*https://asp.zone-secure.net/v2/index.jsp?id=4463/5806/65573&lng=fr%20*]

Il est donc décidé l'utilisation d'un raccourcisseur d'url. C'est le site ulmin.com qui sera choisi, un peu au hasard.

Le site hébergé en Espagne, par OVH c'est fait piraté depuis une dizaine de jours…, tout ceci permettra au hacker de modifier les URL pour faire du phishing en amenant les gens cliquant sur le lien vers des sites douteux.

Tout ça pour dire que les serveurs et cloud sont de plus en plus nombreux à stocker des solutions logiciels est que même chez des professionnel les failles existe toujours