UNIVERSITÉ DE RENNES 1

La sécurité et vous

date de la formation :

09/01/2019

lieu de la formation : Rennes

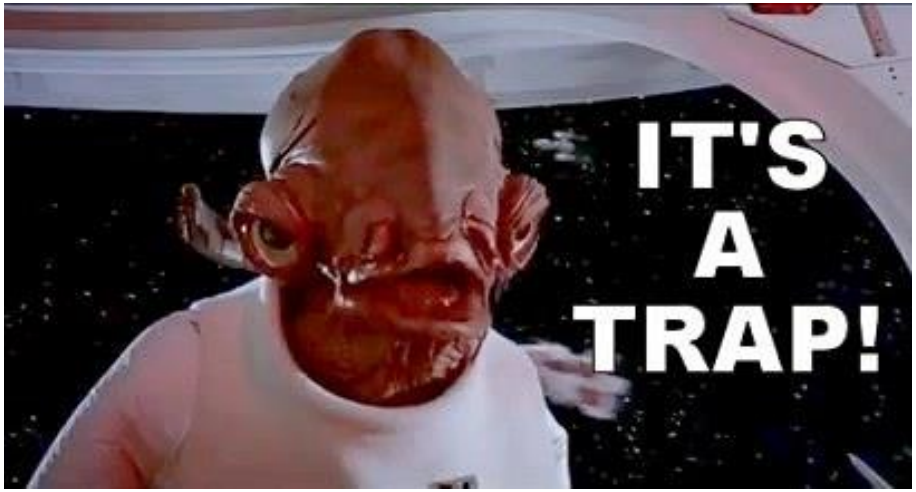
UNIVERSITÉ DE RENNES 1

La sécurité et vous

- Vous allez, au cours de votre vie professionnelle, développer, intégrer, mettre en œuvre, protéger une plateforme, infrastructure, service, application

La sécurité et vous

- Dans tous les cas, on va vous attaquer !



Sommaire

partie 1 : attaquants

partie 2 : traces

partie 3 : espionnage

partie 4 : éthique

partie 5 : habilitation

Sommaire

Taxonomie des attaquants

- L'ANSSI dresse six catégories d'attaquants :
  - Agresseurs
  - Fraudeurs
  - Employés malveillants
  - Militants
  - Espions
  - Terroristes

- Version ANSSI : http://circulaire.legifrance.gouv.fr/pdf/2009/05/cir_25550.pdf

Taxonomie des attaquants : agresseurs

- hacker ou passionné
  - individu **curieux**, qui cherche à se faire plaisir. Pirate par jeu ou par défi, il **ne nuit pas intentionnellement** et possède souvent un code d'honneur et de conduite. En général il n'a pas conscience de la mesure de ses actes. L'agresseur passionné est de moins en moins expérimenté.

- cracker ou casseur
  - plus **dangereux** que le hacker, **cherche à nuire** et montrer qu'il est le plus fort. Souvent mal dans sa peau et dans son environnement, il peut causer de nombreux dégâts en cherchant à se venger d'une société - ou d'individus - qui l'a rejeté ou qu'il déteste. Il veut prouver sa supériorité et fait partie de clubs où il peut échanger des informations avec ses semblables.

Taxonomie des attaquants : fraudeurs

- Le fraudeur bénéficie souvent d'une **complicité**, volontaire ou non, chez ses victimes,

- Il cherche à **gagner de l'argent** par tous les moyens. Son profil est proche de celui du malfaiteur traditionnel. Parfois lié au grand banditisme organisé ou non, il peut :
  - attaquer une banque,
  - falsifier des cartes de crédit,
  - se placer sur des réseaux de transferts de fonds et, si c'est un particulier, il peut vouloir falsifier sa facture d'électricité ou de téléphone.

Taxonomie des attaquants : employés

- Le fraudeur interne
  - possède de **bonnes compétences** sur le plan technique, il est souvent informaticien et sans antécédents judiciaires. Il peut penser que ses qualités ne sont pas reconnues, qu'il n'est pas apprécié à sa juste valeur.

- Il veut se venger de son employeur et chercher à lui nuire en lui faisant perdre de l'argent. Il peut répondre à un besoin matériel personnel qui induit des conduites de dépendances (jeux, sexe…). Pour parvenir à ses fins, il **possède les moyens**, qu'il connaît parfaitement, et qui ont été mis à sa disposition par son entreprise.

Taxonomie des attaquants : militants

- Motivés par une idéologie ou la religion,
  - ils disposent de compétences techniques très variables.
  - Leurs objectifs peuvent être limités à la diffusion massive de messages, comme ils peuvent s'étendre à des nuisances effectives sur les systèmes d'information des organismes en opposition avec leur idéologie.

Taxonomie des attaquants : espions

- Ils participent à la guerre économique. Ils travaillent pour un État ou pour un concurrent. Ils sont **patients** et **motivés**. Ils savent garder le secret de leur réussite pour ne pas éveiller les soupçons et continuer leur travail dans l'ombre. Ils agissent souvent depuis l'intérieur de l'organisme,
  - soit en ayant trouvé un moyen d'y pénétrer,
  - soit en soudoyant une personne ayant accès aux biens.

- Ils ont pour but de **voler des informations** ou de **détruire des données stratégiques** (vitales) pour l'organisme. Dans tous les cas, les espions ont un excellent niveau de maîtrise de soi, ainsi qu'une grande capacité d'adaptation aux environnements.

Taxonomie des attaquants : terroristes

- Souvent appelés les **cyber-terroristes**, moins courants, les terroristes sont aidés dans leur tâche par l'interconnexion et l'ouverture croissante des réseaux : **très motivés**, ils veulent faire peur et faire parler d'eux.

- Les actions se veulent **spectaculaires, influentes, destructrices, meurtrières**.

- Ce profil est pris de plus en plus au sérieux par les États depuis l'attentat du 11 septembre 2001. Ils considèrent qu'une cyber-attaque perpétrée par un terroriste pourrait gravement nuire aux infrastructures économiques et critiques d'un État devenu très dépendant de ses systèmes d'informations vitaux.

Sommaire

partie 1 : attaquants

partie 2 : traces

partie 3 : espionnage

partie 4 : éthique

partie 5 : habilitation

La sécurité et vous

- Depuis l'avènement d'internet, la sécurité informatique a toujours été reléguée au même statut que la plomberie de votre maison : c'est une évidence que vous souhaitez que tout fonctionne sans accroc, mais vous ne voulez surtout pas y penser 99,9% du temps.

- Jusqu'à il y a peu, cela pouvait signifier devoir passer quelques heures à réinstaller votre PC, perdre votre sauvegarde à Sim City, ou perdre les 500Go de photographies accumulées au fil des années

Rappelez-vous…

Anonymat

- L'anonymat fait couler beaucoup d'encre depuis ces dernières années, notamment depuis l'avènement des réseaux sociaux et des dispositifs de surveillance.

- Être anonyme sur Internet est devenu un luxe, et nombreux sont les internautes prêts à payer pour anonymiser leur connexion et leurs traces sur Internet.

- Ces traces sont les supports des données personnelles, disséminées dans notre environnement : mon nom sur ma boîte aux lettres, mon numéro de téléphone dans l'annuaire, des photos de moi dans un album papier ou sur Facebook,... La mise en réseau des sites sur lesquelles les données sont distribuées, va indexer les traces et permettre une recherche.

Traces Internet

- Saviez-vous que :
  - Les robots de Facebook lisent littéralement vos messages privés afin de mieux cibler les publicités ?
  - Les robots de Facebook toujours, peuvent vous reconnaitre sur des photos ou vous êtes de dos.
  - Votre adresse IP, vos cookies, les informations sur votre navigateur, vos habitudes de navigation, vos données transmises en clair… peuvent être récupérées ou interceptées très facilement ?
  - Les SpyWare ne détruisent rien sur votre système mais récupèrent toutes sortes d'informations sur votre ordinateur et surtout sur VOUS à diverses fins (surtout publicitaires) ?

Traces Internet

- Saviez-vous que :
  - La révélation par un quotidien britannique de l'existence du programme de surveillance appelé PRISM, mené par la National Security Agency (NSA), démontre que Google, Facebook, Yahoo… sont associés au programme afin de surveiller les internautes ?
  - Google en sait plus sur vous que votre mère. Par exemple, Google connaît et retient tous les termes que vous aviez recherchés, voir ici :
    - https://history.google.com/history/
  - Les données que vous croyez avoir supprimées d'un site, blog, forum… sont encore en ligne et visibles par tout le monde ?

Traces Internet

- En utilisant Internet, chacun de nous laisse des traces :
  - Publication de contenus : blog, podcast, videocast, encyclopédies collaboratives (Wikipédia), plateforme de FAQ collaborative (Yahoo! Answers, Google Answers)
  - Partage de contenus : photos (FlickR), vidéos (YouTube, Dailymotion, Vimeo...), musique ou liens (delicious)
  - Publication d'avis sur des produits, des services, des prestations (TripAdvisor, Epinions, ...)
  - Participation à des réseaux sociaux : sur un thème particulier (motos, cuisine, jeux...) entre des professionnels (LinkedIn, Viadeo, Xing...) ou sur des thèmes universels (MySpace, Facebook, Orkut...)
  - Achats en ligne sur des sites comme Amazon, eBay ou Ricardo.ch avec des systèmes de paiement type Paypal
  - Sites de rencontres (Meetic, celibataire.ch)
  - Sites de jeux en ligne (World of Warcraft, Everquest...) ou univers virtuels (SecondLife, Playstation Home...)

Sommaire

L'espionnage industriel

- Les attaques ciblées dans un but de cyber-espionnage vont continuer d'augmenter, constituant désormais la menace la plus importante pour les entreprises

- Leur principe : être conçu pour pénétrer spécifiquement le système d'information d'une société afin d'y dérober des données sensibles qui pourront ensuite être revendues sur le "marché noir".

- Ces attaques ciblées sont souvent caractérisées par un degré de sophistication élevé. Cependant, le point de départ de nombreuses attaques est souvent l'élément humain : les individus malintentionnés trouvent des astuces pour amener des employés à divulguer des informations qui seront exploitées par la suite pour accéder aux ressources de l'entreprise

L’espionnage industriel

- Le volume grandissant d'informations partagées en ligne et l'utilisation croissante des médias sociaux dans les entreprises a contribué à alimenter de telles attaques.

- Dans ce contexte, les membres du personnel qui interagissent avec les clients, notamment les commerciaux ou les spécialistes du marketing, sont particulièrement vulnérables.

- Toutes les sociétés détiennent des données qui peuvent avoir de la valeur pour les cybercriminels

- elles peuvent simplement être utilisées comme «tremplin» pour atteindre d'autres sociétés

L'espionnage industriel

- Prenez Michel par exemple : ce hacker espionne pour le compte de toutes sortes de sociétés.
- Il suffit d'un virus attaché à un mail qu'on envoie à des salariés, pour pirater les données d'un concurrent.
- Ce travail lui rapporte 50 000 euros en moyenne, la plupart du temps remis dans des enveloppes en liquide.
- Résultat : en 2013, le manque à gagner à cause du piratage pour les entreprises françaises serait de 46 milliards d'euros.

L'espionnage industriel & le cloud

- L'informatique dans le nuage serait une aubaine pour les cybercriminels.
- Il s'agit toujours de cyber-espionnage industriel avec comme objectif de voler des données d'entreprises.
- Mais elles sont désormais hébergées auprès de prestataires d'informatique dont le niveau de sécurité est variable.
- L'avantage est qu'ici, le cybercriminel peut accéder aux informations de plusieurs sociétés en exploitant un "point unique de défaillance ".

L'espionnage étatique

- Les Américains ont pris l'habitude de poursuivre les entreprises françaises, même si elles n'ont rien commis d'illégal aux États-Unis.

- Une fois qu'elles les ont condamnées, ils placent à l'intérieur ce qu'on appelle des monitors : des personnes officiellement chargée de vérifier que l'entreprise agit dans la légalité, mais qui de fait, peuvent faire remonter des secrets aux américains.

- Sans oublier les attaques dites de « haut niveau » qui ont pour but d'espionner les données sensibles des états.

Sommaire

partie 1 : attaquants

partie 2 : traces

partie 3 : espionnage

partie 4 : éthique

partie 5 : habilitation

L'éthique

- Pour faire face à ce niveau accru de menaces à l'encontre des données personnelles et professionnelles, les politiques de sécurité ont dû s'adapter.

- Le rôle d'un RSSI lui impose de couvrir les trois principes clés de contrôle des menaces de sécurité modernes :
  - Prévention
  - Protection
  - Détection / réaction

- Des questions d'éthique se posent à chacun de ces principes

L'éthique

- Est-il raisonnable de lire les mails des personnes que l'on administre parce qu'on le peut ?

- Est-il raisonnable de superviser les sites Web visités par les personnes que l'on administre ?

- Est-il raisonnable de mettre en œuvre des keyloggers pour savoir ce que tout le monde frappe au clavier ?

- Est-il raisonnable de lire tous les documents ou graphiques stockés sur les PC des personnes que l'on administre ?

L'éthique

2 regards de l'éthique cybersécurité dans l'entreprise

les salariés avec des missions sensibles **dans** l'entreprise ou **pour** l'entreprise

des entreprises & des services

INSIDE

Ethique **dans** l'entreprise

OUTSIDE

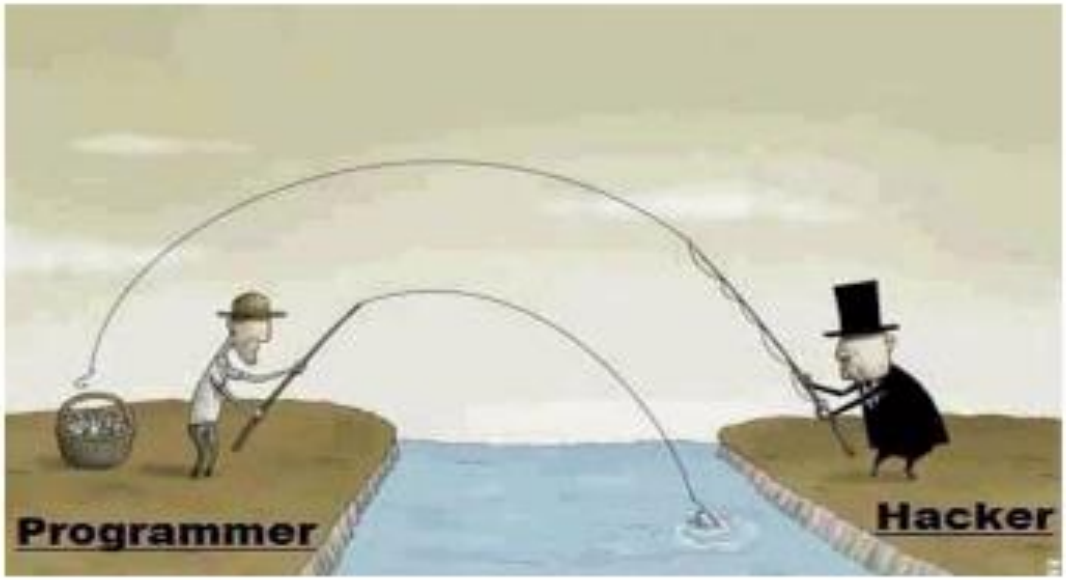
Ethique **pour** l'entreprise

« Ethique » **de** l'entreprise

L'éthique

- On ne parle pas du point légal
- Une société a le droit de superviser ce que fait un employé avec son équipement informatique
- En tant qu'administrateurs réseaux ou professionnels de sécurité vous aurez les droits et privilèges de surveiller ce que fait quiconque avec son ordinateur

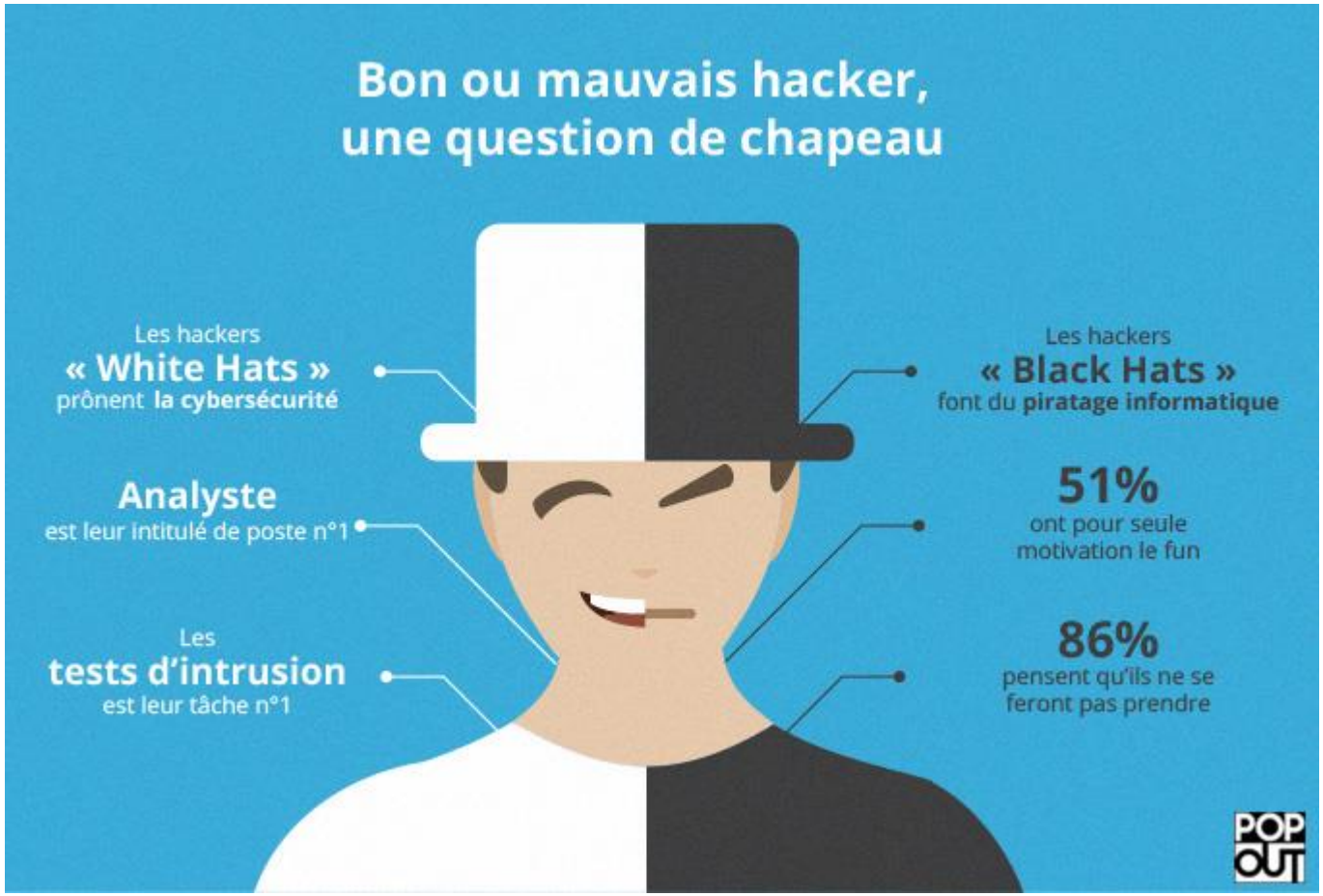
Ethical Hacking



Ethical Hacking

- 1974 : L'U.S. Air Force organise le premier hack éthique de l'Histoire, afin d'évaluer le système d'exploitation Multics.
- 1995 : Le vice-président d'IBM John Patrick invente le terme de hacking éthique, rappelant au passage qu'à l'origine, le mot "hacker" n'était pas forcément péjoratif.
- 2003 : La communauté en ligne OWASP crée un guide permettant de cadrer et d'améliorer les différents tests d'intrusion.
- 2015 : Le business mondial de la cyber-sécurité est désormais un marché de 77 milliards de dollars.
- 2031 : Des hackers "Gold Hats" sont désormais embauchés pour veiller à la cyber-sécurité des hackers "White Hats".

Ethical Hacking



Ethical Hacking

- une éthique professionnelle « irréprochable » !

Ethical Hacking

- Les hackers éthiques travaillent majoritairement dans :
  - **Les télécommunications :** Assez logiquement, c'est dans le domaine des télécoms que travaillent plus de 30% des "White Hats".
  - **La finance :** Régulièrement attaqué par des mauvais hackers, le milieu de la finance embauche quant à lui plus de 19% des hackers éthiques.
  - **Le juridique :** Plus de 7% des gentils pirates travaillent dans le domaine juridique et veillent contre les infiltrations dans les réseaux des institutions.
  - **Les banques :** Afin de lutter contre les cyberattaques dont elles sont la cible, les banques emploient environ 6% des hackers éthiques pour sécuriser leurs données.
  - **L'électronique :** Les hackers ont beau être souvent de fins connaisseurs en électronique, ils ne sont pourtant qu'à peu près 2% à travailler dans ce secteur.

Sommaire

partie 1 : attaquants

partie 2 : traces

partie 3 : espionnage

partie 4 : éthique

partie 5 : habilitation

L’habilitation

- L’habilitation donnant accès à des informations classifiées fait partie d’un dispositif réglementaire important

- Les différentes étapes de cette procédure sont :
  - la demande d'habilitation par la hiérarchie du service employeur ;
  - l'intéressé remplit une notice individuelle de sécurité ;
  - l'instruction du dossier d'habilitation par le ministère de l'Intérieur ou de la Défense.

- La décision d’habilitation est conditionnée par les résultats d’une enquête conduite par les services de sécurité compétents.

L'habilitation

- Sous réserve du « besoin d'en connaître » défini ci-dessus, les durées de validation sont :
  - Très Secret - Défense (TSD): 5 ans
  - Secret - Défense (SD): 7 ans
  - Confidentiel - Défense (CD): 10 ans

- Tout changement d'affectation d'un poste figurant dans le catalogue des emplois à un autre poste répertorié, ou que l'autorité compétente souhaite voir répertorier, implique obligatoirement une nouvelle décision d'habilitation.

La classification

Dénomination	Dénomination anglaise	Description
Extrêmement secret	Extremely Secret	Le plus haut niveau de secret de l'information. La divulgation publique d'une information pourrait nuire très gravement et de manière irréversible à la sécurité mondiale.
Très secret	Top Secret	La divulgation publique de cette information pourrait causer un dommage grave pour la sécurité nationale.
Secret	Secret	La divulgation publique d'une information classée secret pourrait nuire sérieusement à la sécurité nationale.
Confidentiel	Confidential	La publication d'une information classée confidentielle peut nuire ou être préjudiciable à la sécurité nationale.
Restreint	Restricted	La divulgation publique d'une information classée restreinte pourrait causer des effets indésirables. Tous les pays n'utilisent pas cette classe.
Non protégé	Unclassified	Ce niveau est utilisé pour les documents gouvernementaux dont le niveau de sensibilité ne correspond pas à une des classes ci-dessus. Leur lecture ne nécessite pas d'habilitation spécifique.

La classification

- Lorsqu'une administration nationale souhaite partager des informations avec une administration d'un ou plusieurs gouvernements étrangers, une procédure spécifique est généralement employée, avec l'accord préalable des correspondants

- Des informations sensibles partagées par les alliés de l'OTAN sont classées dans quatre niveaux de secret :
  - Cosmic Top Secret (CTS),
  - NATO Secret (NS),
  - NATO Confidential (NC)
  - ATO Restricted (NR)

La réglementation de défense

- Arrêté du 30 novembre 2011 et l'Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.

- Instruction interministérielle n° 920 du 12/01/2005, relative aux systèmes traitant des informations de niveau confidentiel-défense

- Instruction interministérielle n°901 du 11/02/ 2015 relative à la protection des systèmes d'information sensibles

- Document disponible sur le site de l'ANSSI : http://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/

Les trois principes

- Un document doit être marqué

- Le personnel doit être habilité et sensibilisé

- Le personnel doit avoir le besoin d'en connaitre

Le marquage des informations

- Le marquage vaut pour tous les supports (papier, CD, disque dur, clés USB…) ou informations.
  - Classification

  - Protection

  - Mention

- Une absence de marquage est ambigüe et ne signifie pas non protégé.
- Le niveau de classification est spécifié par l'annexe de sécurité

Le marquage des informations

- Un document peut contenir des informations de niveau de classification différents. Dans ce cas il sera classifié au niveau de classification le plus élevé contenu dans le document

- Tout extrait de document classifié est lui-même classifié sauf mention explicite.

- L'annexe de sécurité est un document contractuel qui régit la classification des fournitures et/ou des données.

- Le détenteur de l'information peut « déplacer » de l'information du niveau n vers le niveau n-1 de manière discrétionnaire. Responsabilité pénale de la personne en cas de déclassification non pertinente.

Habilitation et sensibilisation

- L'accès à l'information est réservé aux personnes habilités
  - Une exception : le diffusion restreinte
  - Le contrôle est de la responsabilité du chef de projet et de l'officier de sécurité

- La sensibilisation à la sécurité lieu à trois moments clés
  - À l'embauche (nouvel arrivant)
  - À la notification de décision (engagement de responsabilité – volet 1)
  - À la fin du contrat (engagement de responsabilité – volet 2)
  - Et en fonction des besoins…

- La réglementation est là pour vous protéger
  - Ne pas se mettre en danger.

Habilitation et sensibilisation

- Etre habilité, c'est engager sa responsabilité
  - Signature de l'engagement de responsabilité (volet 1 et volet 2)
  - A la notification de décision et lors du départ (poste ou entreprise)
  - Etre habilité est une information protégée (DR)
  - Réservé aux seules personnes ayant le besoin d'en connaitre.
  - Pas de trace sur les CV ou sur les profil des réseaux sociaux

- L'officier de sécurité doit être prévenu
  - en cas de changement dans la situation matrimoniale,
  - en cas de sentiment de recherche d'informations sur vous ou sur votre travail (sur des salons, dans des lieux publics, association, internet…)
  - VICES (Vénalité, Idéologie, Compromission, Ego, Sexe)

Habilitation et sensibilisation

- dura lex sed lex
  - Articles 121-2, 411-1 à 411-11, 413-9 à 413-12 et 414-7 à 414-9 du code pénal (reprise dans l'IGI 1300 et sur Legifrance).
  - S'introduire sans autorisation à l'intérieur des locaux (art. 413-7) est puni de six mois d'emprisonnement et de 7.500 euros d'amende
  - Donner l'accès à une personne non qualifiée ou de le porter à la connaissance du public ou d'une personne non qualifiée une information classifiée est puni de sept ans d'emprisonnement et de 100.000 euros d'amende (art. 413-10)
  - S'assurer la possession, accéder à, ou prendre connaissance une information classifiée est puni de cinq ans d'emprisonnement et de 75.000 euros d'amende (art. 413-11)

Besoin d'en connaitre

- Deux personnes habilitées au même niveau n'ont pas le même besoin de connaissance
  - C'est la base du cloisonnement de l'information
  - S'applique uniquement dans les zones multi-projets

- Le besoin d'en connaitre est formalisé par le catalogue des emplois
  - Document qui précise le rôle de la personne et le niveau d'habilitation requise.

Questions

Merci