INTRODUCTION

Importance de la cybersécurité

Enjeux de la sécurité des SI

Le mot « cybersécurité », popularisé dans les années 1990, désigne le rôle de l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les actifs informatiques matériels et immatériels des organisations. La cybersécurité fait donc appel à toutes les techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

En raison de la numérisation progressive de la société moderne, la protection des données a acquis une importance fondamentale pour le bon fonctionnement de toute entreprise et collectivité. Une atteinte à la sécurité des données de ces organisations peut entraîner des conséquences multiples : interruption des processus métier, pertes financières, sanctions juridiques, atteinte à l'image.

La cybersécurité s'est également invitée dans la sphère privée : la plupart des informations qui nous sont précieuses sont stockées sous forme numérique : informations bancaires, messages électroniques, carnets d'adresses, documents administratifs, photos et vidéos. Une négligence dans la protection de ces informations est synonyme d'ennuis en tout genre.

Nos données personnelles sont parfois désignées sous le nom d'« or numérique », car elles sont au centre d'intérêts colossaux, notamment :

- Financiers : ciblage publicitaire, marketing comportemental, revente d'informations, actions illégales (par exemple usurpation d'identité, vol de secrets, vengeance).
- Politiques : manipulation de l'opinion publique, endoctrinement, surveillance de masse, espionnage.

Le règlement général sur la protection des données (RGPD) a été mis en place à l'échelle de l'Union européenne comme instrument juridique de défense des données à caractère personnel ; nous y reviendrons dans la suite du cours.

Panorama des menaces cyber

L'actualité regorge malheureusement de récits de cyberattaques ; aucune structure n'est épargnée : collectivités locales, établissements de santé, entreprises du CAC 40, entreprises de services du numérique (ESN), ETI, PME et TPE.

Selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI)[1], les sources des cyberattaques peuvent être regroupées en trois grandes catégories :

1. Nuisances quotidiennes : cette catégorie englobe des actions automatisées menées par une multitude d'acteurs, malveillants ou non, qui peuvent perturber le fonctionnement des systèmes d'information. Parmi ces nuisances figurent les scans de ports, les campagnes de spams et les tentatives massives d'exploitation de vulnérabilités.
2. Menaces cybercriminelles : principalement motivées par des intérêts financiers, ces attaques visent à générer des profits à travers des actes malveillants sur les systèmes d'information. Il existe un véritable marché autour de cela, pouvant inclure le vol de données sensibles ou personnelles pour revente, le rançonnage par chiffrement (*ransomware*), ou encore les attaques par déni de service (DDoS).
3. Menaces étatiques : opérées par des attaquants soutenus par des États et particulièrement sophistiquées, ces attaques ciblent précisément des entités afin de récolter des informations stratégiques, technologiques et économiques, ou encore de réaliser des actions de sabotage.

1. *https://cyber.gouv.fr/*

Chapitre 1

CONCEPTS DE BASE

Critères D, I, C, P

Définitions

L'objectif des disciplines regroupées sous le nom de cybersécurité est de protéger les besoins en sécurité de l'information : disponibilité, intégrité, confidentialité et preuve.

Pour bien comprendre cela, analysons les termes introduits :

- **Information** : il s'agit d'un concept clé, qui a fait l'objet d'intenses études théoriques, notamment à partir de la moitié du XX^{e} siècle avec les travaux de Claude Shannon. La norme ISO 27000, référentiel international des termes et définitions autour de la sécurité, fait pourtant l'impasse sur cette notion. Dans le contexte de cet écrit, désignons l'information comme « élément de connaissance susceptible d'être représenté à l'aide de conventions pour être conservé, traité ou communiqué ». De façon plus pragmatique, cela indique le patrimoine de connaissances et savoir-faire d'une entreprise, qui peuvent être

stockés sous forme de données électroniques, papier, ou même faire l'objet d'une transmission exclusivement orale.

- **Disponibilité** : propriété d'être accessible et utilisable à la demande par une entité autorisée. S'il n'est pas immédiat d'associer ce critère à la sécurité, il est pourtant essentiel, notamment si on pense à des données de santé, dont l'indisponibilité en situation d'urgence peut potentiellement mener au décès d'un patient.
- **Intégrité** : propriété d'exactitude et de complétude. L'intégrité est touchée en cas d'altération illicite des données.
- **Confidentialité** : propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés. Ce critère est probablement le plus intuitif des quatre.
- **Preuve** : propriété permettant de retrouver, avec une confiance suffisante, les circonstances dans lesquelles l'information est traitée. Cette propriété englobe la traçabilité des actions menées, l'authentification des utilisateurs et l'imputabilité du responsable de l'action effectuée.

Cas de violation

Pour mieux apprécier les besoins en sécurité, aussi appelés « critères de sécurité », passons en revue des cas de violation :

Disponibilité :

- Attaque par déni de service, à travers laquelle le système ciblé n'est plus en mesure de répondre aux requêtes légitimes. Le cas le plus classique concerne un service web rendu inutilisable, bombardé par du trafic malveillant, souvent généré par un ensemble d'ordinateurs, parfois plusieurs dizaines de milliers, contrôlés par l'attaquant (botnet).
- Suppression d'informations, résultant d'une action hostile délibérée ou juste d'une erreur humaine.
- Incident hardware ou software qui met un système hors service, le rendant incapable de traiter les requêtes des utilisateurs.
- Mauvaise configuration des droits d'accès, qui prive les utilisateurs légitimes d'un accès à l'information.
- Infection par un virus de type *cryptolocker* (rançongiciel), qui chiffre les données les rendant inutilisables et demande souvent une rançon pour la transmission d'une clé de déchiffrement.
- Défaillance du processus de sauvegarde et de restauration, avec comme résultat l'impossibilité de récupérer les informations qu'on croyait préservées.

RETOUR D'EXPÉRIENCE ET RÉFLEXIONS PRATIQUES

- C'est une mauvaise idée de « bricoler » un algorithme de chiffrement ou de hachage maison : il faut utiliser des algorithmes éprouvés (cf. principe de Kerckhoffs[4]).
- Quand il s'agit de la protection des secrets et des clés de chiffrement, il faut se mettre dans un état d'esprit presque paranoïaque et réfléchir à tous les risques de fuite. Les solutions hardware basées sur des HSM offrent un niveau de sécurité plus élevé que les solutions software, mais sont coûteuses et demandent la mise en place de processus de gestion lourds, notamment des cérémonies des clés.
- Il ne faut jamais transmettre par mail des informations sensibles en clair, ni transmettre par mail un fichier chiffré avec le mot de passe dans le corps du mail.
- N'hésitez pas à utiliser le chiffrement pour protéger vos informations personnelles sensibles, par exemple des numérisations de documents d'identité. Un logiciel comme Cryptomator peut être utile à cet égard.

4. https://fr.wikipedia.org/wiki/Principe_de_Kerckhoffs

Chapitre 2

CADRE LÉGAL ET RÉGLEMENTAIRE

Introduction

Avec l'essor des menaces numériques et l'augmentation des données sensibles circulant sur les réseaux, les organisations doivent répondre à des exigences de conformité toujours plus complexes.

Il existe une multitude de référentiels, normes et réglementations couvrant des secteurs variés. Ce chapitre se concentre sur quatre référentiels clés, qui illustrent les principales approches de sécurisation d'un système d'information :

- Règlement général sur la protection des données[1] (RGPD, GDPR en anglais), le texte européen de référence en matière de protection des données à caractère personnel.

1. https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR