M1
Sécurité des systèmes d'informations
2023-2024

UNIVERSITE PARIS 8 VINCENNES-SAINT-DENIS
Christophe Villeneuve
@hellosct1
@hellosct1@mamot.fr

Session 5 : Gestion de la cybersécurité au sein d’une organisation

- ~~Correction TP 4~~
- ~~La sécurité au sein d’une organisation~~
- ~~La sécurité dans les projets~~
- Difficultés liées à la prise en compte de la sécurité
- Conseiller d’orientation
- TP : Brainstorming
- Guide de conformité

- La sécurité au sein d’une organisation
- La sécurité dans les projets
- Difficultés liées à la prise en compte de la sécurité

Une compréhension insuffisante des enjeux

- Liée
  - A un problème d’éducation
  - A un problème de formation
- Entraînant de nombreux risques
  - Pour l’entreprise ou pour l’organisation
  - Pour les États

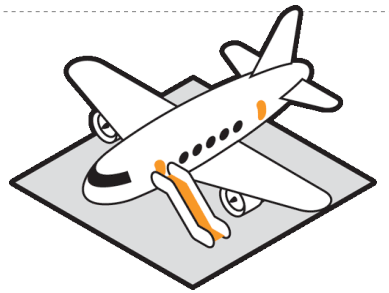
Lié

Problème d'éducation problème de formation

L'information a une valeur importante pour l'entreprise, pour les concurrents, pour les États.

→ On parle aujourd'hui de « guerre de l'information »

- Chaque année des centaines de compagnies en France sont victimes d'espionnage industriel ou économique :
  - Écoute des conversations
  - Espionnage des écrans d'ordinateurs
  - Social engineering, etc..
- Des actes aisés dans les transports : train, avion, etc.



Les voyageurs aux USA perdent environs

12 000 pc portables chaque semaine*

*source : Ponemon Institute

Lié

Problème d'éducation **problème de formation**

- Des dirigeants qui n'ont pas tous une culture sécurité
- Des évolutions vers le poste de « RSSI »

  → sans formation complémentaire adéquate :

  - personnel issu de la technique : administrateur réseau, système…
  - personnel issu de la qualité : responsable qualité…
- Un coût lié à la sécurité qui rebute en période de crise :
  - Authentification forte : achats de jetons/carte à puce
  - Plan de secours : acheter en double certains équipements
  - Personnel : former aux bonnes pratiques en sécurité…

Entrainant de nombreux risques

Entreprise / Organisation Les états

- Perte d’informations essentielles
- Arrêt de la production
- Détérioration de l’image/réputation
- Risques juridiques/réglementaires…

Entrainant de nombreux risques

Entreprise / Organisation **Les états**

- Indisponibilité de services
- Perte de crédibilité
- Divulgation d’informations sensibles
- Risques de conflits avec d’autres États…

L’implication nécessaire de la direction

- Rien ne peut se faire sans l’aval de l’exécutif.
- Le chef d’entreprise doit être conscient des enjeux de sécurité pour l’avenir de son entreprise :
  - Être **proactif** plutôt que réactif. La PSSI est une réflexion stratégique : Elle permet de prévoir l’avenir de l’organisation ;
  - **Prendre le temps** de comprendre, ne pas être absorbé que par ses marchés, ses clients, ses concurrents, son relationnel ;
- La sécurité :
  - **va au-delà de la technique**. L’humain joue un rôle central ;
  - **ne doit pas rester un domaine d’experts**. La sécurité est l’affaire de tous et une préoccupation de tous les responsables ;
  - n’est pas seulement une contrainte coûteuse mais **elle est aussi un investissement**, un atout supplémentaire pour l’organisation.

L’implication nécessaire de la direction

- Investir dans la sécurité ne suffit pas.
  - Il faut être conscient des enjeux vis-à-vis de l’organisation.
  - La dynamique sécurité viendra de la direction.

  Le dirigeant doit montrer l’exemple
  - d’abord en y accordant un intérêt : charismatique,
    - il est le premier à sensibiliser les personnes concernées
- Motiver
  - son RSSI ou ses administrateurs
    - pour faire appliquer la politique de sécurité de l’organisation
    - et maîtriser leurs systèmes le mieux possible

- Responsabiliser
  - en désignant un responsable de la coordination, qui distribuera les tâches au sein des équipes
- Réagir en cas d’attaque avérée :
  - mettre des ressources à disposition, permettre l’expertise juridique et porter plainte
- Impliquer
  - ses personnels, les sensibiliser et leur permettre de suivre des formations.

Difficulté pour faire des choix en toute confiance

- Il est important de faire des choix éclairés
  - en prenant en compte la sécurité.

"L'implantation en France des chinois Huawei et ZTE pose une question de sécurité nationale"

Par JMBockel (Express Yourself) publié le 01/10/2012 à 15:12, mis à jour à 15:25

Vie privée : La NSA s'octroie un backdoor dans tous les systèmes Windows

Le Gouvernement Chinois a adopté une nouvelle régulation exigeant aux entreprises qui vendent des ordinateurs aux banques chinoises de fournir le code source et de se soumettre à des audits.

Ayez confiance !!!

- Quels sont aujourd'hui les matériels ou logiciels de confiance ?
  - Ceux issus de
    - l'industrie nationale VS ceux de nos partenaires de confiance : alliés, fournisseurs
  - Ceux issus du monde libre (« open source »)
  - Les matériels qualifiés par l'ANSSI.
- Quels sont les organismes de confiance ?
  - Les entreprises nationales ou européennes
    - mais qui sont les actionnaires
  - Nos partenaires de longue date
  - Les autorités gouvernementales
  - Les prestataires de service qualifiés par l'ANSSI.

contexte : exemple 1

- Authentification requise pour chaque application dans l'entreprise

- Problème pour l'utilisateur :
  - J'ai besoin de travailler chaque jour avec 5 applications

    et je dois à chaque fois y saisir un mot de passe différent.

- Réaction pour l'utilisateur :
  - Je note certains mots de passe sur papier

contexte : exemple 1

- Utiliser une application de chiffrement pour partager les fichiers chiffrés avec des partenaires

- Problème pour l'utilisateur :
  - l'interface de Crypt&Share n'est pas ergonomique.

- Réaction de l'utilisateur :
  - « Je vais utiliser Box ou DropBox pour partager les informations avec mes partenaires ».

contexte : exemple 1

- Les informations classifiées au niveau 4 (niveau de sensibilité le plus élevé) ne doivent pas sortir du S.I.

- Problème pour l'utilisateur :
  - J'ai besoin de l'avis d'un prestataire extérieur sur certaines informations de niveau 4.

- Réaction de l'utilisateur :
  - Déclassification des informations de manière à ne jamais avoir de niveau 4
  - mais uniquement des niveaux 3 ou 2.

Le délicat équilibre entre productivité et sécurité (1/2)

- Les usages fondent les pratiques…
  - entre ce qui est acceptable à l'utilisateur
  - ce qui est nécessaire au bon fonctionnement
    - de l'organisme et ses besoins de sécurité.

Le délicat équilibre entre productivité et sécurité (2/2)

Les usages fondent les pratiques	D'où l'importance

- D'où l'importance :
  - De la pédagogie : expliquer à quoi servent les procédures, leurs bienfondés, leur intérêt pour l'organisation
  - De l'implication des dirigeants : qui viendront renforcer ces convictions
  - De la prise en compte des remarques et éventuelles oppositions des utilisateurs : ergonomie, pratique, simplicité de mise en œuvre etc.
  - La mise en place d'une charte informatique signée et connue de tous
  - De régulièrement rappeler les règles : changer les mots de passe, rejouer les procédures, créer une check-list etc.
  - De sensibiliser en évoquant les incidents réels qui se produisent et peuvent se produire dans l'organisation.

productivité VS sécurité

- Écouter les utilisateurs et prendre en compte leurs besoins lors de l'étude de solutions de sécurité :
  - Proposer des mesures en concertation et avec l'adhésion des utilisateurs concernés autant que possible
  - Former les utilisateurs pour les aider à prendre en main les nouveaux outils et à bien appliquer les mesures.
- Tester les procédures, dans le but d'évaluer son efficacité (applicabilité, réalisation des objectifs, risques encourues) :
  - Éviter de multiplier les moyens de protection si ceux-ci ne sont pas respectés
  - il faut parfois investir moins dans la sécurité mais avoir des procédures efficaces.
- Confier la responsabilité de la sécurité à un collaborateur qui a le pouvoir ou les ressources pour la faire appliquer.
- Choisir les solutions les plus adaptées à sa propre structure, à son fonctionnement, au niveau de maturité l'entreprise.

Le Cloud (1/

- Les technologies Cloud se popularisent de plus en plus au sein des entreprises.
  - Les raisons évoquées sont diverses et peuvent être :
    - Réduction des coûts
    - Meilleure accessibilité
    - Gestion confiée à un tiers
- Mais les mesures de sécurité et réglementaires constituent toutefois des « freins ».
- Le SaaS (Software as a Service) est l'usage du Cloud le plus rencontré en entreprise :
  - SaaS est la fourniture d'applications sous forme de service à la carte.
  - L'application est installée dans le Cloud (Datacenter) et l'utilisateur paye une licence d'utilisation.

  Les utilisateurs finaux souscrivent aujourd'hui à des services SaaS sans l'aval de la direction informatique et en dépit des règles de sécurité.
  - Ils accèdent au SaaS à travers divers terminaux souvent non contrôlés par l'entreprise. On parle alors de « Shadow IT » :
    - Dans une entreprise du CAC, le DSI estimait à près de 100 le nombre total d'applications.

      Un audit de découverte du Cloud à révéler près de 2500 usages SaaS.

Le Cloud (2/

Le recours à des services type Cloud pose de nouvelles problématiques que l'entreprise se doit de résoudre, notamment :

- Le choix d'un fournisseur
  - Est-ce que le fournisseur dispose de certification relatives à l'hébergement (Exemple : SAS 70 II)?
  - Est-ce que le fournisseur est agréé par une autorité nationale?
- Le stockage
  - A qui appartiennent légalement les données lorsqu'elles sont hébergées ?
  - Quelles sont les mesures de protection des données stockées?
  - Les systèmes sont-ils mutualisés avec d'autres clients ou nous sont-ils dédiés ?
  - Qui doit fournir les clés cryptographiques ?
  - Comment les données sont-elles sauvegardées, redondées ?
- Le transport des données
  - Qui fournit l'infrastructure de transport?
  - quels sont les mécanismes de sécurité en place?
- Fin de contrat : réversibilité
  - Que deviennent les données lorsque le contrat expire ?
  - Comment sont-elles restituées au client, supprimées du Cloud et qu'advient-il des données sauvegardées sur bande ?

Le Cloud (3/

- Les guides suivants peuvent être utiles pour choisir un fournisseur SAAS :
  - Guide Contractuel SAAS : http://www.syntec-numerique.fr/content/publication-du-guide-contractuel-saas
  - Recommandations CNIL pour la souscription au SAAS :
    - http://www.cnil.fr/linstitution/actualite/article/article/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services/
  - Guide de l'ANSSI : « Sécurité de l'externalisation » :

    http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/externalisation/
- Les Cloud Access Security Brokers (CASB) ou les Cloud Security Gateway (CSG) sont des composants logiciels ou matériels qui se situent entre les utilisateurs et le fournisseur SaaS et permettent :
  - de protéger les données des utilisateurs de l'entreprise de manière à ce que l'éditeur SaaS ne puisse les lire ;
  - de gérer les accès et de l'authentification unique (SSO) ;
  - de conserver les données en local via de la tokenisation ou de les chiffrer avant de les envoyer vers le fournisseurs SaaS…

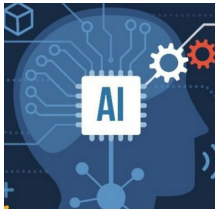
Le Cloud (4/

- Le Cloud pourrait à terme rendre les autres moyens de sauvegarde désuets :
  - sauvegarder une copie de son S.I. au sein du Cloud permettra à l'organisation de redémarrer une activité saine à tout moment en cas d'incident ;
  - A partir d'une sauvegarde, un espace de travail peut être accessible de n'importe quel endroit du monde pour tous ceux qui y sont autorisés.
- La fédération d'identité est un usage du Cloud qui peut permettre aux entreprises de mieux gérer les identités de ses utilisateurs et de :
  - centraliser les comptes utilisateurs ;
  - d'octroyer et de retirer facilement les droits d'accès sur plusieurs applications en interne ou en externe ;
  - tracer les utilisateurs et leurs actions…

Le Big Data

- « Big Data » recouvre l'exploitation des données massives impossibles à manipuler avec les outils classiques comme les bases de données.
  - Le « Big Data » comme outil de sécurité :
    - Modélisation des comportements et détection des anomalies sur la base de corrélation des données issues du trafic réseau ;
    - Détection possible des attaques persistantes avancées (APT) ;
    - Meilleure efficacité des outils tels que des SIEM, IDS, ou IPS ;
    - Surveillance du trafic réseau pour identifier des botnets.
  - Le « Big Data » représente un enjeu pour la sécurité des S.I. :
    - La source de données doit être fiable, et intègre (comme dans toute collecte d'information) ;
    - L'anonymisation des données manipulées représente une véritable difficulté compte tenu de leur volume important ;
    - La localisation des données car le « big data » est souvent exploité dans le « cloud » et les réglementations applicables ;
    - La protection de données exploitées est importante et le chiffrement peut être difficile à assurer. Un vol de données aura une ampleur beaucoup plus importante.

Intelligence Artificielle (1/2)



- Un processus d'imitation de l'intelligence humaine
  - Repose sur la création et l'application d'algorithmes exécutés

    dans un environnement informatique dynamique
- But de permettre
  - à des ordinateurs de penser
  - d'agir comme des êtres humains.
- Pour y parvenir, trois composants sont nécessaires :
  - Des systèmes informatiques
  - Des données avec des systèmes de gestion
  - Des algorithmes d'IA avancés

Intelligence Artificielle (2/2)

- Cybersécurité
  - AI dans la sécurité de l'email
    - Adoption accrue du cloud et de la prolifération d'attaques ciblées

      → les lacunes des passerelles de messagerie sécurisées sont devenues évidentes
    - Hacker améliorer leurs méthodes d'attaque

      → Solutions de sécurité de l'email doivent adopter une approche prédictive en matière de détection des menaces
  - Algorithme supervisé
    - Phishing, Ransonware, Redirection URL/pages
  - Algorithme non supervisé
    - Malware, usurpation identité

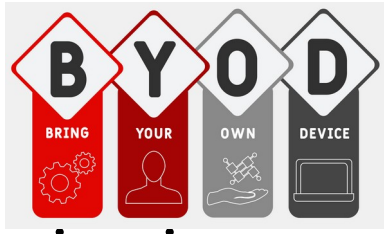
Des frontières floues

entre sphères professionnelle, publique, et privée

- Quel est le périmètre de confiance?
  - Internet est un réseau mondial ouvert ; dans un monde concurrentiel, il est naturel qu'il soit source de menaces
  - Les réseaux d'entreprises sont des réseaux internes, généralement protégés de façon périmétrique, mais peu protégés en interne…
  - Les multinationales possèdent souvent de grands réseaux ouverts à des exploitants, des services de télémaintenance et des sous-traitants qui ont des d'accès conséquents sur ces réseaux, et qui possèdent eux-mêmes leurs propres informations
  - De plus, de nombreux « nouveaux » appareils sont utilisés

    → smartphones, tablettes etc.
    - faiblement sécurisés et connectés directement à Internet (Wifi, 3G/4G, etc.)

BYOD



- =Apportez Votre Equipement personnel de Communication
  - Focus sur le smartphone personnel (ou la tablette personnelle) :
    - Il nous accompagne au travail, lors de nos déplacements
    - On le connecte à notre PC de bureau pour le recharger en USB
    - Il remplace souvent notre téléphone professionnel, peut-être moins performant ou restreint en terme de fonctionnalités
    - Pour des raisons de facilité, on y configure notre messagerie professionnelle, nos contacts, notre emploi du temps… autant d'informations qui peuvent potentiellement être sensibles pour l'entreprise.
- La frontière entre nos informations privées et nos informations professionnelles devient donc très floue
- Dès que les informations sont stockées sur un smartphone personnel

Vie privée (1/2)

- Raconter, partager sa vie privée sur l'Internet c'est y être pour la postérité…
  - Nos données nous échappent dès l'instant où nous les publions : Dans le meilleur des cas, on pourra effacer notre propre publication, mais on ne pourra pas effacer les multiples copies que l'on ne contrôle pas (droit à l'oubli illusoire par manque de maîtrise de l'information)
  - C'est permettre à tout inconnu, d'entrer dans notre sphère privée ; la restriction des accès aux « amis » n'est qu'illusoire dans l'absolu
  - c'est permettre aux Ressources Humaines de filtrer notre CV ; et déterminer le profil privé du candidat correspondant au profil professionnel recherché
  - à nos collègues et supérieurs d'interpréter nos propos…

Vie privée (2/2)

- Partager les problèmes que l'on rencontre au travail : personnels, techniques, relationnels ; consulter des sites personnels au travail…
  - c'est peut-être mettre en danger son organisation : en offrant à un pirate ou un concurrent des informations précieuses
    - version d'un logiciel, faille de sécurité, fournisseurs, secrets commerciaux, informations RH…
  - transgresser la déontologie du travail, ou la charte de confidentialité
  - potentiellement s'exposer à des sanctions en interne qui peuvent aller jusqu'au pénal

En résumé

- Évolution
  - des modes, des besoins, des technologies, des habitudes
- Au-delà des nouveautés
  - Toujours le même problème :
    - la non-prise en compte de la sécurité
      - développement, implémentation, exploitation, formation
- Un périmètre d'attaque et d'accident plus étendu mais peu nouveau
- Une prise en compte permanente des enjeux et de la sécurité par tous (hygiène informatique) et par le chef d'entreprise
- Un accroissement des besoins de sécurité :
  - besoin en compétences et en professionnels.

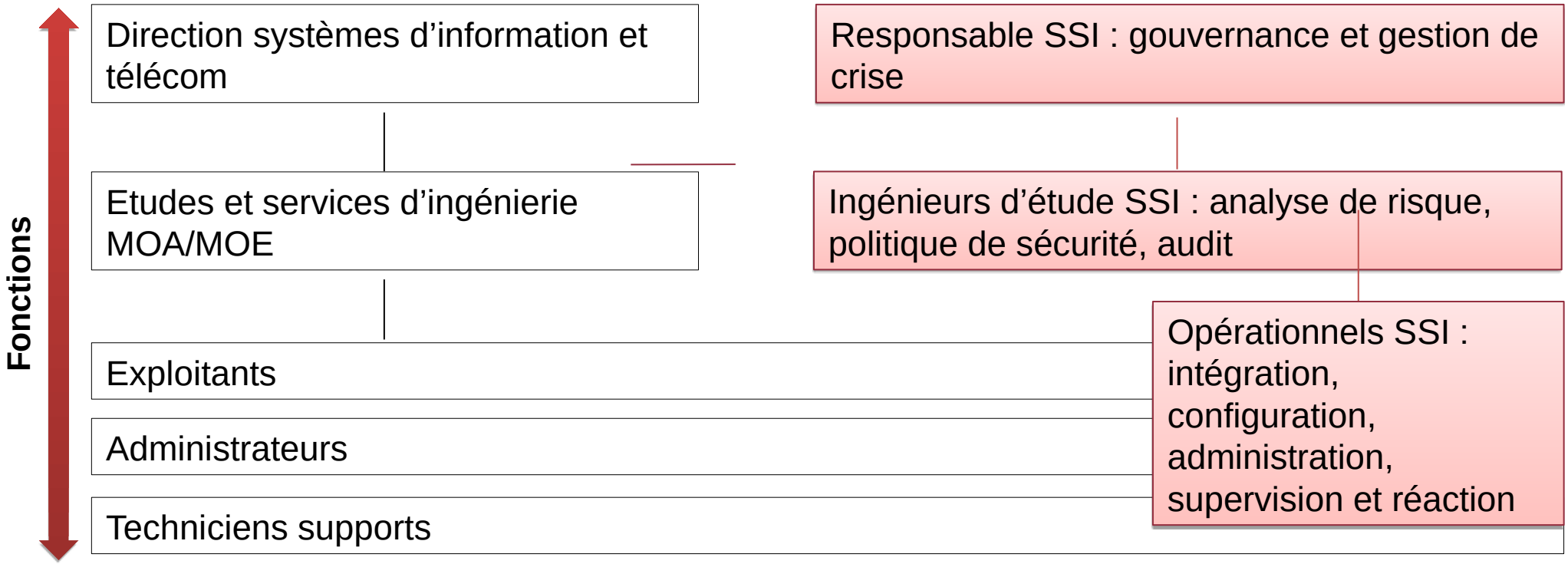
https://school.hello-design.fr

5C

- La sécurité au sein d’une organisation
- La sécurité dans les projets
- Difficultés liées à la prise en compte de la sécurité
- Conseiller d’Orientation

Les métiers au sein des organisations (1/2)

- La cybersécurité est transverse à toute activité



Les métiers au sein des organisations (2/2)

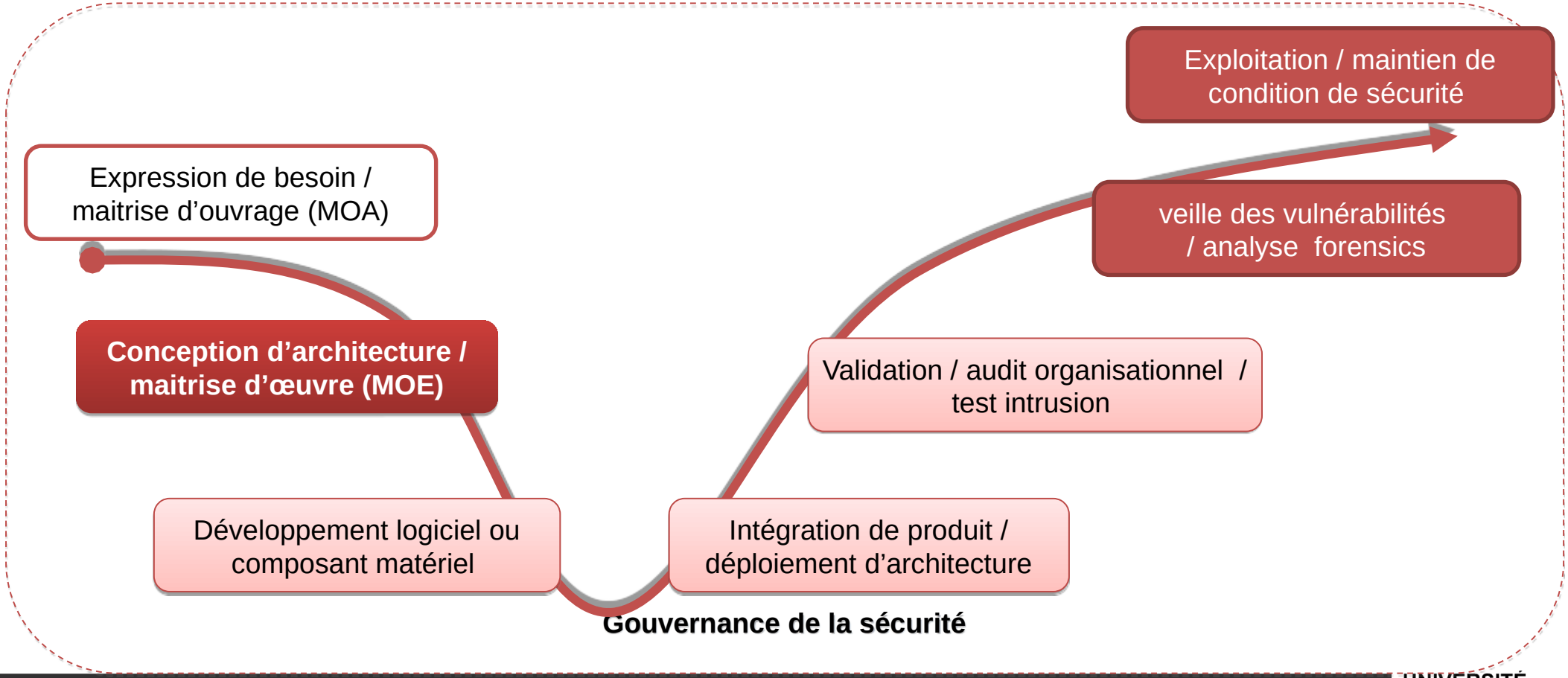
- Selon la taille de l'organisation (PME/PMI/Grande entreprise…)
  - Fonctions liées à la cybersécurité nécessitent une charge de travail qui varie

ETP = Équivalent Temps Plein
DSI = Direction des Systèmes d'Information
SSI = Sécurité des Systèmes d'Information
PSSI = Politique de Sécurité des Systèmes d'Information

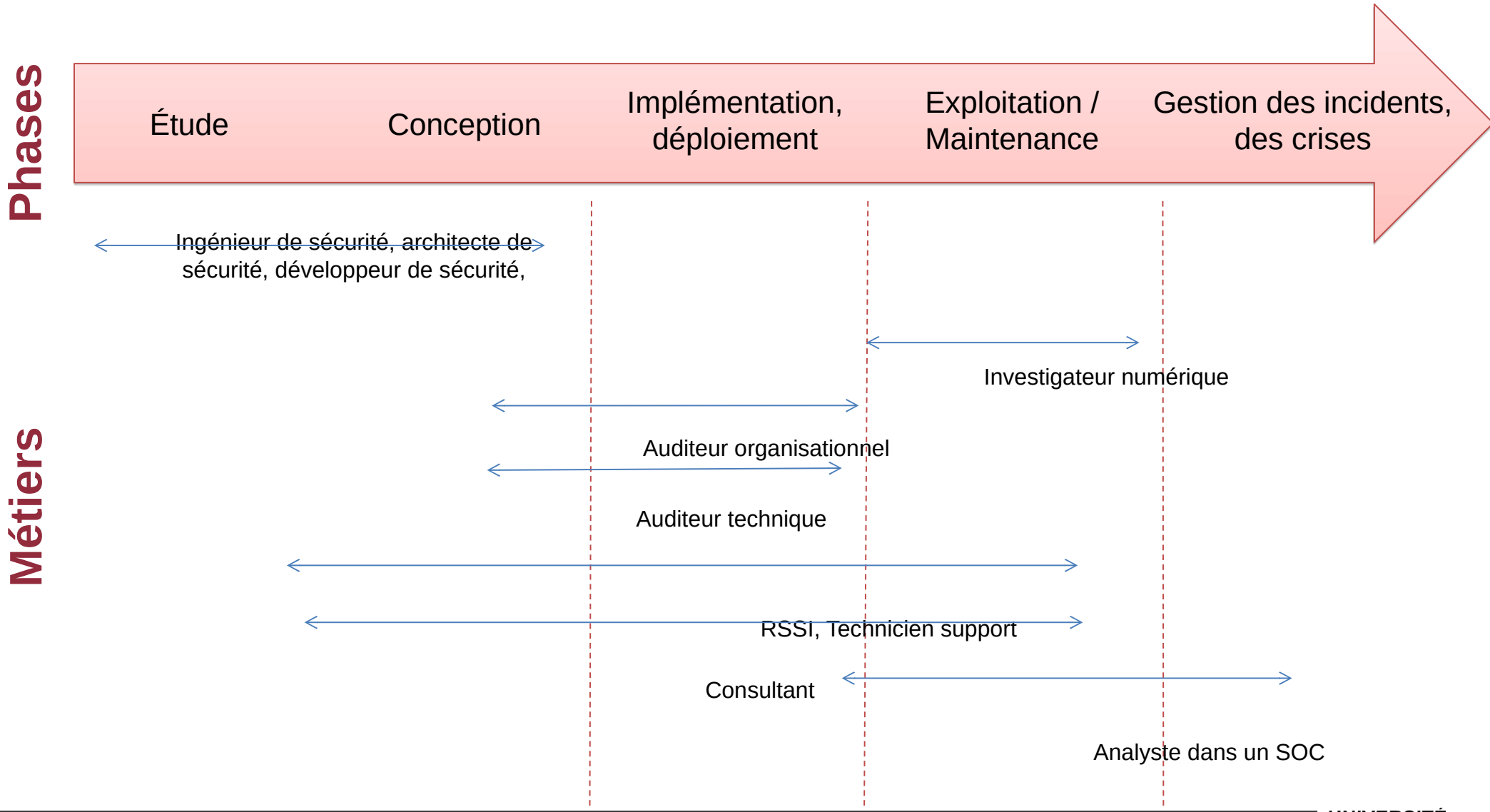
	PME/PMI DSI 15 pers	Grande entreprise DSI 500 pers
Responsable SSI : gouvernance et gestion de crise	¼ ETP du Dir. du S.I.	3 à 5 ETP
Ingénieurs d'étude SSI : analyse de risque, mise en œuvre PSSI, audit…	¼ ETP des études S.I.	5 à 10 ETP
Opérationnels SSI : intégration, configuration, administration, supervision et réaction	1 ETP réparti sur l'exploitation du S.I.	20 à 50 ETP si H24 7/7

Cartographie des métiers et compétence en SSI (1/

- Les métiers se répartissent dans le cycle de vie d'un projet
  - De expression de besoin → retrait de l'exploitation
    - Sous la responsabilité de la gouvernance globale de l'organisation.



Cartographie des métiers et compétence en SSI (2/3)



Cartographie des métiers et compétence en SSI (3/

- Les métiers se répartissent dans les familles de l'informatique et des réseaux.

	Nb année expérience	Compétence technique	Compétence management
Gouvernance des systèmes d'information			
•Responsable ou Directeur	15 à 20	X	XXX
•Chef de projet / Consultant MOA	5 à 15	XX	XX
Conception et déploiement de système d'information			
•Chef de projet / Consultant MOE	5 à 15	XX	XX
•Architecte système	10 à 15	XXX	
Développement logiciel et matériel			
•Architecte/concepteur logiciel/composant	5 à 10	XXX	
•Développeur logiciel (dont cryptologue)	0 à 10	XXX	
Exploitation			
•Technicien système et réseau	0 à 10	XXX	
•Administrateur système et réseau	0 à 10	XXX	X
•Analyste veille/gestion des incidents/forensics	0 à 10	XXX	X
Validation / Audit			
•Auditeur technique SSI (dont test intrusion)	0 à 10	XXX	X
•Auditeur organisationnel SSI	5 à 10	X	X

Compétence requise :
X : peu de compétence
XX : niveau moyen
XXX : forte compétence

Profils et carrières (1/

- Responsable de la Sécurité des Systèmes d'Information (RSSI) :
  - définit la politique de sécurité du SI et veille à son application
    - Assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte.
- Architecte [système, logiciel] sécurité :
  - l'architecte sécurité structure les choix techniques, technologiques et méthodologiques d'un ensemble [système, logiciel]
    - Répond à des exigences de sécurité.
- Développeur [produit, logiciel] de sécurité :
  - le développeur de sécurité assure le sous-ensemble des activités d'ingénierie nécessaires à la réalisation d'éléments [produit, logiciels]
    - Répond à des exigences de sécurité.

Profils et carrières (2/

- Technicien ou Administrateur système et réseau
  - assure ou est responsable de diverses activités de support, de gestion ou d'administration de la sécurité aux plans techniques ou organisationnel.
- Analyste
  - assure la veille sur les vulnérabilités des produits et logiciel, , recherche et détecte les incidents de sécurité coordonne le suivi de l'application des correctifs.
- Auditeur Organisationnel
  - contrôle la prise en compte de la sécurité au niveau organisationnel sur la gouvernance, les procédures de sécurité notamment vis-à-vis de la nome ISO27K. Il vérifie la conformité des mesures mises en œuvre.
- Auditeur Technique
  - contrôle les configurations des équipements et logiciels. Il est en mesure de pénétrer les défenses d'un système d'information et d'identifier les divers chemins d'intrusions possibles et leurs conséquences. Il vérifie l'efficacité des mesures en place pour protéger le système.

Profils et carrières (3/

- La majeure partie des postes SSI sont occupés actuellement par des personnes ayant une formation informatique ou télécom, s'étant spécialisées au cours de leur carrière par des formations / certifications.
- Certaines certifications en SSI peuvent être effectuées en 5 jours et se terminer par un examen comme par exemple :

ISO 27001 Lead Auditor
ISO 27001 Lead Implementor
ISO 27005 Risk Manager
CISSP : Certified Information System Security Professional
CEH : Certified Ethical Hacker

Compétence Technique : X
Compétence Management : XXX

Compétence Technique : XXX
Compétence Management : X

Compétence Technique : XX
Compétence Management : XXX

Attention : Accroissement des formations spécialisées en sécurité de niveau bac+4/5
Elles permettent généralement de démarrer une carrière sur des postes qui requièrent des compétences techniques.

Possibilité de progression de carrière
depuis la production technique jusqu'à de la direction/management en passant par de la vente ou du marketing de produits/services.

Perspectives d’embauche (1/2)

- Métiers avec une forte demande annoncée pour prochaines années :
  - progression de la virtualisation de IT et des réseaux,
  - révolution digitale des services aux usagers (BToC) et entre entreprise (BtoB),
  - Internet des objets…
- Dans tous les secteurs privés banque, industrie, commerce…
- Ainsi que dans le secteur public : administration, collectivité territoriale, hôpitaux, universités…
- Mais surtout au sein de sociétés de service, principaux employeurs de diplômés depuis 20 ans pour intervenir en sous-traitance ou assistance technique pour les entreprises et les administrations :
  - les organisations tendent à se concentrer sur leur métier et faire de la délégation de service pour les fonctions supports dont la sécurité.

Perspectives d'embauche (2/2)

- Exemples d'organisations spécialisées dans la cybersécurité et qui recrutent :
  - Éditeurs/Constructeurs de produit de sécurité (anti-virus, boitier de chiffrement, pare-feu, ICG…)
    - développement, marketing et vente
  - Tiers de confiance qui exploite des infrastructures pour des clients (produits/services de sécurité en mode IaaS, Saas)
    - conception et déploiement, exploitation, marketing et vente
  - Sociétés de service/cabinet de conseil
    - conseil, expertise, audit…
  - Organismes étatiques comme l'ANSSI, ministère de la défense (DGSE, Armées), ministère de l'intérieur (DGSI, police judiciaire, gendarmerie nationale), la CNIL : conseil, expertise, audit… ;
  - Entreprises proposant ou gérant des SOC.

Hacker / Pirate

CE N'EST PAS UN METIER

Le FBI arrête l'administrateur
du plus important forum de hackers
18 mars 2023

https://www.numerama.com/cyberguerre/1309606-le-fbi-frappe-fort-en-arretant-le-meneur-du-plus-important-forum-de-hackers.html

En résumé

- Les métiers de la cybersécurité sont à avenir
- La frontière est fine
  - Le Bien VS Le Mal

https://school.hello-design.fr

5d

TP 5

TP 5 : Brainstorming

Rappels

- Groupe :
  - 4/5 membres
- Chaque participant

  a un droit de parole
- Ne pas critiquer les idées des autres

Composition des groupes

- Par RND()
- Email dédié
- Contenu de l’email
  - Lien vers le site B2B
  - 1 canal vidéo dédié
  - 1 PAD
    - pour noter
    - partager les réponses

Que faire ?

- Sujet
  - Dans un projet de site marchand,
    - Vous devez identifier les problèmes de sécurité et de vie privée
- Délais

  ~ 1 heure

- Identifier :
  - Les points faibles
  - Failles de sécurités éventuelles
  - Risques liés à ce site
  - Les expliqués comment ils ont fait
  - Rechercher des badges

- But :
  - Naviguer sur
    - le site / boutique
  - Inspecter le site
  - Trouver le score Board
  - Suivre les pistes du score Board
- Complément :
  - Création de compte
  - Ajout d’un produit
  - Ajout d’un commentaire
  - ...


solution
finding
cognitive
reasoning
focused
simulation
engineering
resolution
solutions
solving
analysis
research
emotional
attention
semantically
product
cause
share
book
action
difficulty
motivational
analyzed
field
approaches
theory
possible
analogous
solved
studying
goals
existing
tracing
taken
relatively
prove
try

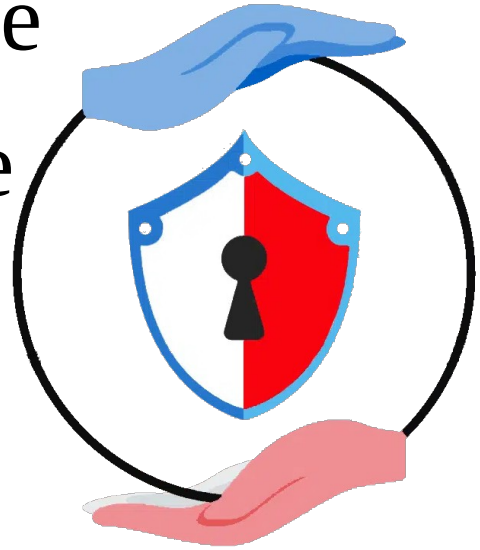
TP 5

Correction

- Le détail sera envoyé avec les notes

- La sécurité au sein d’une organisation
- La sécurité dans les projets
- Difficultés liées à la prise en compte de la sécurité
- Guide de conformité

Guide de la conformité à la cybersécurité



- Impact dans tous les secteurs d'activité
- Le paysage de la cybersécurité évolue
  - Exigences de conformité
    - pour les entreprises de tous les secteurs
  - Difficile de se tenir au courant
    - de ces règles de conformité en matière de cybersécurité
  - Indispensable pour protéger votre entreprise.
- De nombreuses règles de conformité existent
  - En cybersécurité pour les entreprises

Soins de santé

- Secteur des soins de santé est régi
  - par la loi HIPAA (Health Insurance Portability and Accountability Act)

    → les informations de santé protégées (PHI) et les informations personnelles identifiables (PII).
- Conformité à la loi HIPAA exige
  - Entreprises prennent des mesures pour protéger
    - la confidentialité, l'intégrité et la disponibilité des PHI.
  - S'agit de veiller à ce que seules les personnes autorisées aient accès aux PHI, d'utiliser le cryptage pour protéger les PHI en transit
  - de mettre en place un plan de reprise après sinistre en cas d'atteinte à la protection des données.
- Les IPI sont toutes les informations qui peuvent être utilisées pour identifier une personne.
  - Important de protéger ces données
  - Les entreprises du secteur de la santé doivent prendre des mesures pour protéger les IPI contre tout accès, utilisation, divulgation ou destruction non autorisés.

Commerce de détail (1/3)

- Le secteur du commerce de détail est principalement réglementé
  - Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)
  - Le règlement général sur la protection des données (RGPD).

Commerce de détail (2/3)

- La norme PCI DSS exige des entreprises
  - Prendre des mesures pour protéger
    - Les informations relatives aux cartes de crédit des clients contre l'accès et la divulgation non autorisés.
    - La conformité à la norme PCI DSS, comprend
      - Mise en œuvre de mesures de protection physiques
      - Administratives et techniques
      - Réalisation d'évaluations régulières des risques

Commerce de détail (3/3)

- La conformité au RGPD exige des entreprises
  - Mesures pour protéger les données personnelles des individus dans l'Union européenne.
  - S’assurer que les données personnelles sont
    - Collectées et traitées de manière légale
    - Transparente et équitable
    - Les individus ont le droit d'accéder à leurs données personnelles
      - d'en demander la suppression.

Services financiers

- Les entreprises du secteur des services financiers sont soumises à diverses réglementations en matière de cybersécurité, notamment la loi Gramm-Leach-Bliley (GLBA), la loi sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA), la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS), le règlement général sur la protection des données (GDPR) et la loi Sarbanes-Oxley (SOX).

  La loi SOX a été spécialement créée pour protéger les investisseurs contre la possibilité de pratiques comptables frauduleuses de la part de sociétés cotées en bourse. La conformité en matière de cybersécurité est un élément essentiel de la loi SOX et s'applique à toute entreprise qui offre des produits ou des services dans le cadre du commerce interétatique, ainsi qu'à toute entreprise dont les titres sont cotés sur des bourses nationales.

Le droit

- Les cabinets d'avocats sont la cible de cyberattaques car ils traitent de nombreuses informations sensibles. Ils sont soumis à toutes sortes de règles de conformité en matière de cybersécurité, en fonction de leur secteur d'activité. Les réglementations varient également d'un État à l'autre.
- Parmi les réglementations les plus courantes auxquelles les cabinets juridiques doivent se conformer en matière de cybersécurité figurent la loi Gramm-Leach-Bliley (GLBA), la loi sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA) et la loi Sarbanes-Oxley (SOX).

Le gouvernement

- Les agences fédérales doivent se conformer au Federal Information Security Management Act (FISMA) et au National Institute of Standards and Technology (NIST) Cybersecurity Framework. En Europe, les agences fédérales doivent également se conformer à la loi européenne sur la cybersécurité et au RGPD.
- La FISMA exige que les agences développent, documentent et mettent en œuvre un programme à l'échelle de l'agence pour assurer la sécurité de l'information et des systèmes d'information qui soutiennent les opérations et les actifs de l'agence.
- Le NIST est une agence non réglementaire qui fournit le cadre de cybersécurité du NIST, un guide volontaire qui aide les organisations à mieux gérer et réduire les risques de cybersécurité. Les organisations peuvent utiliser le cadre pour évaluer leurs risques de cybersécurité, identifier les contrôles de cybersécurité pour atténuer ces risques et suivre leurs progrès au fil du temps.
- La loi européenne sur la cybersécurité a été créée pour améliorer la cybersécurité des réseaux et des systèmes d'information dans l'Union européenne. Elle impose aux États membres de désigner une autorité nationale de cybersécurité, de créer un système de certification de la cybersécurité et de mettre en place une Agence européenne de cybersécurité.

L'énergie

- Les entreprises du secteur de l'énergie et des services publics sont soumises à la réglementation de la Federal Energy Regulatory Commission (FERC) en matière de cybersécurité.
- Les réglementations de la FERC en matière de cybersécurité sont conçues pour protéger le réseau électrique national contre les menaces liées à la cybersécurité. Les réglementations exigent que les services publics d'électricité développent et mettent en œuvre un programme de cybersécurité comprenant des évaluations des risques, des contrôles de sécurité et des plans d'intervention en cas d'incident.

L'assurance

- Les compagnies d'assurance sont également soumises à une série de réglementations en matière de conformité à la cybersécurité,
  - en fonction de leur secteur d'activité.
- Les réglementations de cybersécurité typiques pour les compagnies d'assurance comprennent
  - la loi Gramm-Leach-Bliley (GLBA)
  - la loi sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA),
  - le règlement général sur la protection des données (GDPR)
  - la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS).

Automobile

- Les véhicules étant de plus en plus connectés, des règles de conformité en matière de cybersécurité sont en cours d'élaboration afin de protéger les véhicules contre les menaces qui pèsent sur eux.
  - La National Highway Traffic Safety Administration (NHTSA) a publié des orientations sur la cybersécurité pour l'industrie automobile.
- Ces orientations sont facultatives, mais elles fournissent des recommandations sur les meilleures pratiques en matière de cybersécurité pour l'industrie automobile et mentionnent des moyens de protéger les véhicules contre le piratage.

Industrie manufacturière

- Les entreprises du secteur manufacturier
  - Soumises à la norme de cybersécurité de l'Organisation internationale de normalisation (ISO)
  - Si les entrepreneurs fournissent des services au ministère de la défense
    - Se conformer aux exigences de cybersécurité du DFARS
      - DFARS = Defense Federal Acquisition Regulation Supplement
- La norme ISO sur la cybersécurité est une norme internationale volontaire qui fournit des orientations sur les risques et les contrôles en matière de cybersécurité.
  - Les exigences du DFARS en matière de cybersécurité sont obligatoires.
  - Le modèle de certification de la maturité de la cybersécurité (CMMC) a été créé par le DoD pour aider à évaluer la conformité en matière de cybersécurité.
  - Il remplacera le DFARS pour devenir la norme de protection des informations non classifiées contrôlées (CUI).
- La Connectivity Standards Alliance a récemment publié la norme Matter 1.0 qui définit une nouvelle façon pour les appareils IoT de communiquer et d'interagir entre eux.
  - Matter utilise une infrastructure à clé publique pour authentifier les appareils et assure une transmission cryptée des messages pour la sécurité des données.
  - Les utilisateurs pourront ainsi connecter en toute sécurité leurs appareils IoT au nuage et à d'autres systèmes connectés.

Conformité au niveau de l'État

- La conformité varie en fonction des réglementations étatiques et locales
  - y compris au niveau international.
- Par exemple, en 2018, la Californie a adopté la loi californienne sur la protection de la vie privée des consommateurs (CCPA).
  - La CCPA est une loi d'État qui réglemente la manière dont les entreprises traitent les données personnelles des résidents californiens, quel que soit l'endroit où l'entreprise est située. La CCPA exige des entreprises qu'elles divulguent les données personnelles qu'elles collectent, les raisons pour lesquelles elles les collectent et les personnes avec lesquelles elles les partagent. Les entreprises doivent également permettre aux consommateurs de refuser la vente de leurs données personnelles.
- En 2017, New York a adopté le règlement sur la cybersécurité du NYDFS. Ce règlement s'applique à toute entreprise soumise à la juridiction du NYDFS et qui possède, stocke ou utilise des informations non publiques. Elle exige des entreprises qu'elles élaborent un programme de cybersécurité et précise ce qu'elles doivent y inclure.
- Le règlement sur l'identification électronique, l'authentification et les services de confiance (eIDAS) est un règlement de l'Union européenne qui a été créé en 2014.
  - Il établit un cadre juridique pour les signatures électroniques et d'autres méthodes d'identification électronique, telles que les e-ID. Le règlement eIDAS s'applique aux entreprises qui fournissent des signatures électroniques ou d'autres méthodes d'identification électronique.
- Récemment, le Conseil britannique de la cybersécurité a été créé dans le cadre de la stratégie nationale de cybersécurité du Royaume-Uni (NCSS) 2016-2021.
  - Les entreprises britanniques doivent se conformer aux règles de conformité en matière de cybersécurité établies par le conseil. Le conseil façonne et informe les politiques nationales et vise à aider les entreprises britanniques à se conformer à la cybersécurité en leur fournissant des ressources et des conseils.

En résumé

- Suivant le métier et son secteur associé
  - → des normes existent
  - A connaître

Rendez-vous au prochain cours

- Merci de votre attention

En présentiel