Chapitre 2 : Le cube magique de la cybersécurité

On appelle magiciens les professionnels de la cybersécurité qui veillent sur le cyberespace. À l'instar des magiciens des contes fantastiques, les cybermagiciens ont pour mission de faire régner le bien et de protéger les autres. John McCumber peut être considéré comme l'un des premiers magiciens de la cybersécurité. Il a mis au point un modèle, appelé Cube de McCumber, utilisé par les magiciens de la cybersécurité pour protéger le cyberespace. Le Cube de McCumber ressemble à un Rubik's Cube.

La première dimension du cube magique de la cybersécurité comprend les trois principes de la sécurité de l'information, que les professionnels de la cybersécurité désignent sous le nom de « Triade CID ». La deuxième dimension identifie les trois états des informations ou des données. La troisième dimension du cube identifie les « pouvoirs magiques » qui assurent la protection du cyberespace. Il s'agit, en fait, des trois catégories de protections en matière de cybersécurité.

Ce chapitre présente également le modèle de cybersécurité ISO. Ce modèle représente un cadre international qui vise à standardiser la gestion des systèmes d'informations.

# Les principes de la sécurité

La première dimension du cube magique de la cybersécurité identifie les objectifs à protéger sur Internet. Les objectifs identifiés dans la première dimension constituent les principes fondateurs du monde de la cybersécurité. Ces trois principes sont la confidentialité, l'intégrité et la disponibilité. Ces principes permettent au magicien de la cybersécurité de cibler ses efforts et d'établir des priorités dans les mesures à prendre pour assurer la protection de ses ressources sur Internet.

Le principe de confidentialité consiste à empêcher la divulgation d'informations à des personnes, des ressources ou des processus non autorisés. L'intégrité représente l'exactitude, la cohérence et la fiabilité des données. Enfin, la disponibilité garantit l'accès aux informations lorsque les utilisateurs autorisés en ont besoin. Souvenez-vous de ses principes avec les initiales CID.

# Dispositifs de protection en cybersécurité

La troisième dimension du cube magique de la cybersécurité définit les types de pouvoirs auxquels un magicien de la cybersécurité peut avoir recours pour protéger le cyberespace. Les professionnels de la cybersécurité doivent utiliser tous les pouvoirs dont ils disposent pour protéger les données du cyberespace.

Le cube magique identifie les trois types de pouvoirs, ou armes, utilisés pour assurer leur protection. Le premier type de pouvoir comprend les technologies, les appareils et les produits disponibles pour protéger les systèmes d'information et repousser les cybercriminels. Les professionnels de la cybersécurité sont connus pour maîtriser les outils technologiques mis à leur disposition. Cependant, John McCumber leur rappelle que les outils technologiques seuls ne suffisent pas pour mettre en échec les cybercriminels. En effet, ils doivent également ériger de solides défenses en développant des politiques, des procédures et des directives permettant aux citoyens du cyberespace de rester protégés et de respecter de bonnes pratiques d'utilisation. Enfin, comme c'est le cas dans le monde de la magie, les citoyens du cyberespace doivent en apprendre toujours plus sur leur monde et sur les dangers qui le menacent. Ils doivent être assoiffés de connaissances, et établir une culture d'apprentissage et de prise de conscience.

# Le principe de confidentialité

Le principe confidentialité consiste à empêcher la divulgation d'informations à des personnes, des ressources ou des processus non autorisés. Une autre expression utilisée pour la confidentialité est le respect de la vie privée. Au sein des entreprises, l'accès est limité afin de s'assurer que seuls les opérateurs autorisés peuvent utiliser les données ou d'autres ressources réseau. Par exemple, un programmeur ne doit pas avoir accès aux informations personnelles de tous les employés.

Les entreprises doivent former leurs collaborateurs sur les bonnes pratiques permettant de préserver la confidentialité des informations sensibles afin de se protéger eux-mêmes et leur entreprise contre des attaques. Diverses méthodes permettent de garantir la confidentialité des données, notamment le chiffrement des données, l'authentification et le contrôle d'accès.

Protection de la vie privée

Les entreprises collectent de grandes quantités de données dont la majeure partie n'est pas sensible, car elles sont accessibles publiquement, comme les noms et les numéros de téléphone. Toutefois, parmi les données collectées, d'autres peuvent être sensibles. Les informations sensibles sont protégées contre les accès non autorisés afin de protéger un individu ou une entreprise. Il existe trois types d'informations sensibles :

* Celles qui permettent d'identifier une personne. La Figure 2 répertorie cette catégorie de données.
* On parle d'informations commerciales pour désigner toutes les informations qui présentent un risque pour l'entreprise si elles sont divulguées au public ou à un concurrent. La Figure 3 répertorie cette catégorie de données.
* Les informations classifiées sont des informations qui appartiennent à un organisme gouvernemental et qui sont classées en fonction de leur niveau de sensibilité. La Figure 4 répertorie cette catégorie de données.

Contrôle d'accès

Le contrôle d'accès définit plusieurs dispositifs de protection conçus pour interdire les accès non autorisés à un ordinateur, un réseau, une base de données ou d'autres ressources de données. Les concepts désignés par AAA correspondent à trois services de sécurité : l'authentification, l'autorisation et la journalisation (Authentification,Authorization, Accounting). Ces services fournissent le cadre principal pour le contrôle d'accès.

Le premier « A » désigne l'authentification. ***L'authentification*** vérifie l'identité d'un utilisateur afin d'empêcher tout accès non autorisé. Les utilisateurs prouvent leur identité au moyen d'un nom d'utilisateur ou d'un ID. Ils doivent, en outre, confirmer leur identité en fournissant l'un des éléments suivants, comme illustré à la Figure 1 :

* Un élément qu'ils connaissent (comme un mot de passe)
* Une chose qu'ils possèdent (comme un jeton ou une carte)
* Un élément qui les caractérise (comme une empreinte digitale)

Par exemple, pour retirer de l'argent à un guichet automatique, vous avez besoin de votre carte de crédit (c'est-à-dire une chose que vous possédez) et vous devez connaître votre code secret. Il s'agit également d'un exemple d'authentification multifacteur, en ce sens qu'elle nécessite plusieurs types d'authentification. La forme d'authentification la plus répandue est l'utilisation de mots de passe.

***Les services d'autorisation***identifient les ressources auxquelles les utilisateurs peuvent accéder, ainsi que les opérations qu'ils peuvent effectuer (comme le montre la Figure 2). Pour ce faire, certains systèmes utilisent une liste de contrôle d'accès ou ACL. Cette liste détermine si, une fois authentifié, un utilisateur dispose de certains privilèges d'accès. Le fait que vous puissiez vous connecter au réseau d'entreprise ne signifie pas nécessairement que vous êtes autorisé à utiliser l'imprimante couleur haut débit. L'autorisation permet également de contrôler les périodes au cours desquelles un utilisateur peut accéder à une ressource spécifique. Par exemple, il est possible que les employés puissent accéder à une base de données des ventes pendant les heures de travail, mais que cet accès leur soit interdit en dehors des heures de bureau.

***La journalisation***consiste à suivre les actions des utilisateurs : les éléments auxquels ils accèdent, le temps d'accès aux ressources, les modifications effectuées. Une banque, par exemple, opère ce type de contrôle pour chaque compte client. Un audit de ce système peut révéler l'heure et le montant de toutes les transactions, ainsi que l'employé ou le système responsable de leur exécution. Dans le domaine de la cybersécurité, les services de journalisation adoptent un fonctionnement identique. Le système effectue le suivi de chaque transaction de données et fournit des résultats d'audit. Un administrateur peut configurer des politiques informatiques, comme illustré à la figure 3, pour activer l'audit du système.

Le concept désigné par les initiales anglaises AAA (Authentication, Authorization, Accounting) est semblable à l'utilisation d'une carte de crédit, comme le montre la Figure 4. La carte de crédit identifie qui est autorisé à l'utiliser, combien cet utilisateur peut dépenser et tient une comptabilité des achats de l'utilisateur.

Dans le domaine de la cybersécurité, le suivi et le contrôle s'effectuent en temps réel. Des sites web, tels que Norse, montrent les attaques en temps réel sur la base des données collectées dans le cadre d'un système de suivi ou de journalisation. Cliquez [ici](http://map.norsecorp.com/) pour consulter le site web de suivi en temps réel Norse.

# Lois et responsabilité

Les notions de confidentialité et le respect de la vie privée peuvent sembler similaires, mais elles désignent des réalités juridiques distinctes. La majorité des données privées est confidentielle, mais toutes les données confidentielles ne relèvent pas de la sphère privée. L'accès aux informations confidentielles est permis après avoir confirmé que l'utilisateur dispose des autorisations nécessaires. Les institutions financières, les hôpitaux, les professionnels de santé, les cabinets d'avocats et les entreprises traitent des informations confidentielles. Toute information confidentielle relève d'un statut non public. Préserver la confidentialité constitue un devoir de nature éthique.

Le respect des informations privées s'attache à l'utilisation des données. Lorsque des entreprises collectent des informations fournies par leurs clients ou leurs collaborateurs, elles doivent limiter l'utilisation de ces données à l'usage prévu. La plupart des entreprises demandent à leurs clients ou à leurs collaborateurs de signer un formulaire les autorisant à utiliser ces données.

Toutes les lois répertoriées dans cette figure comportent une disposition relative au respect de la vie privée, en commençant par les lois des États-Unis dans la Figure 1. La Figure 2 présente un échantillonnage des efforts déployés sur le plan international. La plupart de ces lois ont été promulguées en réponse à la croissance considérable du nombre de données collectées.

Le nombre croissant des lois en matière de confidentialité fait peser un lourd fardeau sur les entreprises qui collectent et analysent des données. Les politiques constituent, pour les entreprises, le moyen idéal pour s'y conformer. Elles leur permettent en effet d'appliquer des règles, des procédures et des processus spécifiques qui balisent la collecte, le stockage et le partage de données.

# Principe de l'intégrité des données

L'intégrité représente l'exactitude, la cohérence et la fiabilité des données pendant tout leur cycle de vie. Un autre terme utilisé pour l'intégrité est la qualité. Les données font l'objet de nombreuses opérations telles que la capture, le stockage, la récupération, la mise à jour et le transfert. Cependant, elles ne doivent, à aucun moment, être altérées par des entités non autorisées.

Les méthodes utilisées pour assurer l'intégrité des données comprennent le calcul de hashs, les contrôles de validité des données et les contrôles d'accès. Les systèmes d'intégrité des données peuvent inclure une ou plusieurs des méthodes répertoriées ci-dessus.

# Importance de l'intégrité des données

L'intégrité des données est une composante fondamentale de la sécurité de l'information. L'importance de l'intégrité des données varie selon l'utilisation qu'une entreprise fait de ces données. Par exemple, Facebook ne vérifie pas les données publiées par un utilisateur sur son profil. Une banque ou une société financière attribuent une importance plus élevée à l'intégrité de leurs données que Facebook. Les transactions et les comptes clients doivent être exacts. Dans un établissement de santé, l'intégrité des données est une question de vie ou de mort ! Les informations de prescription ne tolèrent aucune approximation.

La protection de l'intégrité des données représente un défi permanent pour la plupart des entreprises. La perte de l'intégrité des données peut rendre des ressources de données entières non fiables, voire inutilisables.

# Vérification de l'intégrité

Une vérification de l'intégrité permet de mesurer la cohérence d'un ensemble de données (un fichier, une image ou un enregistrement). Le processus de vérification de l'intégrité consiste à exécuter une opération appelée fonction de hash pour enregistrer l'état des données à un moment précis. Le processus de vérification de l'intégrité utilise cet instantané pour s'assurer que les données ne subissent aucune altération.

Une somme de contrôle est un exemple de fonction hash. Elle vérifie l'intégrité des fichiers, ou des chaînes de caractères, avant et après leur transfert d'un appareil vers un autre via un réseau local ou Internet. Les sommes de contrôle convertissent simplement chaque élément d'information en une valeur et calculent le total. Pour tester l'intégrité des données, le système de réception répète cette opération. Si les deux sommes sont égales, les données sont valides (Figure 1). Dans le cas contraire, une modification s'est produite à un moment donné (Figure 2).

Les fonctions hash courantes sont MD5, SHA-1, SHA-256 et SHA-512. Elles utilisent des algorithmes mathématiques complexes. La valeur hachée est simplement présente pour comparaison. Par exemple, après avoir téléchargé un fichier, l'utilisateur peut vérifier son intégrité en comparant les valeurs de hash de la source avec celles générées par un calculateur hash, quel qu'il soit.

Les entreprises ont recours au contrôle de version pour éviter toute modification accidentelle de la part des utilisateurs autorisés. Un même objet ne peut pas être mis à jour par deux utilisateurs. Les objets peuvent être des fichiers, des enregistrements de base de données ou encore des transactions. Par exemple, le premier utilisateur à ouvrir un document est autorisé à le modifier ; le deuxième dispose, lui, d'une version en lecture seule.

L'exécution rigoureuse de sauvegardes permet de préserver l'intégrité des données en cas de corruption de ces dernières. L'entreprise doit vérifier sa procédure de sauvegarde pour en garantir l'intégrité avant une perte de données.

L'autorisation détermine les personnes autorisées à accéder aux ressources d'une entreprise en fonction de leurs besoins. Par exemple, les autorisations de fichiers et les contrôles d'accès d'utilisateur font en sorte que seuls certains utilisateurs peuvent modifier les données. Un administrateur peut définir les autorisations d'un fichier en lecture seule. Par conséquent, un utilisateur qui y accède ne pourra y apporter aucune modification.

# Le principe de disponibilité

On appelle disponibilité des données le principe selon lequel il est nécessaire d'assurer une disponibilité en continu des systèmes et services d'information. Certains dysfonctionnements et attaques peuvent empêcher l'accès aux systèmes et services d'information. Ainsi, pirater le site web d'un concurrent pour le rendre indisponible peut être bénéfique à une entité rivale. Ces attaques dites de déni de service (DoS) menacent la disponibilité du système et empêchent les utilisateurs légitimes d'accéder aux informations et de les exploiter quand ils en ont besoin.

Plusieurs méthodes existent pour garantir la disponibilité, notamment la redondance du système, les sauvegardes système, la résilience renforcée du système, la maintenance des équipements, la mise à jour des systèmes d'exploitation et des logiciels et l'élaboration de plans de reprise après un incident.