Management de la sécurité des technologies de l'information

Question 1 : Identifiez les causes d'expansion de la cybercriminalité

Internet est un facteur de performance pour le monde criminel. Par sa nature même et ses caractéristiques, le monde virtuel procure une **couche d'isolation protectrice** aux criminels. Il offre au crime la capacité à être **automatisé**, autorisant une réalisation à grande échelle, permettant d'être commis à distance et avec des effets à retardement.

La **dématérialisation** des acteurs, les **accès à distance**, un **relatif anonymat**, des problèmes de conception, de mise en œuvre, de gestion, associés aux pannes, erreurs, incompétences confèrent de facto un certain niveau d'insécurité aux infrastructures numériques.

La **publication des listes de failles** des systèmes et la disponibilité **d'outils d'exploitation** de ces failles, de bibliothèques d'attaques et de logiciels capitalisant le **savoir-faire** criminel dans un programme offre des opportunités sans précédent.

Le manque de **régulation internationale** et de contrôle offre des avantages largement exploités par les criminels. Ces derniers tirent parti de **la non territorialité** d'Internet.

L'uniformisation du monde de l'informatique et des télécommunications par l'adoption universelle des technologies Internet, la **dépendance** des organisations et des Etats à ces mêmes technologies, et **l'interdépendance** des infrastructures critiques, introduisent un **degré de vulnérabilité** non négligeable.

Une exploitation efficace des nouvelles technologies, permet aux criminels de réaliser des crimes économiques « classiques » tout en leur assurant la maximisation des bénéfices et en les exposant à un niveau de risque acceptable. L'information est au cœur des stratégies criminelles et des processus de décision. Les technologies de l'information deviennent un facteur de production et un élément de stratégie des organisations criminelles.

Question 2 : Pourquoi un responsable sécurité à tout avantage à connaître les différentes phases de réalisation d'une attaque informatique ? Quels sont les facteurs de succès de réalisation d'une attaque ?

La connaissance des différentes étapes de réalisation d'une attaque par un responsable sécurité permet un blocage au plus vite dès les premières phases et ainsi de **réagir au mieux** concernant l'attaque.

Les actions suivantes, entre autres, permettent de **réussir une attaque** informatique :

- Rechercher, connaître les **vulnérabilités** et les **failles** des systèmes ciblés par une attaque, récolter le plus d'informations possible sur ces systèmes.
- Identifier les failles **techniques**, **organisationnelles**, **humaines** de l'environnement.
- Connaître les mécanismes et niveaux de sécurité en vigueur concernant **l'identification**, **l'authentification**, le **contrôle d'accès** et la **surveillance**.
- Exploiter les failles de sécurité connues non patchées.
- Exploiter les **outils** disponibles pour attaquer les systèmes.
- Rester **anonyme**, utiliser des pseudonymes ou usurper l'identité numérique des utilisateurs et brouiller les pistes en passant par plusieurs systèmes intermédiaires.

Management de la sécurité des technologies de l'information

Question 3 : Expliquer la notion de risque juridique en matière de sécurité informatique. Expliquer pourquoi sa compréhension par des responsables de la sécurité informatique est importante. Comment ce risque est pris en compte par les responsables de la sécurité informatique ?

L'intelligence juridique devient l'un des facteurs clés de succès de la réalisation de la sécurité informatique où le droit devient omniprésent. La **responsabilité** des acteurs est de plus en plus invoquée lors de sinistre où les ressources informatiques qu'ils gèrent sont l'objet ou le moyen d'une fraude. Il est nécessaire que les responsables puissent démontrer que des **mesures suffisantes de protection** du système d'information et des données ont été mises en œuvre afin de se protéger contre un **délit de manquement à la sécurité** (à défaut d'une obligation de résultat, ils ont une **obligation de moyens**).

Les responsables d'entreprises eux-mêmes doivent être extrêmement attentifs à l'égard du **droit des nouvelles technologies** et s'assurer que leur système d'information est en **conformité juridique**. Les enjeux juridiques liés à la sécurité informatique sont devenus prépondérants et doivent être pris en compte dans la mise en place de solutions de sécurité.

Les organisations se doivent de se doter de **moyens suffisants** de sécurité et de contrôle. La valeur économique des investissements nécessaires à assurer le seuil minimal de sécurité est fonction des **pertes matérielles** et aussi des **risques de réputation et d'image** potentiels encourus par l'organisation.

Le rôle du responsable sécurité est de mettre en place des mesures de sécurité pour protéger les ressources afin de limiter l'impact des risques sur ces dernières. Ce dernier doit également être sensibilisés aux contraintes d'une enquête policière. La prise en compte des lois ainsi que leur compréhension concernant les valeurs de l'entreprise est obligatoire. La démarche sécuritaire est un processus dynamique qui évolue et donc une veille juridique doit être mise en place afin de réévaluer les risques.

Question 4 : Faire un tableau récapitulatif identifiant les critères de sécurité et les types de mesures de sécurité permettant de les satisfaire.

Critères de sécurités	Type de mesures de sécurité
Disponibilité	- Dimensionnement - Redondance - Procédures d'exploitation et de sauvegarde
Intégrité *Confidentialité*	- Chiffrement - Contrôle d'accès - Sécurité physique - Authentification - Détection, prévention d'intrusion, virus - Contrôle d'erreur, de cohérence
Non Répudiation *Authenticité* *Imputabilité* *Conformité aux lois*	- Certification - Enregistrement, traçabilité - Signature électronique - Mécanismes de preuve
Fiabilité *Durabilité* *Continuité*	- Conception - Performances - Ergonomie - Qualité de service - Maintenant opérationnelle

Management de la sécurité des technologies de l'information

Question 5 : Pourquoi faut-il intégrer la prise en compte du risque informatique dans une démarche générale de gestion de risque des organisations ?

L'informatique est le **support** à tous les processus et les systèmes d'information sont les garant de la **pérennité**, de la **profitabilité** et de la **compétitivité** de l'entreprise. La finalité de la sécurité informatique au sein d'une organisation est de garantir qu'aucun préjudice ne puisse mettre en péril cette **pérennité**. Cela consiste à diminuer la probabilité de voir des menaces se concrétiser, à en limiter les atteintes ou dysfonctionnements induits, et à autoriser le retour à un fonctionnement normal à des coûts et des délais acceptables en cas de sinistre.

Le risque informatique est encore trop souvent sous-estimé par les organisations, il ne doit plus être ignoré et l'idée de pouvoir le transférer via des mécanismes d'assurance ne satisfait pas le besoin d'utilisation efficace des technologies du numérique. Il reste donc à le **maîtriser**.

La démarche sécurité est un **projet d'entreprise** dans la mesure où chacun en général est concerné par sa réalisation. La prise en compte de l'analyse des risques liés aux systèmes d'information dans un processus de gestion de risques, guide toute la démarche de sécurité d'une organisation. Le risque informatique, informationnel ou technologique, quel que soit le nom retenu, doit être **identifié**, au même titre que tous les **autres risques** de l'organisation (risque métier, social, etc.) auxquels doit faire face une entreprise. Le risque informatique est un risque **opérationnel** qui doit être maîtrisé.

La sécurité est de moins en moins une juxtaposition de technologies hétérogènes de sécurité. Elle est dorénavant appréhendée et traitée comme un **processus continu**. Cette vision « processus » met en avant la dimension **managériale** de la sécurité qui vise à l'optimisation et à la rationalisation des investissements, tout en assurant la **pérennité** et **l'efficacité** des solutions de sécurité dans le temps.

La technologie ne suffit pas, elle doit être intégrée dans une démarche de **gestion**. Seule la dimension **managériale** de la sécurité permet de faire face au caractère **dynamique** du risque. La sécurité des systèmes d'information n'est qu'une composante de la sécurité **globale** de l'organisation.

Question 6 : En matière de sécurité informatique, faut-il privilégier une démarche proactive ou réactive ?

Une démarche réactive consiste en l'analyse des évènements notifiés qui ont eu, ou auraient pu avoir, un impact sur la sécurité. Une démarche proactive consiste, sans attendre l'occurrence d'un évènement mettant en cause la sécurité, à identifier leurs précurseurs afin de mettre en place les défenses nécessaires. Une démarche proactive est constituée de :

- La sensibilisation et la prise des responsabilités des différents acteurs.
- La mise en place des techniques organisationnelles.
- La politique de sécurité : mise en place / réalisation des mesures.
- L'analyse des risques.

Les deux démarches sont donc à prendre en compte mais la démarche de prévention sécuritaire est par définition proactive. Elle touche aux dimensions humaines, juridiques, organisationnelles, économiques et technologiques.

Management de la sécurité des technologies de l'information

Question 7 : Quelle est la place, le rôle, les avantages, les inconvénients et les limites de la fonction d'audit dans une démarche de sécurité informatique ?

Afin d'évaluer le **niveau de sécurité de l'existant**, les différentes cibles de sécurité font l'objet d'un **audit** spécifique qui sera confié à **l'organe de révision**. Ce dernier doit être **externe** et pourra être mandaté par le **conseil d'administration**. Selon la cible, et sur la base d'un **référentiel** préalablement **établi** et **validé** par les commanditaires, on distinguera les points suivants traité par l'audit : financier et organisationnel, sécurité, centres d'exploitation et de développement, réception des applications, ensemble des acteurs du système d'information.

Cependant, la fonction d'auditeur n'est pas toujours bien perçue (pour certaines personnes, l'audit est un peu comme la "police").

Question 8 : Quelle importance accorder à la formation des managers d'entreprise concernant la sécurité de l'information ? Quelle relation existe-t-il entre une démarche de sensibilisation à la sécurité informatique et une charte d'éthique ?

Les managers sont les personnes **responsables** de la bonne marche de l'entreprise. Ils doivent avoir la bonne information au bon moment (**critères de sécurité** : Disponibilité / Intégrité / Confidentialité). Ils connaissent les **actifs** et les **processus** de l'entreprise et par ce fait, doivent donc devenir des **maillons** fort de la **chaine sécuritaire**. Les managers seront aussi responsables des **budgets** alloués pour la sécurité.

Une démarche de **sensibilisation** est importante. Des actions **d'information** et de **formation** sur les **enjeux**, les **risques** et les **mesures** préventives et dissuasives de sécurité sont nécessaires pour éduquer l'ensemble du personnel à adopter une démarche sécurité. Une **charte d'éthique** ou d'utilisation, établie par l'organisation, sera un **outil** de cette sensibilisation. Elle précisera les **droits**, les **devoirs** et la **responsabilité** des employés au regard de l'utilisation des ressources informatiques et télécoms que l'entreprise met à leur disposition.

Question 9 : Identifiez les rôles, les fonctions, les mécanismes, les avantages, les inconvénients et les limites de la signature numérique.

Le système de **chiffrement asymétrique** propose un mécanisme implicite de **signature de messages** qui permet d'authentifier l'émetteur d'un message et d'en vérifier l'intégrité. Une personne chiffre un message avec sa clé privée, si une entité connaissant la clé publique de cette personne peut déchiffrer le message et le lire, cela signifie que le message a bien été créé à l'aide de la clé privée correspondante, la personne étant censée en être la **seule propriétaire**.

Cependant, bien que performant, ce système de signature possède des failles. En effet, rien n'empêche de réutiliser la **signature digitale** d'un message en lieu et place de l'émetteur réel. Par ailleurs, on peut également constituer une **signature numérique** à la place d'un partenaire après lui avoir volé sa clé privée. Augmenter le niveau de sécurité d'un mécanisme de signature électronique est possible en appliquant sur les données une fonction de *hash* et en ayant recours à l'usage d'une infrastructure de gestion des clés offrant des services de certification.

Management de la sécurité des technologies de l'information

Question 10 : Répondre à la question « Qu'est-ce que la sécurité informatique ? », tout en argumentant la phrase suivante « La sécurité informationnelle relève d'une problématique de gestion ».

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

La sécurité informatique a pour **objectifs principaux** de réaliser la confidentialité, l'intégrité, la disponibilité des données et des services des systèmes. Diverses mesures de sécurité permettent de les atteindre. Parmi elles nous pouvons citer : le contrôle d'accès, le chiffrement des données, la gestion des incidents, des erreurs, des dysfonctionnements, des intrusions…

La sécurité est un sujet qui touche tous les composants du système d'information, y compris **l'environnement** et les **utilisateurs**. Assurer la sécurité du système d'information, c'est avant tout conduire une **stratégie globale**, **complète** et **suivie** en s'engageant sur les moyens à mettre en œuvre. Dès la mise en place de solutions de sécurité, une **politique de suivi** doit être initialisée. La définition de **procédures** permet donc, non seulement de **vérifier**, **mesurer** et **superviser** le niveau de sécurité de manière continue, mais autorise également la correction d'éventuelles failles.

La sécurité est de moins en moins une juxtaposition de technologies hétérogènes de sécurité. Elle est dorénavant appréhendée et traitée comme un **processus continu**. Cette vision « processus » met en avant la dimension **managériale** de la sécurité qui vise à l'optimisation et à la rationalisation des investissements, tout en assurant la **pérennité** et **l'efficacité** des solutions de sécurité dans le temps.

La technologie ne suffit pas, elle doit être intégrée dans une démarche de **gestion**. Seule la dimension **managériale** de la sécurité permet de faire face au caractère **dynamique** du risque. La sécurité des systèmes d'information n'est qu'une composante de la sécurité **globale** de l'organisation.