Chapitre 1 : Cybersécurité - Un monde de magiciens, de héros et de criminels

Pendant les années 1960, la plupart des hackers étaient des amateurs d'informatique, des programmeurs et des étudiants. À l'origine, le terme **hacker** décrivait des individus ayant des compétences avancées en programmation. Les hackers utilisaient ces compétences en programmation pour tester les limites et les capacités des premiers systèmes. Ces hackers de la première heure étaient également impliqués dans le développement des tout premiers jeux informatiques. La plupart de ces jeux avaient pour thématique les magiciens et la magie.

À mesure que la culture du piratage a évolué, la lexicologie de ces jeux a été de plus en plus présente. Même le monde extérieur commençait à utiliser l'image de puissants magiciens pour faire référence à cette culture peu connue du piratage. Des livres tels que *« Les sorciers du Net : les origines de l'Internet »,* publié en 1996, n'ont fait qu'entretenir le mystère autour de la culture du piratage. L'image et la lexicologie sont restées. Aujourd'hui, de nombreux groupes de piratage ont adopté cette imagerie. L'un des groupes de hackers les plus tristement célèbres se fait appeler Legion of Doom. Pour comprendre les criminels du monde virtuel et leurs motivations, il est important de comprendre la cyberculture.

Sun Tzu était un philosophe et guerrier chinois au 6e siècle avant JC. Sun Tzu a écrit un livre intitulé *« L'art de la guerre ».*Ce classique de la littérature présente différentes stratégies pour vaincre l'ennemi. Ce livre a servi de référence aux tacticiens à travers les âges.

L'un des principes directeurs de Sun Tzu était l'importance de connaître son adversaire. Il faisait certes référence à la guerre, mais une bonne partie de ses conseils peuvent être appliqués à d'autres aspects du quotidien, notamment les challenges de la cybersécurité. Dans ce chapitre, nous commençons par expliquer la structure du monde de la cybersécurité et les raisons pour lesquelles il continue à se développer.

Dans ce chapitre, nous traitons également du rôle des cybercriminels et de leurs motivations. Enfin, dans ce chapitre, nous expliquons comment devenir un spécialiste de la cybersécurité. Ces cyberhéros mettent en échec les cybercriminels qui menacent le monde virtuel.

# Présentation des royaumes

Le monde virtuel se compose de nombreux groupes de données. Les groupes capables de collecter et d'utiliser des quantités massives de données gagnent en pouvoir et en influence. Ces données peuvent se présenter sous forme de chiffres, d'images, de vidéos, de fichiers audio ou tout autre type de données pouvant être numérisé. Ces groupes peuvent potentiellement être si puissants qu'ils fonctionnent comme s'ils étaient des royaumes. Les entreprises comme Google, Facebook et LinkedIn peuvent être considérées comme les châteaux de données du royaume. Si l'on pousse plus loin l'analogie, les personnes qui travaillent dans ces entreprises numériques peuvent être considérées comme des cybermagiciens.

# Les châteaux du monde virtuel

Les cybermagiciens de Google ont créé l'un des premiers châteaux du royaume virtuel, mais aussi l'un des plus puissants. Des milliards de personnes utilisent Google tous les jours pour leurs recherches sur Internet. Google a sans doute créé le plus grand réseau mondial de collecte de données. Google développe Android, les systèmes d'exploitation installés sur plus de 80 % des terminaux mobiles connectés à Internet. Sur chaque appareil, les utilisateurs doivent créer des comptes Google pour enregistrer leurs favoris et leurs informations de compte, stocker les résultats de recherche et même localiser l'appareil. Cliquez [ici](https://www.google.com/intl/en/about/products/) pour voir quelques-uns des nombreux services actuellement proposés par Google. Facebook est un autre château très puissant dans le royaume virtuel. Chez Facebook, les cybermagiciens ont fait en sorte que chaque jour des personnes créent des comptes pour communiquer avec leur famille et leurs amis. Ce faisant, ils divulguent volontairement une grande quantité de données personnelles. Les magiciens de Facebook ont construit un immense château de données permettant aux personnes de se connecter d'une manière auparavant inimaginable. Facebook influence quotidiennement des millions de vies et permet aux entreprises et aux organisations de communiquer de manière plus personnelle et plus ciblée avec ces personnes.

LinkedIn est un autre château de données du royaume virtuel. Les cybermagiciens de LinkedIn ont fait en sorte que leurs membres puissent partager des informations en vue de créer un réseau professionnel. Les utilisateurs de LinkedIn chargent des informations pour créer des profils en ligne et se connecter avec d'autres membres. LinkedIn connecte les employés avec des employeurs et les entreprises avec d'autres entreprises partout dans le monde.

Il suffit de s'approcher de plus près pour voir comment ces châteaux sont construits. Fondamentalement, ces châteaux tirent leur force de leur capacité à collecter les données des utilisateurs avec leur consentement. Ces données incluent souvent les parcours des utilisateurs, leurs discussions, leurs mentions « j'aime », leurs géolocalisations, leurs voyages, leurs intérêts, leurs amis et les membres de leurs familles, leurs professions, leurs passe-temps, et leurs projets professionnels et personnels. Les cybermagiciens créent une formidable valeur ajoutée pour les entreprises souhaitant utiliser ces données pour mieux comprendre et communiquer avec leurs clients et leurs collaborateurs.

# La croissance des royaumes virtuels

Les données collectées dans le monde virtuel vont bien au-delà de celles fournies volontairement par les utilisateurs. Le royaume virtuel croît en même temps que les sciences et les technologies évoluent, permettant aux cybermagiciens de collecter d'autres formes de données. Les cybermagiciens disposent désormais d'une technologie capable d'assurer le suivi des tendances météorologiques dans le monde entier, de surveiller les océans et d'analyser le déplacement et le comportement des personnes, des animaux et des objets en temps réel.

De nouvelles technologies, comme GIS (Geospatial Information Systems) et l'Internet of Everything (IoE), ont fait leur apparition. Ces nouvelles technologies permettent d'identifier les types d'arbres dans un quartier et de localiser très rapidement des véhicules, des appareils, des individus et des matériels. Ce type d'information permet d'économiser de l'énergie, améliorer l'efficacité des systèmes et réduire les risques de sécurité. Chacune de ces technologies contribue également à l'expansion continue de la quantité de données collectées, analysées et utilisées pour comprendre le monde. Les données collectées par les technologies GIS et IoE poseront à l'avenir un vrai défi aux professionnels de la sécurité. Le type de données générées par ces appareils peut potentiellement permettre aux cybercriminels d'accéder aux aspects très intimes de la vie quotidienne des individus.

# Qui sont les cybercriminels ?

Au début de la cybersécurité, les cybercriminels étaient généralement des adolescents ou des amateurs agissant depuis leur ordinateur à domicile, et les attaques se limitaient à des canulars et du vandalisme. Aujourd'hui, le monde des cybercriminels est devenu plus dangereux. Les cybercriminels sont des individus ou des groupes qui tentent d'exploiter des vulnérabilités à des fins personnelles ou financières. Tout les intéresse, des cartes de crédit aux conceptions de produits et tout ce qui a de la valeur.

**Amateurs** : les amateurs, ou « script kiddies », ont peu ou pas de compétences. Ils utilisent souvent des outils ou des instructions trouvés sur Internet pour lancer des attaques. Certains sont simplement curieux, tandis que d'autres essaient de démontrer leurs compétences et provoquent des dommages. Ils peuvent utiliser des outils basiques, mais le résultat peut quand même être dévastateur.

**Hackers** : ce groupe de criminels s'introduit dans les ordinateurs et les réseaux. Leurs motifs sont variés. Selon le type d'intrusion, les hackers sont classés dans l'une des trois catégories suivantes : hackers au chapeau blanc, gris ou noir. Les hackers au chapeau blanc s'introduisent dans les systèmes réseau et informatiques pour en découvrir les faiblesses et en améliorer la sécurité. Les propriétaires du système leur donnent l'autorisation de s'y introduire et reçoivent les résultats du test. D'un autre côté, les hackers au chapeau noir profitent de toute vulnérabilité à des fins personnelles, financières ou politiques illégales. Les hackers au chapeau gris se trouvent entre les Chapeaux noirs et les Chapeaux blancs. Parfois, les hackers au chapeau gris détectent une vulnérabilité et en font part aux propriétaires du système si cela s'intègre à leurs objectifs Mais certains hackers au chapeau gris publient leurs découvertes sur Internet pour que d'autres hackers puissent les exploiter.

La figure propose des détails sur les termes pirate informatique Chapeau blanc, pirate informatique Chapeau noir et pirate informatique Chapeau gris.

**Hackers organisés** : ces criminels sont notamment des organisations de cybercriminels, des hacktivistes, des terroristes et des hackers financés par des gouvernements. Les cybercriminels sont généralement des groupes de criminels professionnels qui misent sur le contrôle, le pouvoir et la richesse. Ils sont très expérimentés et organisés, et ils peuvent même proposer leurs services dans le secteur du cybercrime. Les hacktivistes effectuent des déclarations politiques pour sensibiliser sur les questions qui leur sont importantes. Les hacktivistes rendent publiques des informations compromettantes sur leurs victimes. Les agresseurs financés par des gouvernements rassemblent des renseignements ou commettent des sabotages au nom de leurs gouvernements. Ces agresseurs sont généralement très entraînés et disposent de fonds importants. Leurs attaques ciblent des objectifs spécifiques présentant un avantage pour leur gouvernement. Certains hackers financés par des gouvernements sont même membres des forces armées de leurs pays.

Cliquez [ici](http://www.watchguard.com/tips-resources/hacker-profiles.asp) pour voir les représentations graphiques des profils de pirates.

# Motivations des cybercriminels

Les profils et les motivations des cybercriminels ont changé au fil des ans. Le hacking a commencé dans les années 1960 par le piratage téléphonique (phone freaking ou phreaking). Cette pratique consistait à utiliser différentes fréquences audio pour manipuler les systèmes téléphoniques. Dans le milieu des années 1980, les criminels utilisaient des modems commutés pour connecter des ordinateurs à des réseaux et utilisaient des programmes de piratage de mots de passe pour accéder aux données. Aujourd'hui, les criminels ne se contentent plus de voler des informations. Les criminels utilisent maintenant les malwares et les virus comme armes technologiques. Toutefois, la plus grande motivation de la plupart des cybercriminels est financière. La cybercriminalité est devenue plus lucrative que le trafic de stupéfiants.

Les profils et les motivations des hackers ont sensiblement changé. La figure présente différents modes de hacking et une description de chacun.

# Pourquoi devenir un spécialiste de la cybersécurité ?

C'est le nombre d'offres d'emploi pour des spécialistes en cybersécurité qui a le plus augmenté dans le secteur de l'informatique. Les technologies qui transforment le royaume et les vies quotidiennes des individus les rendent aussi plus vulnérables aux attaques. La technologie seule ne permet pas d'empêcher, de détecter et de résoudre les incidents de cybersécurité, ni de s'en remettre. Analysons les faits suivants :

* Le niveau de compétence requis pour être un spécialiste de la cybersécurité performant et la pénurie de professionnels de la cybersécurité qualifiés permettent d'envisager des salaires plus élevés.
* Les technologies de l'information évoluent en permanence. Il en est de même pour la cybersécurité. De par sa nature dynamique, le domaine de la cybersécurité est à la fois fascinant et stimulant.
* Un spécialiste de la cybersécurité peut aussi avoir une carrière très mobile. Des offres d'emploi sont proposées presque partout dans le monde.
* Les spécialistes de la cybersécurité sont très importants pour leur entreprise, à leur pays et à leur société, un peu comme les services de police ou d'urgence.

Devenir spécialiste de la cybersécurité offre une opportunité de carrière enrichissante.

Contrer les cybercriminels

Contrecarrer les plans des cybercriminels est une tâche difficile. Il n'existe pas de solution « miracle ». Toutefois, les entreprises, les gouvernements et les organisations internationales commencent à mener des actions coordonnées pour les limiter ou les contrer. Voici quelques exemples d'actions coordonnées :

* Création de bases de données complètes des vulnérabilités connues des systèmes et des signatures des attaques (organisation unique des informations permettant d'identifier la tentative d'exploitation d'une vulnérabilité connue par un hacker). Les entreprises partagent ces bases de données dans le monde entier pour se préparer aux attaques courantes et les contrer.
* Mise en œuvre de capteurs d'alerte et de réseaux d'alerte. En raison du coût et de l'incapacité à surveiller chaque réseau, les entreprises surveillent les cibles de choix ou créent des impostures ressemblant à des cibles à haute valeur ajoutée. Ces cibles étant plus susceptibles de subir des attaques, elles avertissent les autres d'attaques potentielles.
* Partage d'informations relatives à la cybersécurité. Les entreprises, les organismes publics et les pays collaborent désormais pour partager des informations essentielles au sujet d'attaques graves sur des cibles critiques. Cela permet d'empêcher que des attaques similaires touchent d'autres cibles. De nombreux pays ont créé des agences de renseignement sur la cybersécurité pour collaborer à l'échelle mondiale en combattant des cyberattaques de grande ampleur.
* Établissement de normes de gestion de la sécurité des informations au sein des organisations nationales et internationales. La norme ISO 27000 est un bon exemple de ces efforts au niveau international.
* Promulgation de nouvelles lois pour décourager les cyberattaques et les violations de données. Ces lois prévoient des sanctions sévères à l'encontre des cybercriminels ayant commis des actes illégaux.

La figure présente des mesures pour contrer les cybercriminels et une brève description de chacune.

# Les menaces ciblant le peuple du royaume

Les cybermagiciens sont des innovateurs et des visionnaires. Ce sont eux qui construisent le royaume de la cybersécurité. Ils connaissent la puissance des données et savent qu'il faut exploiter cette puissance pour créer de grandes entreprises, fournir des services et protéger les utilisateurs contre les cyberattaques. Ils sont conscients de la menace représentée par les données lorsqu'elles sont utilisées contre des individus.

Les menaces et les vulnérabilités sont leurs principales préoccupations. Une menace est la possibilité qu'un événement nuisible, tel qu'une attaque, survienne. Une vulnérabilité est une faiblesse qui rend une cible susceptible d'être attaquée. Par exemple, entre de mauvaises mains, les données peuvent être responsables de la divulgation de l'identité de leur propriétaire, porter atteinte à leur crédit ou mettre leur carrière ou leurs relations personnelles en péril. Le vol d'identité n'a rien d'anodin. Toutefois, ce ne sont pas forcément les comptes Google et Facebook qui présentent les plus grands risques. Les écoles, les hôpitaux, les institutions financières, les organismes publics, les lieux de travail et le commerce électronique posent des risques encore plus grands. Les entreprises comme Google et Facebook ont les ressources nécessaires pour recruter les meilleurs experts en cybersécurité capables de protéger leur château. Plus les entreprises sont nombreuses à construire des châteaux de données, plus le besoin en professionnels de la cybersécurité augmente. Les plus petites entreprises et organisations se battent donc pour attirer les professionnels de la cybersécurité restants. Les menaces de cybersécurité sont particulièrement dangereuses pour certains secteurs d'activité et les données qu'ils gèrent.

# Types de données personnelles

Dans les entreprises bien établies, on peut par exemple trouver les sources de données ci-après.

**Dossiers médicaux**

Chaque fois que vous vous rendez chez le médecin, il ajoute des informations supplémentaires à votre dossier de santé électronique (DSE). La prescription du médecin traitant est enregistrée dans le DSE. Un DSE inclut des informations sur la santé physique, la santé mentale et d'autres informations personnelles qui pourraient ne pas concerner la santé. Par exemple, un individu peut avoir été suivi dans son enfance par un psychologue suite à des changements majeurs dans sa famille. Cela est enregistré quelque part dans son dossier médical. Parallèlement aux antécédents médicaux et aux informations personnelles, le DSE peut également contenir des informations concernant la famille de la personne concernée. Plusieurs lois encadrent la protection des dossiers des patients.

Les dispositifs médicaux, comme les bracelets de remise en forme, utilisent la plate-forme cloud pour activer le transfert, le stockage et l'affichage sans fil de données cliniques telles que la fréquence cardiaque, la pression artérielle et la glycémie. Ces dispositifs peuvent générer une grande quantité de données cliniques pouvant être enregistrées dans un dossier médical.

**Dossiers scolaires**

Les dossiers scolaires incluent des informations sur les cursus, les résultats aux tests, la présence aux cours, les cours suivis, les récompenses, les diplômes délivrés et les rapports disciplinaires. Ce dossier peut également contenir des coordonnées, des dossiers de santé et de vaccination, ainsi que des dossiers scolaires particuliers, dont les programmes d'éducation personnalisés (IEP).

**Dossiers professionnels et financiers**

Les informations professionnelles incluent les emplois et les performances passés. Les dossiers professionnels peuvent également inclure des informations sur les salaires et les assurances. Les dossiers financiers peuvent inclure des informations sur les revenus et les dépenses. Les dossiers fiscaux peuvent comprendre des fiches de paie, des relevés bancaires, des antécédents de crédit et d'autres informations bancaires.

# Menaces contre les services du royaume

Les services du royaume sont identiques à ceux nécessaires au fonctionnement d'un réseau et d'Internet. Ces services incluent le routage, l'adressage, l'affectation de noms et la gestion de bases de données. Ces services sont également les cibles principales des cybercriminels.

Les criminels utilisent des outils d'interception des paquets pour capturer les flux de données sur un réseau. Cela signifie que toutes les données sensibles, comme les noms d'utilisateurs, les mots de passe et les numéros de carte bancaire, sont susceptibles d'être dérobées. Ces outils surveillent et enregistrent toutes les informations qui transitent sur un réseau. Les criminels peuvent aussi utiliser des appareils non autorisés, comme des points d'accès Wi-Fi non protégés. Si un criminel installe un tel appareil près d'un lieu public, comme un café, les personnes peu méfiantes qui se connectent permettent à l'analyseur de paquet de copier leurs informations personnelles.

Le DNS (service de nom de domaine) convertit un nom de domaine comme [www.facebook.com](http://www.facebook.com/)en l'adresse IP numérique associée. Si un serveur DNS ne connaît pas l'adresse IP, il la demande à un autre serveur DNS. Dans le cadre de l'usurpation DNS (ou empoisonnement du cache DNS), le criminel introduit de fausses données dans le cache d'un résolveur DNS. Ces attaques par empoisonnement exploitent une faiblesse du logiciel DNS qui amène les serveurs DNS à rediriger le trafic d'un domaine spécifique vers l'ordinateur du criminel, au lieu du propriétaire légitime du domaine.

Les paquets transportent les données sur un réseau ou sur Internet. La falsification de paquets (ou injection de paquets) interfère avec une communication réseau établie en créant des paquets qui semblent faire partie d'une communication. La falsification de paquets permet à un hacker de perturber ou d'intercepter des paquets. Ce processus permet au hacker de pirater une connexion autorisée ou refuse à un individu la capacité d'utiliser certains services réseau. Les professionnels de la cybersécurité appellent cela une attaque « man-in-the-middle ».

Les exemples donnés ne font qu'effleurer les types de menaces pouvant être lancées contre les services du royaume.

# Les menaces ciblant les secteurs du royaume

Les secteurs du royaume incluent les systèmes d'infrastructure, comme la fabrication, l'énergie, les communications et le transport. Par exemple, le réseau électrique intelligent est une amélioration du système de génération et de distribution de l'électricité. Le réseau électrique transporte l'alimentation des générateurs centraux vers un grand nombre de clients. Un réseau électrique intelligent utilise les informations pour créer un réseau avancé automatisé de distribution de l'énergie. Les leaders mondiaux savent que la protection de leur infrastructure est essentielle pour protéger leur économie.

Au cours des 10 dernières années, les cyberattaques comme Stuxnet ont prouvé qu'une telle attaque pouvait parvenir à détruire ou interrompre des infrastructures critiques. Concrètement, l'attaque Stuxnet a ciblé le système SCDA (Supervisory Control and Data Acquisition) utilisé pour contrôler et surveiller les processus industriels. SCADA peut être intégré aux divers processus industriels des systèmes de fabrication, de production, de distribution d'énergie et de communication. Cliquez [ici](https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon?language=en) pour en savoir plus sur l'attaque Stuxnet.

Une cyberattaque peut perturber ou interrompre les secteurs d'activité comme les télécommunications, les transports ou les systèmes de génération et de distribution d'électricité. Elle peut également mettre un coup d'arrêt au secteur des services financiers. L'un des problèmes des environnements intégrant des systèmes SCADA est que les concepteurs n'ont pas connecté ces systèmes à un environnement informatique classique et à Internet. Par conséquent, ils n'ont pas correctement pris en compte la cybersécurité pendant la phase de développement de ces systèmes. Comme les autres secteurs d'activité, les entreprises qui utilisent des systèmes SCADA savent combien il est important de collecter des données pour améliorer les opérations et diminuer les coûts. Elles utilisent donc généralement des systèmes SCADA connectés à des systèmes informatiques classiques. Pourtant, cette configuration augmente la vulnérabilité des secteurs d'activités utilisant des systèmes SCADA.

Le risque de menace avancée qui pèse aujourd'hui sur les royaumes exige de faire appel à des spécialistes de la cybersécurité spécifiques.

# Les menaces ciblant les activités quotidiennes d'un royaume

La cybersécurité désigne l'effort permanent nécessaire pour protéger les systèmes et les données du réseau contre tout accès non autorisé. Au niveau personnel, tout le monde doit protéger son identité, ses données et ses appareils informatiques. Au niveau professionnel, chaque collaborateur est responsable de la protection de la réputation, des données et des clients de l'entreprise. Au niveau national, la sécurité nationale ainsi que la sécurité et le bien-être des citoyens sont en jeu. Les professionnels de la cybersécurité sont souvent sollicités par les organismes publics pour les aider à identifier et à collecter les données.

Aux États-Unis, la NSA (National Security Agency) est chargée de collecter des informations et de surveiller des activités. La NSA a construit un nouveau data center spécifiquement pour traiter le volume croissant de données. En 2015, le Congrès des États-Unis a promulgué le USA Freedom Act qui met un terme à la pratique de la collecte en vrac des relevés téléphoniques des citoyens américains. Ce programme générait des métadonnées donnant à la NSA des informations sur les communications envoyées et reçues.

Les efforts consacrés à la protection du mode de vie des citoyens entrent souvent en conflit avec le respect de leur vie privée. Il sera intéressant d'observer de quelle manière va évoluer l'équilibre entre les droits des citoyens et la sécurité du royaume.

Menaces internes et externes

**Menaces internes pour la sécurité**

Les attaques peuvent provenir de l'intérieur d'une entreprise ou de l'extérieur, comme illustré sur la figure. Un utilisateur interne, par exemple un employé ou un partenaire contractuel, peut accidentellement ou intentionnellement :

* mal gérer les données confidentielles ;
* menacer le fonctionnement des serveurs internes ou des périphériques de l'infrastructure réseau ;
* faciliter les attaques venant de l'extérieur en connectant un support USB infecté dans le système informatique de l'entreprise ;
* inviter accidentellement un malware dans le réseau par des e-mails ou des sites Web malveillants.

Les menaces internes sont susceptibles d'entraîner des dégâts plus importants que les menaces externes, car les utilisateurs internes disposent d'un accès direct au bâtiment et à l'équipement de l'infrastructure. Les hackers internes connaissent généralement le réseau de l'entreprise, ses ressources et ses données confidentielles. Ils connaissent aussi parfois les mesures de sécurité, les politiques et les privilèges administratifs de niveau supérieur.

**Menaces externes pour la sécurité**

Les menaces externes provenant de hackers amateurs ou expérimentés tirent parti des vulnérabilités des appareils réseau ou font appel à des techniques d'ingénierie sociale, comme la supercherie, pour accéder aux données. Les attaques externes exploitent les faiblesses ou les vulnérabilités pour accéder aux ressources internes.

**Données traditionnelles**

Les informations de l'entreprise incluent les informations personnelles, la propriété intellectuelle et les données financières. Les informations personnelles incluent des dossiers de candidature, des fiches de paie, des lettres d'offre, des contrats de travail et toute information utilisée dans les prises de décisions sur l'embauche. La propriété intellectuelle, comme les brevets, les marques déposées et les plans produits, permet à une entreprise d'avoir un avantage économique sur ses concurrents. La propriété intellectuelle peut être considérée comme un secret commercial ; la perdre serait désastreux pour l'avenir de l'entreprise. Les données financières, dont les comptes de résultat, les bilans comptables et les tableaux de trésorerie d'une entreprise, donnent un aperçu de la santé de l'entreprise.

# Les vulnérabilités des terminaux mobiles

Avant, les employés utilisaient les ordinateurs fournis par l'entreprise connectés au réseau LAN de cette dernière. Les administrateurs surveillent et mettent à jour ces ordinateurs en permanence pour répondre aux exigences de sécurité. De nos jours, les terminaux mobiles comme les iPhone, les smartphones, les tablettes et les milliers d'autres appareils, remplacent parfaitement les ordinateurs classiques ou viennent les compléter. De plus en plus de personnes utilisent ces terminaux pour accéder aux informations de l'entreprise. La tendance du BYOD (Bring Your Own Device) gagne du terrain. Or, comme il est impossible de gérer et de mettre à jour de façon centralisée ces terminaux mobiles, les entreprises qui autorisent leur utilisation sur leur réseau s'exposent à de grands risques.

# L'émergence de l'Internet des objets

L'Internet des objets (IoT) est l'ensemble de technologies qui permettent de connecter divers appareils à Internet. Combinée à l'avènement de l'IoT, l'évolution technologique modifie les environnements commerciaux et grand public. Les technologies IoT permettent de connecter des milliards d'appareils à Internet, notamment des appliances, des verrous, des moteurs et des appareils de divertissement, pour n'en citer que quelques-uns. Cette technologie accroît le volume de données à protéger. Les utilisateurs accèdent à ces appareils à distance, ce qui augmente le nombre de réseaux à protéger.

Avec l'émergence de l'IoT, vous devez protéger et gérer encore plus de données. Toutes ces connexions, associées à la l'augmentation de la capacité de stockage et aux services de stockage via le cloud et la virtualisation, ont engendré une croissance exponentielle des données. Cette expansion des données a créé un nouveau centre d'intérêt dans le domaine de la technologie et de l'entreprise. C'est ce qu'on appelle le « Big Data ».

L'impact du Big Data

Le Big Data est la conséquence de grands ensembles de données complexes qui rendent les applications classiques de traitement des données inadéquates. Le Big Data présente des challenges et offre des opportunités s'articulant autour de trois dimensions :

* Le volume ou la quantité de données
* La vélocité ou la vitesse des données
* La variété ou la plage de types et de sources de données

Les exemples d'attaques ciblant de grandes entreprises ne manquent pas dans les journaux. Les entreprises comme Target, Home Depot et PayPal subissent des attaques très médiatisées. Par conséquent, les systèmes d'entreprise doivent être profondément remaniés : les solutions de sécurité doivent être repensées et des mises à niveau substantielles des technologies et des pratiques s'imposent. En outre, les gouvernements et les différents secteurs d'activités mettent en œuvre davantage de réglementations et de règles qui exigent une meilleure protection des données et l'application de contrôles de sécurité afin de protéger le Big Data.

# Utilisation d'armes avancées

Les vulnérabilités logicielles reposent aujourd'hui sur les erreurs de programmation, les failles de protocole ou les erreurs de configuration du système. Le cybercriminel n'a plus qu'à exploiter l'une d'entre elles. Par exemple, une attaque commune consiste à configurer une entrée dans le programme pour le saboter et l'empêcher de fonctionner correctement. Ce dysfonctionnement crée une porte d'accès au programme qui provoque la fuite de données.

Aujourd'hui, les cyberattaques sont de plus en plus sophistiquées. Une menace persistante avancée est un piratage informatique continu ciblant un objet spécifique qui reste indétecté. Les criminels choisissent habituellement une attaque persistante avancée pour des raisons économiques ou politiques. Une attaque persistante avancée se déroule sur une longue période sans être détectée grâce à un malware sophistiqué.

Les attaques basées sur des algorithmes assurent le suivi des données autodéclarées du système, comme la quantité d'énergie utilisée par un ordinateur, et les utilisent pour choisir une cible ou lancer de fausses alertes. Les attaques algorithmiques peuvent également désactiver un ordinateur en le forçant à utiliser sa mémoire ou en surchargeant son processeur. Les attaques basées sur des algorithmes sont plus sournoises, car elles exploitent des conceptions utilisées pour multiplier les économies d'énergie, diminuer les pannes du système et améliorer l'efficacité.

Enfin, la nouvelle génération d'attaques choisit plus soigneusement ses victimes. Avant, les attaques sélectionnaient des cibles faciles ou les victimes les plus vulnérables. Mais la détection et l'isolation des cyberattaques étant de plus en plus efficaces, les cybercriminels sont de plus en plus prudents. S'ils sont détectés trop tôt, les spécialistes de la cybersécurité fermeront les grilles du château. En conséquence, la plupart des attaques les plus sophistiquées ne sont lancées que si le hacker est en mesure de reproduire la signature d'objet ciblée.

# Une portée plus large et un effet domino

La gestion des identités fédérées se définit de la manière suivante : les utilisateurs de plusieurs entreprises peuvent utiliser les mêmes informations d'identification pour accéder aux réseaux de toutes les entreprises du groupe. En cas d'attaque, cette situation augmente sa portée et la probabilité d'un effet domino.

L'identité fédérée relie l'identité électronique d'un sujet à plusieurs systèmes distincts de gestion des identifications. Par exemple, un sujet peut se connecter à Yahoo! avec ses informations d'identification Google ou Facebook. C'est un exemple de connexion sociale.

La gestion des identités fédérées a pour objectif de partager automatiquement les informations d'identification à plus grande échelle. Du point de vue de l'utilisateur, cela implique une connexion unique au web.

Il est impératif que les entreprises étudient de près les informations d'identification partagées avec leurs partenaires. Les numéros de sécurité sociale, les noms et les adresses sont autant d'informations que les voleurs d'identité peuvent dérober aux partenaires pour perpétrer une fraude. Pour protéger les identités fédérées, il convient généralement de relier les autorisations de connexion à un appareil autorisé.

# Les implications en matière de sécurité

Les centres d'appel aux États-Unis sont vulnérables aux cyberattaques qui interrompent les réseaux de communication des secours (911), mettant la sécurité publique en danger. Une attaque téléphonique par déni de service (TDoS) consiste à saturer un réseau téléphonique cible d'appels téléphoniques afin d'empêcher les appels légitimes d'aboutir. Les centres d'appels d'urgence de nouvelle génération sont vulnérables car ils utilisent des systèmes VoIP (voix sur IP) au lieu des lignes terrestres classiques. Outre les attaques par déni de service, ces centres d'appel sont également sujets aux attaques par déni de service distribuées (DDoS) qui utilisent un grand nombre de systèmes pour inonder les ressources de la cible, empêchant les utilisateurs légitimes d'accéder à cette cible. Aujourd'hui, il existe plusieurs manières d'appeler les urgences, de l'application pour smartphone au dispositif de sécurité à domicile.

# Une meilleure reconnaissance des menaces de cybersécurité

Au début, les systèmes de défense contre les cyberattaques n'étaient pas nombreux. Un lycéen intelligent ou un script kiddie étaient capables accéder à des systèmes. Les pays du monde entier sont conscients de la menace des cyberattaques. Les cyberattaques arrivent désormais en tête de la liste des principales menaces pour la sécurité nationale et économique de la plupart des pays.

# Gérer le manque de spécialistes en cybersécurité

Aux États-Unis, le NIST (National Institute of Standards and Technologies) a créé un cadre pour les entreprises et les organisations qui recherchent des professionnels de la cybersécurité. Ce cadre leur permet d'identifier les principaux types de responsabilités, de postes et de compétences recherchés. Le cadre national pour l'embauche de collaborateurs experts en cybersécurité classe et décrit les postes de cybersécurité. Il propose un vocabulaire commun pour décrire les postes de cybersécurité avec un ensemble commun de tâches et de compétences requises pour devenir spécialiste de la cybersécurité. Ce cadre permet de définir les exigences professionnelles associées à la cybersécurité.

# Les sept catégories de magiciens de la cybersécurité

Le cadre pour l'embauche de collaborateurs classe les postes du domaine de la cybersécurité en sept catégories.

**Exploiter et maintenir en conditions opérationnelles** inclut l'assistance, l'administration et la maintenance requises pour garantir la performance et la sécurité du système informatique.

**Protéger et défendre** inclut l'identification, l'analyse et la réduction des menaces pour les systèmes et les réseaux internes.

**Enquêter** inclut l'enquête sur les événements informatiques et/ou les cyberattaques impliquant des ressources informatiques.

**Collecter et exploiter** inclut la collecte d'informations sur les opérations frauduleuses, les dénis de service et la cybersécurité.

**Analyser** inclut l'examen et l'évaluation ultra spécialisés des informations de cybersécurité entrantes afin de déterminer si elles sont utiles.

**Surveiller et développer** fournit le leadership, l'encadrement et la direction nécessaires pour assurer l'efficacité des experts en cybersécurité.

**Provisionner en toute sécurité** inclut la conceptualisation, la conception et la création de systèmes informatiques sécurisés.

Chaque catégorie compte plusieurs domaines de spécialité. Ces domaines de spécialité définissent ensuite les divers types de postes les plus courants en cybersécurité.

La figure présente les différentes catégories et une description de chacune.

# Organisations professionnelles

Il arrive souvent que les spécialistes de la cybersécurité travaillent en collaboration. Les entreprises technologiques internationales parrainent souvent des ateliers et des conférences. Dans ces entreprises, les professionnels de la cybersécurité sont généralement stimulés et motivés.

Entreprises spécialisées en sécurité :

# Les compétitions et les groupes d'étudiants dans le domaine de la cybersécurité

Les spécialistes de la cybersécurité doivent avoir les mêmes compétences que les hackers, surtout les hackers « black hat », afin de pouvoir mettre en place des systèmes de protection contre leurs attaques. Comment pouvez-vous acquérir et mettre en pratique les compétences nécessaires pour devenir un spécialiste de la cybersécurité ? Les compétitions comparant les compétences des étudiants sont un bon moyen d'acquérir des compétences et des connaissances dans le domaine de la cybersécurité. Plusieurs compétitions nationales sont ouvertes aux étudiants en cybersécurité.

# Certifications reconnues par le secteur

Dans un monde où les menaces sont omniprésentes, il est indispensable de pouvoir faire appel à des professionnels de la sécurité compétents et qualifiés. Le secteur IT a mis en place des normes qui permettent aux spécialistes de la cybersécurité d'obtenir des certifications professionnelles qui prouvent leurs compétences et leur niveau de connaissance.

**CompTIA Security+**

Security+ est un programme de test parrainé par CompTIA qui certifie la compétence des administrateurs informatiques en garantie d'informations. Le test Security+ couvre les principes les plus importants de sécurisation d'un réseau et de gestion du risque, y compris les préoccupations liées au cloud computing.

**Certified Ethical Hacker (CEH) d'EC-Council**

Cette certification de niveau intermédiaire atteste que les spécialistes de la cybersécurité qui la détiennent possèdent les compétences et les connaissances relatives à diverses pratiques de piratage. Ces spécialistes de la cybersécurité utilisent les mêmes compétences et techniques que celles utilisées par les cybercriminels pour identifier les vulnérabilités des systèmes et les points d'accès aux systèmes.

**GIAC Security Essentials (GSEC) de SANS**

La certification GSEC est un bon choix d'homologation de premier niveau pour les spécialistes de la cybersécurité ayant démontré leur connaissance de la terminologie et des concepts relatifs à la sécurité, ainsi que leurs compétences et leur expertise « pratique » en matière de sécurité. Le programme SANS GIAC propose de nombreuses certifications supplémentaires dans les domaines de la gestion de la sécurité, de l'investigation et des audits.

**Certified Information Systems Security Professional (CISSP)** de **(ISC)^2**

La certification CISSP est une certification indépendante des fournisseurs pour les spécialistes de la cybersécurité ayant beaucoup d'expérience sur le plan de la technique et de l'encadrement. Elles sont également approuvées formellement par le département de la Défense des États-Unis et reconnues par les entreprises du secteur de la sécurité dans le monde entier.

**Certified Information Security Manager (CISM) d'ISACA**

Les cyberhéros responsables de la gestion, du développement et de la supervision des systèmes de sécurité de l'information au niveau d'une entreprise ou ceux développant les meilleures pratiques de sécurité peuvent prétendre à la certification CISM. Les détenteurs de cette certification possèdent des compétences avancées en gestion des risques de sécurité.

# Certifications commanditées par les entreprises

Les certifications commanditées par les entreprises sont également des homologations importantes pour les spécialistes de la cybersécurité. Ces certifications évaluent les connaissances et les compétences relatives à l'installation, à la configuration et à la maintenance des produits de divers fournisseurs. Cisco et Microsoft proposent, par exemple, des certifications testant les connaissances sur leurs produits. Cliquez [ici](https://learningnetwork.cisco.com/community/certifications) pour explorer la matrice des certifications Cisco illustrée dans la figure.

**Cisco Certified Network Associate Security (CCNA Security)**

La certification CCNA Security atteste qu'un spécialiste de la cybersécurité possède les connaissances et les compétences requises pour sécuriser les réseaux Cisco.

Cliquez [ici](https://learningnetwork.cisco.com/community/certifications/security_ccna) pour en savoir plus sur la certification CCNA Security.

Comment devenir un cyberhéros

Pour devenir un spécialiste reconnu de la cybersécurité, le candidat potentiel doit satisfaire certaines exigences uniques. Les héros doivent être en mesure de répondre aux menaces dès qu'elles surviennent. Leurs heures de travail peuvent donc être quelque peu irrégulières.

Les cyberhéros analysent également les politiques, les tendances et les informations collectées pour savoir comment pensent les cybercriminels. Ils jouent donc très souvent le rôle de détectives.

Les recommandations suivantes peuvent aider les aspirants spécialistes en cybersécurité à atteindre leurs objectifs :

* **Étudier**: apprenez les bases en suivant des cours en informatique. Apprenez de nouvelles choses toute votre vie. La cybersécurité est un domaine en perpétuelle mutation et les spécialistes de la cybersécurité doivent rester au fait des nouvelles tendances.
* **Obtenir des certifications** : les certifications commanditées par les entreprises du secteur comme Microsoft et Cisco attestent qu'une personne possède les connaissances requises pour postuler à un emploi de spécialiste de la cybersécurité.
* **Faire des stages**: faire un stage dans le domaine de la sécurité lorsqu'on est étudiant peut créer des opportunités de carrière.
* **Adhérer à des associations professionnelles**: adhérez à des associations de sécurité informatique, assistez à des réunions et des conférences, consultez des forums et des blogs pour vous enrichir de connaissances auprès d'experts.

# Conclusion

Au cours de ce chapitre, nous avons expliqué la structure de l'univers de la cybersécurité et pourquoi il continue à gagner du terrain avec l'augmentation du nombre de données et d'informations à protéger.

Nous vous avons également présenté le rôle des cybercriminels et leurs motivations. Nous avons montré l'étendue des forces obscures liée aux transformations techniques toujours plus nombreuses qui se déroulent partout dans le monde.

Enfin, nous avons expliqué comment devenir un spécialiste de la cybersécurité et lutter contre les cybercriminels qui nourrissent les forces obscures. Nous avons détaillé quelles étaient les ressources disponibles pour augmenter le nombre de héros. Nous avons démontré que les cyberhéros doivent avoir les mêmes compétences que les cybercriminels.

Si vous souhaitez approfondir les concepts présentés dans ce chapitre, consultez la page dédiée aux activités et aux ressources complémentaires dans la section relative aux ressources destinées aux élèves.