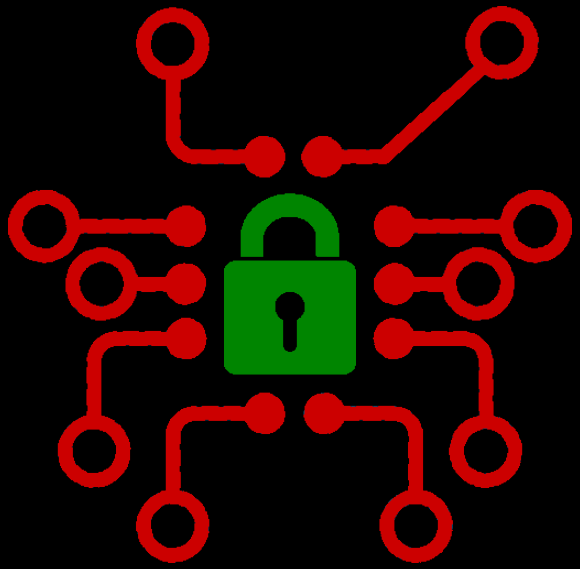
Introduction à la Cybersécurité



Notions de base et règles d'hygiène

François-Xavier Aranda

Plan de la session 301

- Échange sur la sécurité de l'information
- Objectifs du cours
- Enjeux et propriétés de la sécurité
- Panorama des menaces
- Le droit et organisation de la sécurité
- Maîtriser le réseau et sécuriser les terminaux
- Gestion des utilisateur·rice·s
- Sécuriser physiquement, contrôler la sécurité du S.I

Plan de la session 301

- **Échange sur la sécurité de l'information**
- Objectifs du cours
- Enjeux et propriétés de la sécurité
- Panorama des menaces
- Le droit et organisation de la sécurité
- Maîtriser le réseau et sécuriser les terminaux
- Gestion des utilisateur·rice·s
- Sécuriser physiquement, contrôler la sécurité du S.I

Échange sur la sécurité de l'information

- Qu'est-ce qu'un système d'information ?
- Comment prendre en compte la sécurité dans une organisation ?
- Avez-vous déjà été victime d'une attaque informatique ?
- Connaissez-vous des événements récents où une attaque a été avérée ?
- Quels sont les risques principaux pour une organisation vis à vis de la sécurité de ses systèmes d'information ?
- Comment protéger les systèmes d'information des attaques informatiques ?
- Quel est le maillon faible de tous les systèmes d'information ?

Plan de la session 301

- Échange sur la sécurité de l'information
- **Objectifs du cours**
- Enjeux et propriétés de la sécurité
- Panorama des menaces
- Le droit et organisation de la sécurité
- Maîtriser le réseau et sécuriser les terminaux
- Gestion des utilisateur·rice·s
- Sécuriser physiquement, contrôler la sécurité du S.I

Objectifs du cours

- Connaître les notions de disponibilité, d'intégrité, de confidentialité, de preuves et de traçabilité
- Savoir partir des risques pour évaluer la sécurité d'un système d'information
- Savoir identifier les principales failles et vulnérabilités d'un système
- Connaître le rôle de l'ANSSI et le contexte juridique en France
- Comprendre les règles de bon usage des systèmes informatiques
- Les intégrer dans son utilisation personnelle et professionnelle de l'outil informatique
- Apprendre à sensibiliser les personnes aux enjeux de la cybsersécurité

Plan de la session 301

- Échange sur la sécurité de l'information
- Objectifs du cours
- **Enjeux et propriétés de la sécurité**
- Panorama des menaces
- Le droit et organisation de la sécurité
- Maîtriser le réseau et sécuriser les terminaux
- Gestion des utilisateur·rice·s
- Sécuriser physiquement, contrôler la sécurité du S.I

Enjeux et propriétés de la sécurité

- Un étude réalisée en 2018 par l'éditeur McAfee évalue à près de 600 milliards de dollars le coût de la cybercriminalité dans le monde.
- Par rapport à la dernière étude de 2014, il s'agit d'une augmentation de plus de 400 milliards de dollars
- Et il ne s'agit là que d'une étude du coût pour les entreprise qui ne prend pas en compte le coût pour le secteur publique et les particuliers
- Sans surprise, les pays industrialisés ou en voie d'industrialisation sont les plus touchés par ce phénomène
- D'après le rapport aucun ralentissement n'est à envisager pour le moment

Enjeux et propriétés de la sécurité

- Les impacts sur la vie privée des usagers et usagères d'internet et des systèmes d'information sont si nombreux qu'en faire une liste exhaustive n'aurait pas de sens ou peu d'intérêt
- Au delà de la divulgation d'informations sensibles comme par exemple les numéros de votre carte bleue, on s'intéresse aux risques encourus
- Parmi eux on peut citer l'usurpation d'identité, le vol de biens, d'argent ou de données, la diffamation pour atteindre la réputation, l'effacement de données
- Les menaces ne viennent pas nécessairement d'un ordinateur car un système d'information n'est pas seulement un système informatique

Enjeux et propriétés de la sécurité

- Quelques exemples d'attaques de ces dernières années
- MS17-010 : rançongiciel qui a exploité une vulnérabilité critique dans Windows menaçant l'effacement des données

- Prise de contrôle à distance d'une voiture connectée
  - Chris Miller et Chris Valasek (Black Hat 2015)

- Heartbleed en avril 2014 : fuite de données HTTP causé par un débordement de tampon dans OpenSSL

- Stuxnet : attaque sur l'usine d'enrichissement d'Uranium de l'Iran en 2010

Enjeux et propriétés de la sécurité

- Et ce ne sont là que des exemples avérés
- Très grande difficulté de connaître toutes les attaques car publiquement avouer s'être fait attaqué est mauvais pour la réputation
- Les enjeux de la cybersécurité sont donc autant de protéger les systèmes que de récupérer les informations nécessaires pour les préserver dans le temps
- Il y a encore de grandes réticences à fournir des informations critiques même dans le cadre d'audit de la part des entreprises.
- Cela vient d'une méconnaissance totale des métiers de la cybersécurité, l'enjeu est donc également de faire de la pédagogie

Enjeux et propriétés de la sécurité

- Données : informations manipulées et générées par un logiciel ou un·e utilisateur·rice.
- Information : interprétation significative d'une donnée informatique.
- Système d'information : tout système physique, matériel ou logiciel qui manipule des informations.
- Sûreté : moyens mise en œuvre pour assurer le fonctionnement ou l'intégrité des personnes ou du matériel.
- Sécurité : Ensemble des méthodes utilisées pour protéger les systèmes d'informations.

Enjeux et propriétés de la sécurité

- Objectifs de la sécurité : assurer les moyens de détection et de prévention des failles d'un système d'information et de leur exploitation malveillante.
- Les critères d'évaluation de la sécurité des systèmes d'information
- Confidentialité : L'information n'est pas divulguée en dehors de ses destinataires
- Intégrité : L'information n'est pas altérée par des utilisateur·rice·s ou logiciels non-authorisé·e·s
- Disponibilité : L'information est accessible aux utilisateur·rice·s ou logiciels
- Preuve/traçabilité : Par où elle est passé et par qui elle a été manipulé

Enjeux et propriétés de la sécurité

- On se sert principalement des critères CID (Confidentialité, Intégrité, Disponibilité) pour évaluer lé sécurité d'un système.
- Les critères de preuve et de traçabilité s'appliquent aux CID dans le cadre d'audit pour démontrer l'existence d'une faille ou l'efficacité d'une défense
- Les 3 critères CID n'ont pas la même pertinence en fonction des domaines
- Leur hiérarchie dépendra du domaines et des objectifs fixés par les normes :
  - CID : Bancaire, Médical ou Défense
  - IDC & ICD : Avionique, Internet des Objets ou Routage Réseau
  - DIC : Production Automatisée, Opérateur d'Importance Vitale ou Transport

Enjeux et propriétés de la sécurité

- Pour assurer la sécurité des systèmes d'information on se reposera sur certaines propriétés mathématiques ou physiques
- Cryptographie : domaine des mathématiques permettant d'assurer les fonctions principales de la sécurité des systèmes d'information.
- Quelques exemples d'outils utilisés pour assurer la sécurité :
  - Pare-feu : permettent de filtrer les communications réseaux
  - Badge d'identification : filtre physiquement l'accès à des zones
  - Identification par le couple identifiant/mot de passe
  - Algorithmes de chiffrement : assurent la confidentialité des données

Plan de la session 301

- Échange sur la sécurité de l'information
- Objectifs du cours
- Enjeux et propriétés de la sécurité
- **Panorama des menaces**
- Le droit et organisation de la sécurité
- Maîtriser le réseau et sécuriser les terminaux
- Gestion des utilisateur·rice·s
- Sécuriser physiquement, contrôler la sécurité du S.I

Panorama des menaces

- On définit plusieurs notions lorsqu'on parle de cybersécurité
- Faille : faiblesse de programmation, de spécification ou d'implémentation avec un impact CID sur un système ou d'une donnée informatique.
- Vulnérabilité : faille exploitable et identifiée sur un système d'information.
- Risque : effet de l'incertitude sur l'atteinte des objectifs (définition ISO).
- Menace : risque avéré par une vulnérabilité
- Attaque : scénario où une menace a été mise en œuvre par l'exploitation d'une vulnérabilité ayant eu ou pouvant avoir un impact sur les critères CID

Panorama des menaces

- Exemple de vulnérabilité lors de la conception d'une application web
- Les utilisateur·rice·s d'un site permettant de poster des messages à destination d'autres doivent s'authentifier sur le site pour avoir accès au service de messagerie
- Le site dispose d'une base de données des utilisateur·rice·s qui contient l'identifiant et les mots de passes pour vérifier leur authentification
- Si les mots de passes sont envoyés sans être chiffrés au service d'authentification, une personne malveillante peut les récupérer en écoutant les communications réseaux, on parle alors de faille

Panorama des menaces

- Exemple d'exploitation d'une faille
- Le site précédent a appris de ses erreurs et a chiffré les communications au moment de l'authentification des personnes
- Mais dans la base de donnée, les mots de passe sont stockés la forme de hash dont l'algorithme est connu pour avoir des collisions
- Une personne malveillante pourrait retrouver les mots de passe stockés sur la base en employant divers techniques de cryptanalyse comme une attaque en brute-force ou en exploitant les collisions connues

Panorama des menaces

- La principale source des menaces informatiques est ironiquement l'humain
- Difficulté de retenir des mots de passe compliqué
- Difficulté de retenir beaucoup de mot de passe
- Installation de logiciels vérolés
- Ouverture de pièce jointe sans vérification de la source etc.
- Mais il existe des faiblesses qui sont également liées à l'algorithmie et donc directement aux applications
- Recopie de contenu de tableau sans vérification de la taille
- Stockage de données dans des fichiers non protégés etc.

Panorama des menaces

- Hameçonnage (phishing) : méthode permettant d'inciter un·e utilisateur·rice·s à cliquer sur un lien malveillant en trompant sa vigilance
- Exemple d'hameçonnage : vous recevez un mail de la part de votre fournisseur d'adresse mail vous disant qu'il a détecté une activité suspecte et vous invite à cliquer sur un lien pour changer votre mot de passe
- Le lien est évidemment faux mais la page html affichée est identique à celle du fournisseur
- Une fois que vous avez rentré vos nouveaux (et anciens) identifiants votre compte est piraté...

Panorama des menaces

- Ingénierie sociale (Social Ingeneering) : méthode permettant de récupérer des informations sensibles sur une cible
- Exemple d'ingénierie sociale : vous êtes contacté sur votre réseau social préféré par quelqu'un prétendant connaître une de vos connaissance
- Cette personne discute avec vous et se faisant s'informe sur votre travail, où vous résidez, et quand sont vos prochaines vacances
- À votre retour de congé, votre appartement a été cambriolé par la personne malveillante qui a profité de votre absence et utilisé les informations que vous lui avez fourni

Panorama des menaces

- Intrusion informatique : technique permettant à une personne malveillante de s'introduire sur un système informatique pour en dérober ou détruire des informations ou prendre le contrôle d'un poste ou d'un serveur
- Exemple d'intrusion : votre anti-virus n'a pas été mis à jour depuis longtemps et vous voulez télécharger un logiciel de traitement de texte gratuit
- Le site de téléchargement à l'air légitime et est identique à celui de l'éditeur.
- Vous télécharger le logiciel et pendant quelques temps aucun problème
- Puis un beau jour vous vous rendez compte que votre compte a été vidé car un logiciel espion a récupéré vos identifiants de banque en ligne.

Panorama des menaces

- Virus et vers informatiques : exploitent les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction.
- Objectifs : utiliser des failles de logiciels pour se propager.
- Ces failles sont habituellement corrigées par les éditeurs de logiciel dès que les vers apparaissent.
- Il faut systématiquement mettre à jour les systèmes d'exploitations et logiciels si l'on souhaite réduire les risques d'infection

Panorama des menaces

- Dépassement de tampon (Buffer Overflow) : bug par lequel un processus, lors de l'écriture dans un tampon, écrit à l'extérieur de l'espace alloué au tampon, écrasant ainsi des informations nécessaires au processus.
- Lorsque le bug se produit non intentionnellement, le comportement de l'ordinateur devient imprévisible : blocage du programme, voire de tout le système.
- Le bug peut aussi être provoqué intentionnellement
  - technique couramment utilisée par les pirates.
  - détourner le programme bugué en lui faisant exécuter des instructions introduites dans le processus.

Panorama des menaces

- Dénis de service (Deny of Service) : Attaque qui vise à empêcher une ressource (machine ou réseau) de fonctionner convenablement en faisant tomber la machine ou en saturant ses ressources : la bande passante, la mémoire, tables de session…
- C'est une des techniques les plus utilisées sur internet car c'est une des plus facile à mettre en action
- Il existe des dizaines de variante de cette attaque dont la plus répandu est le dénis de service distribué (DDoS)

Plan de la session 301

- Échange sur la sécurité de l'information
- Objectifs du cours
- Enjeux et propriétés de la sécurité
- Panorama des menaces
- **Le droit et organisation de la sécurité**
- Maîtriser le réseau et sécuriser les terminaux
- Gestion des utilisateur·rice·s
- Sécuriser physiquement, contrôler la sécurité du S.I

Le droit et organisation de la sécurité

- Le Premier Ministre définit la politique et coordonne l'action de l'État en matière de sécurité et de défense des systèmes d'information
- L'Agence Nationale de la Sécurité des Système Informatique est rattachée au secrétaire général de la défense et de la sécurité nationale
- Elle est l'autorité nationale en matière de sécurité et de défense des systèmes d'information.
- Elle propose des guides synthétiques en droite ligne des exigences réglementaires et s’appuyant sur les méthodes et normes en vigueur.

Le droit et organisation de la sécurité

- D'un point de vue du droit, la cybersécurité n'est pas reconnu comme une branche spécifique ni même une discipline du droit de l'informatique
- La sécurité informatique : L'ANSSI crée par le décret n°2009-834
- Code de la défense : articles L1332-1 à 6
- Code des postes et communications électronique : article L 32-1
- Loi 78-17 de 1978 pour la sécurité des données personnelles
- Loi 2006-575 de 2004 pour la sécurité de l'économie numérique
- Ordonnance 2005-1516 pour la sécurité des échange électronique
- Loi 2013-1168 dite de programmation militaire pour les opérateurs critiques

Le droit et organisation de la sécurité

- La Cybercriminalité dans le droit
- Code pénal
  - articles 226-16 et 17 pour les règles pour les données à caractère personnel
  - article 227-23 par rapport à la pédopornographie
  - articles 323-1 à 8 pour l'atteinte aux systèmes d'information
- Code monétaire et financier :
  - articles L 133-4 et L163-3 sur la falsification de moyen de paiement
- Code de la propriété intellectuelle :
  - article R 335-2 sur la protection des logiciels

Le droit et organisation de la sécurité

- En février 2011, l'ANSSI a rendu publique la Stratégie de la France en matière de défense et de sécurité des systèmes d'information.
- Pour se prémunir des attaques informatiques et garantir la sécurité des Français, des entreprises et de la Nation dans le cyberespace, la stratégie française pose quatre objectifs stratégiques :
  - être une puissance mondiale de cyberdéfense et appartenir au premier cercle des nations majeures dans ce domaine tout en conservant son autonomie
  - garantir la liberté de décision de la France par la protection de l'information de souveraineté ;
  - renforcer la cybersécurité des infrastructures vitales nationales ;
  - et assurer la sécurité dans le cyberespace.

Le droit et organisation de la sécurité

- Pour les entreprises on a différente réglementation en vigueur pour l'utilisation, fourniture et importation des moyens et prestations de cryptographie :
  - articles 29 à 40 de la loi pour la confiance en l'économie numérique no 2004-575 du 21 juin 2004 JORF no 143 du 22 juin 2004 page 11 168
  - décret no 2007-663 du 2 mai 2007, pris pour l'application des articles 30, 31 et 36 de la loi no 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie (JORF du 4 mai 2007) ;
  - arrêté du 25 mai 2007 définissant la forme et le contenu des dossiers de déclaration et de demande d'autorisation d'opérations relatives aux moyens et aux prestations de cryptologie (NOR : PRMD0753669A, JORF du 3 juin 2007).

Plan de la session 301

- Échange sur la sécurité de l'information
- Objectifs du cours
- Enjeux et propriétés de la sécurité
- Panorama des menaces
- Le droit et organisation de la sécurité
- **Maîtriser le réseau et sécuriser les terminaux**
- Gestion des utilisateur·rice·s
- Sécuriser physiquement, contrôler la sécurité du S.I

Maîtriser le réseau et sécuriser les terminaux

- Avant de mettre en place la sécurité dans une organisation, il faut connaître les appareils et entités qui constituent son système d'information
- En général, toute les entreprises sont sensées disposer de cet inventaire
- Il peut cependant arriver qu'il ne soit pas à jour pour plusieurs raisons
- Réaliser cet inventaire est essentiel pour pouvoir évaluer les points sensibles de l'infrastructure du système d'information et l'améliorer
- Il existe de nombreuse méthodes pour réaliser cet inventaire qui consistent à identifier les composants du SI par catégorie et de lister les connexions et interconnexions qu'ils peuvent utiliser

Maîtriser le réseau et sécuriser les terminaux

- Voici quelques exemples de catégories d'éléments d'un SI
- Éléments terminaux : poste de travail, serveurs, automates, imprimantes, lecteurs de toutes sortes, caméras de surveillance etc.
- Éléments réseaux : hub, switch, routeurs, passerelles, VPN, VLAN, câbles et liaisons radios, points d'accès Wifi, émetteurs infrarouge etc.
- Versions des logiciels : système d'exploitation, firmware des routeurs et automates, logiciels de bureautique, clients/serveurs et protocoles réseau etc.
- Compte d'utilisation et droits : utilisateur·rice·s, admin, dossiers partagés ...
- Éléments de sécurité : pare-feux, badgeuses, alarmes, anti-virus ...

Maîtriser le réseau et sécuriser les terminaux

- Pour sécuriser un réseau interne (intranet) on prendra soin de mettre en pratique le principe de défense en profondeur.
- Chaque entité du réseau sera placée en fonction de son niveau de criticité dans une couche du réseau : plus l'entité est critique, plus elle sera enfouie
- Exemple : le serveur du site web de l'entreprise est moins critique que celui permettant aux employé·e·s de saisir leur notes de frais
- On segmentera le réseau en plaçant les serveurs dans des zones démilitarisées (DMZ) entouré de pare-feux (à l'entrée et à la sortie)

Maîtriser le réseau et sécuriser les terminaux

- Les accès distants à un réseau d'entreprise ou à un réseau en production sont devenus nécessaires pour
  - Accéder à des document partagés en intranet
  - Effectuer des maintenances
  - Lire et envoyer des mails professionnels
- Ces accès sont potentiellement vecteurs d'attaques et doivent être limités selon le besoin réel qui on été identifiés au préalable
- On commencera donc par réaliser une étude des besoins des admins et des utilisateur·rice·s pour les confronter aux nécessités de la sécurité

Maîtriser le réseau et sécuriser les terminaux

- IPSec (Internet Protocol Security) est un protocole fournissant un mécanisme de sécurisation au niveau de la couche réseau (IP)
  - permet de chiffrer et/ou d'authentifier les échanges entre deux équipements (équipements actifs du réseau ou postes de travail)
- SSL/TLS (Secure Socket Layer/Transport Layer Security) sont des protocoles agissant au niveau transport de la couche réseau (TCP)
  - permet d'assurer l'authentification des terminaux, la confidentialité et l'intégrité des données échangées
- SSH (Secure SHell) : ensemble d'outils permettant des connexions sécurisées entre des machines
  - chiffre et compresse (sur demande) un tunnel de session qui sécurise les données transmises permettant d'accéder à distance à une ligne de commande

Maîtriser le réseau et sécuriser les terminaux

- Les réseaux véhiculés à l'aide d'onde radio (Wifi, bluetooth) sot extrêmement sensible car, si un câble peut être difficilement accessible, une onde radio se propage sans limite dans l'espace-temps
- La sécurisation des accès Wifi, notamment, est devenue essentielle après la démonstration de leur faiblesses
- Il est préconisé pour le Wifi d'utiliser le protocole WPA2 point à point qui est le plus résistant aux attaques.
- Un inventaire des points d'accès est évidemment essentiel et peut se réaliser grâce au repérage sur les alentours du lieux à sécuriser

Maîtriser le réseau et sécuriser les terminaux

- Les postes de travail est serveurs peuvent utiliser des versions obsolètes des applications et systèmes d'exploitation
- La mise à jour systématiques de ces terminaux est essentielle pour préserver les appareils de menaces potentielles
- Les machines dans un parc d'entreprise sont généralement connectées à un serveur de mise à jour qui vérifie en permanence l'état des versions
- Ce serveur installe les mises à jour des applications et systèmes d'exploitation aussi régulièrement que nécessaire
- Tout écart de version pour diverses raisons doit être documenté

Maîtriser le réseau et sécuriser les terminaux

- Protéger les machines contre du code malveillant permet d'offrir une barrière de protection supplémentaire en cas d'introduction d'un malware par support amovible, téléchargement internet ou par mail.
- Pour cela on utilise les antivirus sur les postes de travail et les serveurs de messagerie
- Ces applications analysent en permanence les fichiers et communication à la recherche de signature de code malveillant qui correspondent à celles stockées en base de données et lèvent des alertes le cas échéant
- Elles ont la capacité de placer des fichiers en quarantaine

Maîtriser le réseau et sécuriser les terminaux

- La protection des données personnelles passe généralement par leur chiffrement.
- Chiffrer des données revient à les rendre illisibles pour quiconque ne dispose pas de la clef de déchiffrement
- On utilise généralement des conteneurs chiffrés (VeraCrypt Zed)
- Les copies de sauvegardes permettent elles d'assurer la disponibilité des données et d'éviter qu'un effacement (volontaire ou non) ne mettent en péril les informations
- Enfin, on utiliser des algorithmes pour vérifier l'intégrité des données

Maîtriser le réseau et sécuriser les terminaux

- Le durcissement de la configuration permet d'éviter que des services inutilisés restent actifs sur les terminaux.
- Cela consiste à supprimer tous les logiciels et services superflus et à sécuriser ceux qui sont vraiment nécessaires
- L'avantage est de rendre la maintenance des postes et serveurs plus légère tout en évitant qu'un service actif oublié et donc obsolète se fasse corrompre et serve de vecteur d'attaque potentiel
- C'est une des méthodes les plus efficace pour la protection des terminaux mais c'est aussi l'une des moins utilisée compte tenu du travail et de la rigueur nécessaires.

Plan de la session 301

- Échange sur la sécurité de l'information
- Objectifs du cours
- Enjeux et propriétés de la sécurité
- Panorama des menaces
- Le droit et organisation de la sécurité
- Maîtriser le réseau et sécuriser les terminaux
- **Gestion des utilisateur·rice·s**
- Sécuriser physiquement, contrôler la sécurité du S.I

Gestion des utilisateur·rice·s

- L'humain est le premier responsable des problèmes de sécurité
- Nous sommes tou·te·s inconscient·e·s des risques de nos pratiques
- Sécuriser un système d'information passe donc par une restriction des privilèges accordés aux utilisateur·rice·s en fonction de leurs besoins
- Tous les systèmes d'exploitations proposent une gestion des privilèges basées sur la ségrégation des types de comptes (admin, user...)
- Mais la gestion des privilèges ne se limite pas à l'outil informatique
- Elle peut s'accompagner par une restriction des accès à des zones particulières (salle des serveurs, laboratoire, bureaux administratifs)

Gestion des utilisateur·rice·s

- Les privilèges informatiques sont de trois natures et s'appuient sur ce que peut ou ne peut pas faire un compte sur un fichier
- Lecture : le compte à le droit de lire le contenu d'un fichier
- Écriture : le compte peut modifier ou effacer un fichier
- Exécution : le compte peut exécuter le fichier c-à-d le faire interpréter par le processeur comme une série d'instruction
- On pourra mettre en pratique le principe de moindre privilège pour définir la politique des droits d'utilisation du SI

Gestion des utilisateur·rice·s

- Les mots de passe ou les phrases de passe (passphrases) sont un des moyens d'authentification privilégié par de nombreux SI
- Ils ont l'avantage de déporter la responsabilité sur l'utilisateur·rice·s pour la protection de ses données et de son poste de travail
- Ils doivent répondre à certains critères
  - Ils doivent être assez long pour ne pas être susceptibles d'être découverts
  - Ils doivent être composés de caractères mélangés (alphanumériques et spéciaux)
  - Ils ne doivent pas être des phrases ou mots connus
  - Ils doivent être régulièrement changés

Gestion des utilisateur·rice·s

- D'autres moyen d'authentification existent en complément des mots de passe
- Certificats et signatures : attribués à une personne ou entité, il permettent de l'authentifier grâce à des serveurs qui vérifient leur validité
- Ielles sont délivré·e·s par des autorités qui permettent d'assurer à un système d'authentification que la personne ou l'entité qui le présente est bien celle qu'elle prétend être
- On peut coupler ces méthodes avec d'autres méthodes d'authentification
  - Carte à puces, données biométriques, mot de passe etc.

Gestion des utilisateur·rice·s

- Toutes ses méthodes ne sont d'aucune utilité si les utilisateur·rice·s n'ont pas conscience de leur nécessité
- C'est pourquoi la mise en place de politiques de sécurité des systèmes d'information (PSSI) passe nécessairement par une sensibilisation
- On y développe les bonnes pratiques comme
  - Ne pas noter son mot de passe sur un post-it collé sur l'écran
  - Changer régulièrement ses mots de passe
  - Ne pas télécharger de pièces jointe venant d'une source inconnue
  - Ne pas brancher de support amovible sans en connaître la source

Plan de la session 301

- Échange sur la sécurité de l'information
- Objectifs du cours
- Enjeux et propriétés de la sécurité
- Panorama des menaces
- Le droit et organisation de la sécurité
- Maîtriser le réseau et sécuriser les terminaux
- Gestion des utilisateur·rice·s
- **Sécuriser physiquement, contrôler la sécurité du S.I**

Sécuriser physiquement, contrôler la sécurité du S.I

- Nous avons déjà commencé à aborder les aspects de sécurité physique par la limitation des accès aux zones sensibles
- Cette sécurité physique est souvent appelée "safety" dans la littérature anglophone ce que l'on traduit par sûreté
- Cela consiste notamment à assurer que les personnes et le matériel ne subissent pas de dommages physiques portant à leur intégrité
- C'est pourquoi, au delà des zones sensibles à cause des informations qu'elles contiennent, on limitera également l'accès aux zones dangereuses pour les personnes (armoire électrique, système de climatisation etc.)

Sécuriser physiquement, contrôler la sécurité du S.I

- L'impact des systèmes n'étant pas considérés comme composant le SI sur ce dernier est également pris en compte dans la sûreté
- En effet, ces systèmes ne sont pas directement connectés au réseau mais ont néanmoins un risque qui s'associe à celui du SI
- C'est notamment le cas
  - De la climatisation (pour les salles serveurs par exemple)
  - Des systèmes d'alertes incendies
  - Des systèmes électriques
  - Des canalisations

Sécuriser physiquement, contrôler la sécurité du S.I

- Pour l'ensemble des systèmes (SI et autre) une organisation devra assurer
- Leur maintenance au travers de contrats ou de services intégrés
- Leur assurance pour la gestion financière des risques
- Leur support en cas de panne ou de mauvaise configuration
- Ces contrats sont nécessaires mais pas suffisant.
- Ainsi les personnes habilitées à travailler avec différents systèmes devront également être sensibilisées aux aspects de sécurité physiques et informatiques qui y sont liés

Sécuriser physiquement, contrôler la sécurité du S.I

- La gestion des incidents et leur détection est une part importante du maintient en condition de fonctionnement et de sécurité
- Une fois qu'un système d"information a subi les conversions nécessaires à sa sécurisation, son maintient dépendra de la capacité de l'entreprise à
  - Détecter les problèmes
  - Répondre aux problèmes
- Comme pour les accès sur le site, on surveillera un SI grâce à des collecteurs d'événements et des analyseurs permettant de révéler des tentatives d'intrusions ou d'exploitation de failles

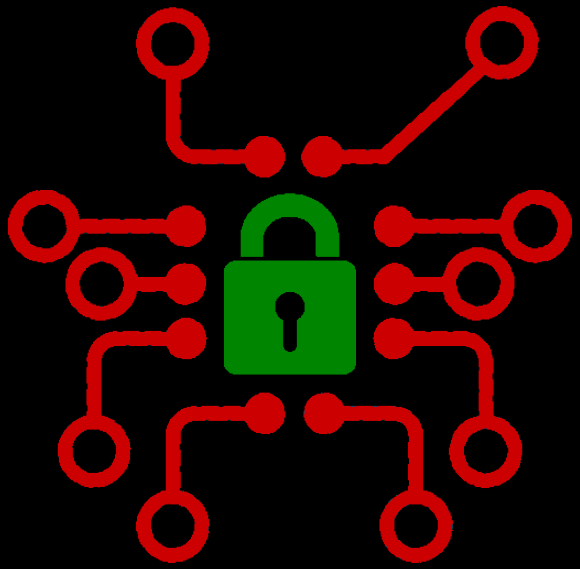
Sécuriser physiquement, contrôler la sécurité du S.I

- Les entreprises devront être munies d'un plan de secours en cas d'attaque
- Ce plan comprendra les différentes actions à mener pour restituer le système d'information et tirer le bilan des informations perdues
- Ce plan est nécessaire pour définir la politique de sauvegarde des données
- Il est généralement obligatoire dans tout contrat d'assurance
- Il peut être réalisé en faisant la part entre les risques potentiels qui ont un fort impact et une récurrence élevée de ceux n'ayant que peu de probabilité d'apparition et un faible impact.

Sécuriser physiquement, contrôler la sécurité du S.I

- L'audit de sécurité est un des outils permettant d'évaluer la qualité des moyens mis en place par l'entreprise pour assurer la sécurité de son SI
- Il se décompose en plusieurs étapes
  - Prise d'empreinte : évaluation de la surface d'attaque et des informations accessibles sur le net
  - Analyse de l'infrastructure : architecture réseau, configuration et conformité
  - Test applicatif : analyse de code, performance des solutions
  - Analyse de vulnérabilité : recherche des vulnérabilités connues
  - Tests d'intrusion : exploitation des vulnérabilité et test des vecteur d'attaques

Fin de la session 301



Notions de base et règles d'hygiène

François-Xavier Aranda