

Notion de risques : Chap.1.b - Introduction à la cybersécurité - Part 1

dimanche 28 janvier 2024 10:42

Chapitre 1 : Introduction à la Cybersécurité

Objectifs

- Connaitre les domaines d'application de la cybersécurité, son positionnement par rapport à la sécurité de l'information et la sécurité informatique
- Impact de la cybersécurité sur les individus, les entreprises et les gouvernements.
- Terminologie : Compléments

A. Introduction et définition.

- La cybersécurité est une partie de la sécurité informatique. Elle est d'une importance capitale pour les sociétés et les états car elle impacte des domaines comme : le domaine de la Donnée, le domaine économique et le domaine de la sécurité nationale.
- Définition de la Cybersécurité :
 - La cybersécurité peut être définie comme la pratique de protéger les systèmes informatiques, les réseaux, les données et les informations contre les menaces numériques telles que les cyberattaques, les piratages, et les intrusions malveillantes.
- Quelques domaines impactés par la cybersécurité :
 - Domaine de la Donnée :
 - **Confidentialité** : La confidentialité en cybersécurité se réfère à la protection des données et des informations sensibles contre l'accès ou la divulgation non autorisés. Cela signifie que seules les personnes ou les entités autorisées ont accès aux données confidentielles.
 - **Intégrité** : L'intégrité concerne la garantie que les données et les informations ne sont pas altérées de manière non autorisée pendant leur stockage, leur traitement ou leur transmission. L'intégrité garantit que les données restent exactes et fiables.
 - **Disponibilité** : La disponibilité fait référence à la capacité à accéder aux données et aux ressources informatiques quand cela est nécessaire. Cela signifie que les systèmes et les données doivent être accessibles et fonctionnels sans interruption.
 - Domaine Économique :
 - Les cyberattaques peuvent causer d'énormes pertes financières aux entreprises et aux gouvernements.
 - Domaine de la Sécurité Nationale :
 - Les infrastructures critiques telles que l'énergie, la santé et la défense dépendent de la cybersécurité pour fonctionner en toute sécurité.
- Sources de Référence (en français) :
 - [\[Cybersécurité - Wikipédia\]\(https://fr.wikipedia.org/wiki/Cybers%C3%A9curit%C3%A9\)](https://fr.wikipedia.org/wiki/Cybers%C3%A9curit%C3%A9) : Pour une définition complète et détaillée de la cybersécurité.

B. Histoire de faire le lien

B.1. Un peu d'histoire...

- La Première Guerre Mondiale et la Tour Eiffel :

Histoire : Pendant la Première Guerre mondiale, les Français utilisaient la Tour Eiffel comme station de surveillance pour capter les messages des Allemands. Cette opération a souligné l'importance du chiffrement dans la communication militaire.

Parallèle en Sécurité de l'Information : Comprendre comment la cybersécurité peut être comparée à la protection des communications militaires pendant la Première Guerre mondiale.

Parallèle en Sécurité Informatique : Cela met en évidence l'importance de chiffrer les données sensibles pour protéger la confidentialité des informations, car tout système non sécurisé peut être vulnérable à l'espionnage.

- La Ligne Maginot

Histoire : La France s'est sentie protégée derrière la Ligne Maginot, une infrastructure de défense solide, mais les Allemands l'ont contournée, montrant les limites de cette approche.

Parallèle en Sécurité Informatique : Examiner comment la stratégie de défense française avec la Ligne Maginot peut être comparée aux pare-feux (firewalls) en sécurité informatique.

Cela souligne l'importance de la diversification des mesures de sécurité, car un seul pare-feu ne peut pas garantir la protection totale contre les attaques. Il faut une approche en couches pour renforcer la sécurité.

- La Machine Enigma ([M332 : Enigma](#))

Histoire : La machine Enigma était un dispositif de cryptage allemand très avancé utilisé pendant la Seconde Guerre mondiale. Les Alliés ont réussi à déchiffrer ses messages.

Parallèle en Sécurité de l'information : Analyser la machine Enigma et son déchiffrement pour comprendre l'importance de la cryptographie en cybersécurité.

Parallèle en Sécurité Informatique : Cela met en évidence l'importance de la cryptographie moderne pour protéger les données sensibles. Tout comme Enigma a été déchiffrée en raison de certaines failles, il est crucial de comprendre les vulnérabilités potentielles de l'algorithme de chiffrement.

- Les Débuts de la Cybersécurité

Les débuts de la cybersécurité remontent aux premiers virus informatiques et au développement d'ARPANET, le précurseur d'Internet.

Les Premiers Virus Informatiques : Les premiers virus informatiques étaient des programmes malveillants conçus pour se propager à travers les ordinateurs en infectant leurs fichiers ou leurs systèmes. Ces virus étaient souvent diffusés via des disquettes partagées et pouvaient causer des dommages aux systèmes en altérant ou en effaçant des données. Les virus informatiques ont souligné la nécessité de protéger les systèmes contre les menaces numériques.

Développement d'ARPANET : L'ARPANET, créé par le département américain de la Défense dans les années 1960, était le précurseur d'Internet. Il s'agissait d'un réseau de communication militaire conçu pour résister aux attaques nucléaires. Le développement d'ARPANET a marqué une étape importante dans l'histoire de la cybersécurité car il a posé les bases de la communication en ligne, tout en soulevant des préoccupations concernant la sécurité des données et des informations sensibles.

Transition d'ARPANET à Internet : La transition d'ARPANET à Internet a eu lieu progressivement, mais une date clé est le 1er janvier 1983, lorsque le protocole TCP/IP a été officiellement adopté. Cela a marqué le début de l'utilisation généralisée du TCP/IP, le protocole fondamental d'Internet tel que nous le connaissons aujourd'hui. Cette transition a eu un impact significatif sur la cybersécurité, car elle a élargi la portée des communications en ligne, nécessitant une protection accrue contre les menaces numériques.

B.2. L'Évolution de la Cybersécurité

- L'évolution de la cybersécurité a vu la transition de la cybercriminalité à la cyberguerre, avec des attaques de plus en plus sophistiquées et des enjeux géopolitiques.

De la Cybercriminalité à la Cyberguerre :

Cybercriminalité : Au début, la principale menace en ligne était la cybercriminalité, impliquant le piratage, le vol d'identité, la fraude en ligne et la diffusion de logiciels malveillants à des fins lucratives.

Espionnage Économique : L'évolution a vu la montée de l'espionnage économique, où des États et des groupes ciblaient des entreprises et des gouvernements pour voler des secrets commerciaux et des informations sensibles.

Cyberguerre : La cyberguerre est un domaine émergent où les États-nations s'engagent dans des opérations offensives et défensives sur Internet, ciblant infrastructures critiques, institutions gouvernementales et militaires, avec des conséquences graves sur la sécurité nationale.

B.3 Sources de Référence (en français)

- [Histoire de la cybersécurité - NordVPN](<https://nordvpn.com/fr/blog/histoire-de-la-cybersecurite/>) : Un article détaillant l'évolution de la cybersécurité.
- [Définition et historique de la cybersécurité | Cairn.info]([Cairn.info](https://shs.cairn.info/recherche?lang=fr&term=cybers%C3%A9curit%C3%A9)) : Ouvrages et sur la cybersécurité : <https://shs.cairn.info/recherche?lang=fr&term=cybers%C3%A9curit%C3%A9>

C. Notion et principes fondamentaux

C.1. Notions essentielles en terme de sécurité

Avant d'approfondir les principes fondamentaux de la cybersécurité, il faut bien comprendre la différence qui réside entre la sécurité de l'information, la sécurité informatique et la cybersécurité. Chaque thème a une portée différente et il convient de donner notre propre définition.

- Sécurité de l'information
 - Définition : La sécurité de l'information vise à protéger toutes les informations d'une organisation, peu importe leur forme (numérique, physique ou verbale). Elle se base sur trois grands principes : la confidentialité (seules les personnes autorisées peuvent accéder aux informations), l'intégrité (les informations doivent rester exactes et complètes), et la disponibilité (les informations doivent être accessibles aux personnes autorisées lorsqu'elles en ont besoin).
 - Objectif : Préserver l'ensemble des données sensibles de l'organisation (données clients, propriété intellectuelle, dossiers financiers, etc.), qu'elles soient stockées en ligne, sur des supports physiques, ou transmises de manière orale.
- Sécurité Informatique
 - Définition : La sécurité informatique est un sous-ensemble de la sécurité de l'information qui se concentre spécifiquement sur la protection des systèmes informatiques (matériel et logiciel) et des réseaux. Elle s'applique aux infrastructures techniques comme les ordinateurs, serveurs, réseaux et bases de données.
 - Objectif : Protéger les informations contre les menaces liées aux technologies de l'information, comme les virus, les logiciels malveillants, les cyberattaques, les pannes matérielles ou logicielles, et les erreurs humaines.
- Cybersécurité
 - Définition : La cybersécurité est un sous-domaine de la sécurité informatique qui se concentre sur la protection des systèmes connectés, des réseaux et des données contre les cybermenaces, c'est-à-dire les attaques d'origine externe, comme le piratage, le phishing, le ransomware et d'autres formes de cybercriminalité. Elle intègre également les aspects humains (formation, sensibilisation) et la gestion des risques liés aux

comportements des utilisateurs.

- Objectif : Prévenir, détecter et répondre aux menaces provenant de l'extérieur et de l'intérieur des réseaux numériques de l'entreprise. Elle couvre donc les cyber-risques spécifiques à l'ère de la connectivité et de l'internet.

C.2. Notions essentielles en terme de hiérarchie

En terme de hiérarchie de sécurité, la cybersécurité est donc un sous-ensemble de la sécurité informatique qui elle-même est un sous-ensemble de la sécurité de l'information.

A la croisée des métiers de l'entreprise, on trouve des noms comme actifs gérés (Assets). La sécurité de l'information va donc s'intéresser à la protection des actifs (Assets) tout comme la cybersécurité mais à des menaces légèrement différentes.

Classification des Actifs en Sécurité de l'Information et Cybersécurité:

Catégorie d'Actifs	Sécurité de l'Information	Cybersécurité	Intersection (SI & Cyber)
Informations et Données	<ul style="list-style-type: none"> - Documents papier, archives - Données clients et financières - Rapports et contrats 	<ul style="list-style-type: none"> - Données stockées sur les serveurs - Données en transit dans les réseaux - Bases de données 	<ul style="list-style-type: none"> - Données clients (sensible pour les deux) - Confidentialité des informations critiques
Actifs Techniques	<ul style="list-style-type: none"> - Infrastructures physiques (locaux, centres de données) - Equipements d'archivage 	<ul style="list-style-type: none"> - Routeurs, serveurs, firewalls, IDS/IPS - Systèmes connectés et virtualisés - Applications web 	<ul style="list-style-type: none"> - Systèmes de stockage - Dispositifs de sécurité (firewalls, IDS)
Personnes et Connaissances	<ul style="list-style-type: none"> - Personnes clés avec savoir-faire stratégique - Connaissances organisationnelles 	<ul style="list-style-type: none"> - Administrateurs réseau - Équipe SOC (Security Operations Center) - Comptes d'utilisateurs 	<ul style="list-style-type: none"> - Gestion des accès - Sensibilisation à la sécurité
Processus et Services	<ul style="list-style-type: none"> - Processus RH - Plans de continuité d'activité - Politiques de confidentialité 	<ul style="list-style-type: none"> - Surveillance des réseaux - Réponse aux incidents - Gestion des logs 	<ul style="list-style-type: none"> - Gestion des incidents - Plan de reprise après sinistre
Logiciels et Applications	<ul style="list-style-type: none"> - Applications métiers internes (gestion RH, comptabilité) - Logiciels non connectés 	<ul style="list-style-type: none"> - Logiciels de sécurité (antivirus, EDR) - Applications hébergées en cloud 	<ul style="list-style-type: none"> - Plateformes de gestion documentaire - Application de gestion de vulnérabilités

C.3. Cybersécurité : 3 principes fondamentaux (CIF) et d'autres principes essentiels

En plus de ces trois principes fondamentaux (CIF), d'autres propriétés sont également essentielles dans le domaine de la cybersécurité :

- 3 principes fondamentaux (CIF)
 - **Confidentialité** : Assure que les informations ne sont accessibles qu'aux personnes autorisées à les voir, empêchant l'accès non autorisé aux données sensibles.
 - **Intégrité** : Garantit que les informations sont exactes et complètes, et n'ont pas été modifiées de manière non autorisée, assurant ainsi la fiabilité des données.
 - **Disponibilité** : Assure que les informations et les ressources sont accessibles aux

utilisateurs autorisés quand ils en ont besoin, ce qui est crucial pour le fonctionnement continu des opérations.

- Autres principes essentiels :
 - **Authenticité** : Vérifie que les utilisateurs sont bien ceux qu'ils prétendent être et que les informations proviennent de sources fiables, souvent à travers des mécanismes d'authentification.
 - **Responsabilité** (Accountability) : Assure que toutes les actions effectuées sur un système peuvent être attribuées à un utilisateur individuel, permettant ainsi de tracer les activités et d'identifier les responsables en cas d'incident de sécurité.
 - **Non-répudiation** : Empêche qu'un individu ou une entité nie avoir effectué une action spécifique, en fournissant une preuve irréfutable de l'acte, souvent à travers des mécanismes cryptographiques comme les signatures numériques.

Pour assurer la **confidentialité** dans le domaine de la cybersécurité, plusieurs moyens et pratiques peuvent être mis en œuvre :

1. **Chiffrement** : Utiliser des technologies de chiffrement pour protéger les données en transit (comme le SSL/TLS pour les communications web sécurisées) et les données au repos (comme le chiffrement des disques durs ou des bases de données). Le chiffrement transforme les données en un format illisible sans la clé de déchiffrement appropriée.
2. **Contrôle d'accès** : Mettre en place des politiques et des systèmes de contrôle d'accès stricts pour s'assurer que seules les personnes autorisées peuvent accéder aux informations sensibles. Cela inclut l'authentification des utilisateurs par des mots de passe, des jetons, la biométrie, ou l'authentification multi-facteurs (MFA).
3. **Gestion des identités et des accès (IAM)** : Utiliser des solutions IAM pour gérer les identités des utilisateurs et contrôler leurs accès aux ressources en fonction de leur rôle, de leur responsabilité et de leur contexte opérationnel.
4. **Réseaux privés virtuels (VPN)** : Utiliser des VPN pour créer des connexions sécurisées et chiffrées sur Internet, permettant aux employés d'accéder de manière sécurisée aux ressources de l'entreprise à distance.
5. **Politiques de sécurité des données** : Établir et appliquer des politiques claires concernant le stockage, la transmission et le partage des données pour garantir que les informations sensibles sont manipulées de manière sécurisée.
6. **Masquage des données et pseudo anonymisation** : Appliquer des techniques pour masquer ou remplacer les informations sensibles par des alias ou des données non sensibles, en particulier dans les environnements de développement et de test.
7. **Gestion des clés de chiffrement** : Mettre en place des procédures sécurisées pour la gestion du cycle de vie des clés de chiffrement, y compris leur création, distribution, stockage, rotation et destruction.
8. **Sécurité des terminaux** : Assurer la sécurité des dispositifs utilisateurs finaux par des logiciels antivirus, des pare-feu, et d'autres mesures de protection pour prévenir les fuites de données.
9. **Formation et sensibilisation des utilisateurs** : Éduquer régulièrement les employés sur les meilleures pratiques de sécurité, les menaces potentielles et les procédures à suivre pour protéger les informations confidentielles.
10. **Accords de confidentialité** : Faire signer des accords de non-divulgation (NDA) aux employés, aux sous-traitants et aux partenaires pour les sensibiliser juridiquement à l'importance de la confidentialité des données.

Pour assurer l'**intégrité des données et des systèmes en cybersécurité**, plusieurs stratégies et outils doivent être mis en place :

1. **Contrôles d'accès** : Limiter l'accès aux données et aux systèmes uniquement aux utilisateurs autorisés pour prévenir les modifications non autorisées. Utiliser des systèmes de gestion des identités et des accès pour contrôler strictement qui peut modifier les informations.
2. **Hachage cryptographique** : Utiliser des fonctions de hachage pour créer une empreinte numérique unique des données. Toute modification des données entraînera un changement de l'empreinte, révélant ainsi toute altération.
3. **Signature numérique** : Appliquer des signatures numériques aux documents et aux logiciels pour vérifier l'authenticité et l'intégrité des données. Les signatures numériques utilisent la cryptographie à clé publique pour prouver que les données n'ont pas été modifiées depuis leur signature.
4. **Gestion des versions et des correctifs** : Maintenir les systèmes et les applications à jour avec les derniers correctifs de sécurité pour protéger contre les vulnérabilités connues qui pourraient être exploitées pour compromettre l'intégrité des données.
5. **Sauvegardes régulières** : Effectuer des sauvegardes régulières et sécurisées des données importantes pour pouvoir les restaurer en cas de corruption ou de perte.
6. **Vérification de l'intégrité des fichiers** : Utiliser des outils de vérification de l'intégrité pour surveiller les changements inattendus ou non autorisés dans les fichiers système et les configurations critiques.
7. **Sécurité des terminaux** : Protéger les dispositifs utilisateurs finaux avec des solutions antivirus et antimalware pour prévenir les infections qui pourraient altérer les données ou les systèmes.
8. **Réseaux sécurisés** : Protéger les communications de données à l'aide de protocoles sécurisés comme SSL/TLS pour prévenir les interceptions et les modifications des données en transit.
9. **Politiques de sécurité des données** : Établir des politiques claires pour la manipulation, le stockage et le transfert des données afin de garantir que les pratiques de sécurité sont suivies pour maintenir l'intégrité des données.
10. **Formation et sensibilisation** : Éduquer les employés sur l'importance de l'intégrité des données et les former sur les meilleures pratiques pour éviter les erreurs humaines qui pourraient compromettre l'intégrité.

La **disponibilité** garantit que les systèmes, les données et les services informatiques sont accessibles et fonctionnent de manière fiable lorsque nécessaire. Voici quelques moyens à mettre en œuvre pour assurer la disponibilité des systèmes et des services informatiques :

1. **Plan de reprise d'activité (PRA) et plan de continuité d'activité (PCA)** :
 - Élaborer des plans solides de reprise d'activité et de continuité d'activité pour faire face aux pannes matérielles, aux catastrophes naturelles, aux cyberattaques et à d'autres événements susceptibles d'affecter la disponibilité des systèmes.
2. **Sauvegarde régulière des données** :
 - Mettre en place des procédures de sauvegarde régulières pour prévenir la perte de données en cas de panne ou d'incident. Assurez-vous que les sauvegardes sont stockées de manière sécurisée et testez régulièrement leur restauration.

3. **Redondance :**

- Utiliser la redondance pour garantir la disponibilité des systèmes. Cela peut inclure la duplication de matériels critiques, la mise en place de clusters ou de systèmes de basculement pour garantir la continuité en cas de défaillance d'un composant.

4. **Surveillance proactive :**

- Mettre en place un système de surveillance proactif pour surveiller en temps réel l'état des systèmes, des réseaux et des services. Les alertes doivent être générées en cas de problèmes ou d'anomalies.

5. **Gestion des vulnérabilités :**

- Assurez-vous de suivre et de corriger rapidement les vulnérabilités de sécurité dans vos systèmes et vos logiciels pour éviter les attaques susceptibles d'impact la disponibilité.

6. **Protection contre les attaques DDoS :**

- Utilisez des solutions de protection contre les attaques par déni de service distribué (DDoS) pour minimiser l'impact des attaques visant à saturer les ressources du réseau et à rendre les services indisponibles.

7. **Sécurité physique :**

- Protégez vos équipements informatiques contre les dommages physiques, les vols et les intrusions. Cela peut inclure l'utilisation de salles de serveurs sécurisées et de contrôles d'accès stricts.

8. **Formation du personnel :**

- Formez votre personnel pour qu'il soit conscient des menaces potentielles et des bonnes pratiques en matière de sécurité, ce qui contribuera à prévenir les erreurs humaines pouvant entraîner des pannes.

9. **Plan de gestion des incidents :**

- Mettez en place un plan de gestion des incidents qui inclut des procédures spécifiques pour réagir rapidement aux incidents de sécurité susceptibles d'impact la disponibilité.

10. **Tests de disponibilité :**

- Effectuez régulièrement des tests de disponibilité pour évaluer la capacité de votre infrastructure à résister à divers scénarios de pannes ou d'attaques.