Chapitre 2 : Attaques, concepts et techniques

Ce chapitre couvre les moyens utilisés par les professionnels de la cybersécurité pour analyser les faits survenus suite à une cyberattaque. Cela explique les vulnérabilités des logiciels et du matériel de sécurité, ainsi que les différentes catégories de vulnérabilité de la sécurité.

Les différents types de logiciels malveillants (appelés malware) et les symptômes de logiciels malveillants sont traités. Les différents moyens que peuvent utiliser les pirates pour infiltrer un système ainsi que les attaques par déni de service sont également traitées.

La plupart des cyberattaques modernes sont considérées comme des attaques mixtes. Les attaques mixtes utilisent différentes techniques pour infiltrer et pour attaquer un système. Lorsqu’une attaque ne peut être évitée, il incombe au professionnel de la cybersécurité de réduire l’impact de cette attaque.

# Détecter les vulnérabilités de sécurité

Les vulnérabilités de sécurité représentent un défaut matériel ou logiciel. Après avoir pris connaissance d’une vulnérabilité, les utilisateurs malveillants tentent de l’exploiter. Un *exploit* est le terme employé pour désigner un programme écrit utilisé pour exploiter une vulnérabilité connue. L’utilisation d’un exploit contre une vulnérabilité est considérée comme une attaque. L’objectif de l’attaque est d’obtenir l’accès à un système, aux données hébergées ou à une ressource spécifique.

**Vulnérabilités des logiciels**

Les vulnérabilités des logiciels sont généralement introduites par des erreurs dans le système d’exploitation ou dans le code d’application ; malgré tous les efforts des entreprises pour détecter et corriger les vulnérabilités des logiciels, il est fréquent que de nouvelles vulnérabilités se présentent. Microsoft, Apple et d’autres producteurs de système d’exploitation sortent des correctifs et des mises à jour quasiment tous les jours. Les mises à jour d’applications sont également fréquentes. Des applications comme les navigateurs Web, les applications mobiles et les serveurs Web sont souvent mis à jour par les entreprises ou les organisations responsables.

En 2015, une vulnérabilité majeure, appelée SYNful Knock, a été découverte dans Cisco IOS. Cette vulnérabilité a permis aux agresseurs d’obtenir le contrôle des routeurs professionnels, notamment les routeurs 1841, 2811 et 3825 de Cisco. Ils pouvaient ainsi espionner toutes les communications réseau et infecter d’autres périphériques réseau. Cette vulnérabilité a été introduite dans le système lors de l’installation d’une version modifiée de l’IOS sur les routeurs. Pour éviter cela, vérifiez constamment l’intégrité de l’image IOS téléchargée et limitez l’accès physique de l’équipement au personnel autorisé.

L’objectif des mises à jour logicielles est de rester à jour et d’éviter l’exploitation des vulnérabilités. Lorsque certaines entreprises disposent d’équipes de test de pénétration dédiées à la recherche, à la détection et à la correction des vulnérabilités des logiciels avant d’être exploitables, les experts en sécurité tiers se spécialisent également dans la recherche de vulnérabilités des logiciels.

Projet Zero de Google est un excellent exemple de cette pratique. Après avoir découvert un certain nombre de vulnérabilités sur différents logiciels utilisés par les utilisateurs finaux, Google a constitué une équipe permanente dédiée à la recherche de vulnérabilités des logiciels. Vous pouvez trouver le rapport de recherche sur la sécurité de Google [ici](https://code.google.com/p/google-security-research/issues/list?can=1).

**Vulnérabilités du matériel**

Les vulnérabilités sont souvent causées par des défauts de conception du matériel. La mémoire RAM, par exemple, est essentiellement composée de condensateurs installés étroitement les uns près des autres. Il a été découvert qu’à cause de la proximité, les modifications continues appliquées à l’un des condensateurs pouvaient affecter les condensateurs environnants. Sur la base de ce défaut de conception, un exploit appelé Rowhammer a été créé. En réécrivant à plusieurs reprises la mémoire dans les mêmes adresses, l’exploit de Rowhammer permet de récupérer des données à partir des cellules de mémoire d’une adresse à proximité, même si les cellules sont protégées.

Les vulnérabilités du matériel sont spécifiques aux modèles d'appareils et sont généralement exploitées pour des tentatives compromettantes. Tandis que les exploits sur le matériel sont plus fréquents dans les attaques très ciblées, la protection classique contre les malwares et une sécurité physique constituent une protection suffisante pour l'utilisateur ordinaire.

# Catégoriser les vulnérabilités de sécurité

La plupart des vulnérabilités de sécurité de logiciels font partie des catégories suivantes :

**Débordement de tampon** – Cette vulnérabilité se produit lorsque les données sont écrites au-delà des limites d'un tampon. Les tampons sont des zones de mémoire affectées à une application. En modifiant les données au-delà des limites d'une mémoire tampon, l'application accède à la mémoire allouée à d'autres processus. Cela peut provoquer une panne du système, une compromission des données ou permettre une élévation des privilèges.

**Entrée non validée –** Les programmes interagissent fréquemment avec l’entrée de données. Ces données entrant dans le programme pourraient avoir un contenu malveillant, conçu pour détraquer les activités du programme. Considérons un programme qui reçoit une image à traiter. Un utilisateur malveillant pourrait concevoir un fichier image avec des dimensions d’image non valides. Les dimensions trafiquées de manière malveillante peuvent forcer le programme à répartir les tampons de tailles incorrectes et imprévues.

**Situation de concurrence –** Cette vulnérabilité se produit lorsque la sortie d’un événement dépend de sorties commandées ou planifiées. Une situation de concurrence devient une source de vulnérabilité lorsque les événements nécessaires commandés ou planifiés ne se produisent pas dans l’ordre correct ou en temps voulu.

**Failles dans les mesures de sécurité –**Les données système et les données sensibles peuvent être protégées grâce à des techniques comme l’authentification, l’autorisation et le chiffrement. Les développeurs ne doivent pas tenter de créer leurs propres algorithmes de sécurité, car cela pourrait introduire des vulnérabilités. Il est fortement conseillé aux développeurs d’utiliser les bibliothèques de sécurité déjà créées, testées et vérifiées.

**Problèmes de contrôle d’accès –**Le contrôle d’accès est le processus de contrôle des affectations, de la gestion de l’accès physique à l’équipement dictant l’accès d’une personne à une ressource, notamment un fichier, et ce qu’il peut réaliser avec ce fichier, comme lire ou modifier celui-ci. De nombreuses vulnérabilités de sécurité sont créées par l’utilisation inappropriée des contrôles d’accès.

Quasiment l’ensemble des contrôles d’accès et des pratiques de sécurité peuvent être surmontés si l’agresseur dispose d’un accès physique à l’équipement cible. Par exemple, même en définissant les autorisations d’un fichier, le système d’exploitation ne peut empêcher une personne de contourner le système d’exploitation et la lecture directe des données sur le disque. Pour protéger la machine et les données qu’elle contient, l’accès physique doit être limité et les techniques de chiffrement doivent servir à protéger les données d’un vol ou d’une corruption.

# Types de malwares

Les malwares, ou programmes malveillants, représentent tout code pouvant être utilisé pour voler des données, contourner les contrôles d’accès ou pour nuire à un système ou le compromettre. Voici quelques types communs de malware :

**Logiciel espion –** Ce malware est conçu pour suivre et espionner l’utilisateur. Le logiciel espion inclut souvent le suivi des activités, la collecte de frappes sur clavier et la capture des données. Afin de contourner les mesures de sécurité, le logiciel espion modifie souvent les paramètres de sécurité. Le logiciel espion se regroupe souvent avec des logiciels légitimes ou avec des chevaux de Troie.

**Publiciel –** Le logiciel de publicité est conçu pour fournir automatiquement des publicités. Le publiciel est souvent installé avec certaines versions du logiciel. Certains publiciels sont conçus pour ne délivrer que des publicités, mais il est également fréquent que des publiciels soient associés à des logiciels espions.

**Bot –**Du mot robot, un bot est un type de malware conçu pour effectuer automatiquement une action, généralement en ligne. Alors que la plupart des bots sont inoffensifs, une utilisation croissante des bots malveillants constitue des réseaux de zombies. Plusieurs ordinateurs sont infectés de bots programmés pour attendre tranquillement les commandes fournies par l’agresseur.

**Rançongiciel –**Ce malware est conçu pour maintenir un système informatique ou les données qu’il contient en captivité jusqu’à ce qu’un paiement soit effectué. Le ransomware fonctionne habituellement en chiffrant les données sur l’ordinateur à l’aide d’une clé inconnue de l’utilisateur. D’autres versions de ransomware peuvent tirer parti des vulnérabilités spécifiques du système pour le verrouiller. Le ransomware se transmet par un fichier téléchargé ou par une certaine vulnérabilité de logiciel.

**Scareware –**Il s’agit d’un type de malware conçu pour persuader l’utilisateur de faire une action spécifique basée sur la peur. Le scareware crée des fenêtres contextuelles factices avec la même apparence que les fenêtres de dialogue du système d’exploitation. Ces fenêtres transmettent de faux messages indiquant que le système est vulnérable ou a besoin de l’exécution d’un programme spécifique pour reprendre un fonctionnement normal. En réalité, aucun problème n’a été évalué ou détecté et si l’utilisateur accepte et lance le programme mentionné pour l’exécuter, son système sera infecté par un malware.

**Rootkit –** Ce malware est conçu pour modifier le système d’exploitation afin de créer une porte dérobée. Les agresseurs utilisent ainsi la porte dérobée pour accéder à distance à l’ordinateur. La plupart des rootkits profitent des vulnérabilités des logiciels pour effectuer une élévation de privilèges et modifier les fichiers système. Il est également fréquent que les rootkits modifient les investigations du système et les outils de surveillance, ce qui rend très difficile leur détection. Généralement, un ordinateur infecté par un rootkit doit être nettoyé et réinstallé.

**Virus –**Un virus est un code exécutable malveillant attaché à d’autres fichiers exécutables, souvent des programmes légitimes. La plupart des virus nécessitent une activation de la part de l’utilisateur final et peuvent s’activer à une heure ou une date spécifique. Les virus peuvent être inoffensifs et afficher simplement une image, ou ils peuvent être destructeurs, comme ceux qui modifient ou suppriment des données. Les virus peuvent être également programmés pour muter afin d’éviter la détection. La plupart des virus sont actuellement propagés par les lecteurs USB, les disques optiques, les partages réseau ou par e-mail.

**Cheval de Troie –**Un cheval de Troie est un type de malware qui effectue des opérations malveillantes sous le couvert d’une opération souhaitée. Ce code malveillant exploite les privilèges de l’utilisateur qui l’exécute. Souvent, les chevaux de Troie se trouvent dans des fichiers images, des fichiers audio ou des jeux. Un cheval de Troie diffère d’un virus, car il s’attache à des fichiers non exécutables.

**Vers –**Les vers sont des codes malveillants qui se répliquent en exploitant de façon indépendante les vulnérabilités au sein des réseaux. Les vers ralentissent généralement les réseaux. Alors que le virus nécessite un programme hôte pour s’exécuter, les vers peuvent fonctionner par eux-mêmes. À l’exception de l’infection initiale, ils n’exigent plus une participation de la part des utilisateurs. Après l’infection d’un hôte, le ver est capable de se propager très rapidement sur le réseau. Les vers partagent des modèles similaires. Ils s'activent par la présence d'une vulnérabilité, un moyen pour eux de se propager et contiennent tous une charge utile.

Les vers sont responsables de certaines des attaques les plus dévastatrices sur Internet. Comme le montre la Figure 1, en 2001, le ver Code Red avait infecté 658 serveurs. En l’espace de 19 heures, le ver avait infecté plus de 300 000 serveurs, comme le montre la Figure 2.

**L’homme au milieu (MitM) –**L’attaque MitM permet à l’agresseur de prendre le contrôle d’un appareil à l’insu de son utilisateur. Avec ce niveau d’accès, le pirate peut intercepter et s’emparer des informations de l’utilisateur avant de les relayer vers sa destination prévue. Les attaques MitM sont largement utilisées pour dérober des informations financières. De nombreux malware et des techniques existent pour permettre aux agresseurs d’avoir les fonctionnalités MitM.

**L’homme sur appareil mobile (MitMo) –**Une variante du MitM, MitMo est un type d’attaque utilisé pour prendre le contrôle d’un terminal mobile. Après l’infection, le terminal mobile peut recevoir l’instruction d’exfiltrer des informations sensibles de l’utilisateur et de les envoyer aux agresseurs. ZeuS, un exemple d’exploit avec des fonctionnalités MitMo, permet aux pirates de s’emparer discrètement des messages de vérification à 2 étapes envoyés aux utilisateurs.

# Les symptômes du malware

Quel que soit le type de malware infectant le système, voici les symptômes communs des malwares :

* Augmentation de l'utilisation du CPU
* Diminution de la vitesse de l'ordinateur
* L'ordinateur se fige ou tombe souvent en panne
* Diminution de la vitesse de navigation sur Internet
* Problèmes inexplicables avec les connexions réseau
* Des fichiers sont modifiés
* Des fichiers sont supprimés
* Présence de fichiers, de programmes ou d’icônes de bureau inconnus ;
* Des processus inconnus sont exécutés
* Des programmes s'éteignent ou se reconfigurent
* Envoi d'e-mail à l'insu de l'utilisateur ou sans son consentement

Piratage psychologique

Le piratage psychologique est une attaque d’accès qui tente de manipuler les individus dans l’exécution d’actions ou dans la divulgation d’informations confidentielles. Les pirates psychologiques comptent souvent sur la volonté des personnes pour que cela soit efficace, mais aussi sur l’exploitation des faiblesses des personnes. Par exemple, un agresseur pourrait appeler un employé autorisé pour un problème urgent qui nécessite un accès réseau immédiat. L'agresseur pourrait faire appel à la vanité de l'employé, invoquer l'autorité en utilisant des techniques de « name-dropping » en citant des noms ou en faisant appel à la cupidité de l'employé.

Voici quelques types d'attaques d'ingénierie sociale :

* **Usurpation** – Lorsqu'un agresseur appelle un individu et lui ment dans une tentative d'accéder à des données privilégiées. Un exemple implique un agresseur qui prétend avoir besoin de données personnelles ou financières afin de confirmer l’identité du destinataire.
* **Talonnage (tailgating)** – Lorsqu’un agresseur suit rapidement une personne autorisée dans un endroit sécurisé.
* **Une chose pour une autre (contrepartie)** – Lorsqu’un agresseur demande des informations personnelles d’une partie en échange de quelque chose, comme un don gratuit.

# Décryptage de mot de passe Wi-Fi

Le décryptage de mot de passe Wi-Fi est le processus d’identification du mot de passe utiliser pour protéger un réseau sans fil. Voici quelques techniques de décryptage de mot de passe :

**Piratage psychologique** – L’agresseur manipule une personne qui connaît le mot de passe pour le lui fournir.

**Attaques brutales** – L’agresseur tente plusieurs mots de passe possibles pour tenter de deviner le mot de passe. Si le mot de passe est un numéro à 4 chiffres, par exemple, l’agresseur devra essayer chacune des 10 000 combinaisons. Les attaques brutales impliquent généralement un fichier contenant une liste de mots. Il s’agit d’un fichier texte contenant une liste de mots tirés d’un dictionnaire. Ensuite, un programme tente chaque mot et chaque combinaison commune. Du fait que les attaques brutales prennent du temps, l’identification des mots de passe complexes dure beaucoup plus longtemps. Les outils pour le décryptage de mots de passe par attaque brutale incluent Ophcrack, L0phtCrack, THC Hydra, RainbowCrack et Medusa.

**Reniflement de réseau –**En étant attentif et en s’emparant des paquets envoyés sur le réseau, un agresseur peut être en mesure de découvrir le mot de passe si le mot de passe envoyé n’est pas chiffré (en texte brut). Si le mot de passe est chiffré, l’agresseur peut encore être en mesure de le découvrir à l’aide d’un outil de décryptage de mots de passe.

# Hameçonnage

L’hameçonnage se produit lorsqu’un tiers malveillant envoie un e-mail frauduleux comme provenant d’une source de confiance légitime. L’objectif du message est de piéger le destinataire sur l’installation d’un malware sur son appareil ou sur le partage d’informations personnelles ou financières. Un exemple d’hameçonnage est un e-mail factice ayant l’apparence de celui envoyé par un magasin, demandant à l’utilisateur de cliquer sur un lien pour demander un prix. Le lien peut diriger vers un faux site demandant des informations personnelles, ou installer un virus.

L’hameçonnage ciblé est une attaque d’hameçonnage très ciblée. Même si l’hameçonnage et l’hameçonnage ciblé utilisent tous les deux des e-mails pour atteindre les victimes, les e-mails de l’hameçonnage ciblé sont personnalisés pour une personne spécifique. L’agresseur recherche les intérêts de la cible avant d’envoyer l’e-mail. Par exemple, un agresseur apprend que la cible s’intéresse aux voitures et qu’il recherchait un modèle spécifique de voiture. L’agresseur rejoint le même forum de discussion sur les voitures où la cible est membre, crée une fausse mise en vente de voiture et envoie un courrier électronique à la cible. L’e-mail contient un lien vers les photos de la voiture. Lorsque la cible clique sur le lien, le malware est installé sur son ordinateur.

# Exploitation des vulnérabilités

L’exploitation des vulnérabilités est une autre méthode commune d’infiltration. Les agresseurs vont analyser les ordinateurs pour obtenir des informations à leur sujet. Voici une méthode commune pour exploiter les vulnérabilités :

**Étape 1.** Recueillir des informations sur le système cible. Le recueil peut se faire de plusieurs façons différentes, à l’aide d’un scanner de port ou du piratage psychologique. L’objectif est d’en apprendre autant que possible sur l’ordinateur cible.

**Étape 2**. L’un des éléments d’information pertinents appris lors de l’étape 1 pourrait être le système d’exploitation, sa version et une liste des services qui sont en cours d’exécution.

**Étape 3**. Lorsque le système d’exploitation et la version d’exploitation de la cible sont connus, l’agresseur recherche les vulnérabilités spécifiques connues sur cette version de système d’exploitation ou sur d’autres services du système d’exploitation.

**Étape 4**. Lorsqu’une vulnérabilité est détectée, l’agresseur cherche à utiliser un exploit déjà écrit. Si aucun exploit n’a été écrit, l’agresseur peut envisager d’écrire un exploit.

La Figure 1 illustre un agresseur utilisant **WHOIS**, une base de données Internet public contenant des informations sur les noms de domaine et leurs utilisateurs inscrits. La Figure 2 illustre un agresseur utilisant l'outil **NMAP**, un célèbre scanner de port. Avec un scanner de port, un agresseur peut sonder les ports d’un ordinateur cible pour en apprendre davantage sur les services en cours d’exécution sur cet ordinateur.

**Menaces persistantes avancées**

L’un des moyens pour réussir une infiltration est l’utilisation des menaces persistantes avancées. Elles consistent en un fonctionnement furtif et avancé, à plusieurs stades, et à long terme, contre une cible spécifique. En raison de son niveau de complexité et des compétences requises, une menace persistante avancée est généralement bien financée. Une menace persistante avancée cible les entreprises ou les nations pour des raisons commerciales ou politiques.

Habituellement liée à l’espionnage basé sur le réseau, la menace persistante avancée vise à déployer un malware personnalisé sur un ou plusieurs des systèmes de la cible sans se faire détecter. Avec plusieurs stades de fonctionnement et plusieurs types de malware personnalisés qui affectent différents appareils et effectuent des fonctions spécifiques, un seul agresseur ne dispose souvent pas de l’ensemble des compétences, des ressources ou de la persévérance pour mener à bien les menaces persistantes avancées

# DoS

Les attaques par déni de service représentent un type d’attaque réseau. Une attaque par déni de service se traduit par un type d’interruption de service de réseau sur les utilisateurs, les périphériques ou les applications. Il existe deux types majeurs d’attaques par déni de service :

**Quantité encombrante de trafic –** Elle se produit lorsqu’un réseau, un hôte ou une application reçoit une énorme quantité de données à un rythme qui ne peut pas être géré. Cela provoque un ralentissement de la transmission ou de la réponse, ou une panne d’un appareil ou d’un service.

**Paquets formatés de manière malveillante –**Cela se produit lorsqu’un paquet formaté de manière malveillante est envoyé à un hôte ou à l’application et le destinataire est incapable de le traiter. Par exemple, un agresseur transmet des paquets contenant des erreurs qui ne peuvent être identifiées par l’application ou il transmet des paquets mal formatés. Cela provoque un ralentissement de l’appareil récepteur ou une panne.

Les attaques par déni de service sont considérées comme un risque majeur, car elles peuvent facilement interrompre la communication et entraîner une perte importante de temps et d’argent. Ces attaques sont relativement simples à effectuer, même par un agresseur non qualifié.

# DDoS

Une attaque par déni de service distribué (attaque DDoS) est similaire à une attaque par déni de service (attaque DoS), mais elle provient de sources multiples et coordonnées. À titre d’exemple, une attaque par déni de service distribuée peut procéder comme suit :

Un agresseur établit un réseau d'hôtes infectés, appelé réseau de zombies. Les hôtes infectés sont appelés des zombies. Les zombies sont contrôlés par des systèmes de gestionnaire.

Les ordinateurs zombies analysent et infectent constamment plus d’hôtes, et créent ainsi plus de zombies. Une fois prêt, le hacker demande aux systèmes de gestionnaire d’effectuer une attaque par déni de service distribuée par le biais du réseau de zombies.

Cliquez sur Lecture dans la figure pour afficher les animations d’une attaque par déni de service distribuée.

# Empoisonnement par SEO

Les moteurs de recherche comme Google fonctionnent en classant des pages et en présentant les résultats pertinents en fonction des requêtes de recherche des utilisateurs. En fonction de la pertinence du contenu du site Web, celui-ci peut se situer plus haut ou plus bas sur la liste des résultats de recherche. L’optimisation pour les moteurs de recherche ou SEO est un ensemble de techniques utilisées pour améliorer le classement d’un site Web par un moteur de recherche. Alors que de nombreuses entreprises légitimes se spécialisent dans l’optimisation de sites Web pour mieux se positionner, un utilisateur malveillant pourrait utiliser une SEO pour créer un site Web malveillant qui apparaîtrait au sommet des résultats de recherche. Cette technique est appelée empoisonnement par SEO.

L’objectif le plus commun de l’empoisonnement par SEO est d’augmenter le trafic vers des sites malveillants qui peuvent héberger un malware ou effectuer un piratage psychologique. Pour forcer un site malveillant à se classer au sommet des résultats de recherche, les agresseurs tirent parti des termes de recherche populaires.

# Qu'est-ce qu'une attaque mixte ?

Les attaques mixtes sont des attaques qui utilisent plusieurs techniques pour compromettre une cible. En utilisant plusieurs techniques d’attaque différentes simultanément, les agresseurs disposent de malware qui représentent un mélange de vers, de chevaux de Troie, de logiciels espions, d’enregistreurs de frappe, de pourriels et de plans d’hameçonnage. Cette tendance des attaques mixtes est révélatrice de malware plus complexes et met les données des utilisateurs en grand danger.

Le type d’attaque mixte le plus courant utilise des pourriels, des messages instantanés ou des sites légitimes pour distribuer des liens dans lesquels un malware ou un logiciel espion est secrètement téléchargé sur l’ordinateur. Une autre attaque mixte commune utilise les attaques par déni de service distribuée combinées à des e-mails d’hameçonnage. Tout d’abord, l’attaque par déni de service distribuée est utilisée pour détraquer le site Web d’une banque populaire et envoyer des e-mails aux clients de la banque en s’excusant pour la gêne occasionnée. L’e-mail dirige également les utilisateurs vers un site d’urgence factice où leurs vraies informations de connexion peuvent être volées.

La plupart des vers informatiques les plus néfastes comme Nimbda, CodeRed, BugBear, Klez et Slammer sont davantage catégorisés comme des attaques mixtes, comme indiqué ci-dessous :

* Certaines variantes de Nimbda ont utilisé les pièces jointes d’e-mail, les téléchargements de fichier à partir d’un serveur Web compromis et le partage de fichiers Microsoft (par exemple, des partages anonymes) comme méthodes de propagation.
* D’autres variantes de Nimbda ont été en mesure de modifier les comptes invités du système pour fournir à l’agresseur ou au code malveillant des privilèges administratifs.

Les récents vers Conficker et ZeuS/LICAT étaient également des attaques mixtes. Conficker a utilisé toutes les méthodes de distribution classiques.

# Qu’est-ce que la réduction d’impact ?

Même si, de nos jours, la majorité des entreprises prospères sont conscientes des problèmes de sécurité courants et ont déployé des efforts considérables pour les éviter, aucun système de sécurité n'est efficace à 100 %. Etant donné qu’une faille est susceptible de se produire si la valeur est importante, les entreprises et les organisations doivent également être disposées à limiter les dégâts.

Il est important de comprendre que l’impact d’une faille est non seulement lié à son aspect technique, aux données volées, aux bases de données endommagées ou à l’atteinte à la propriété intellectuelle, mais également au préjudice pour la réputation de l’entreprise. La riposte à une violation de données est un processus très dynamique.

Voici quelques mesures importantes qu’une entreprise doit prendre lorsqu’une faille de sécurité est identifiée, selon l’avis de nombreux experts de la sécurité :

* Communiquez le problème. Les employés en interne doivent être informés du problème et appelés à agir. En dehors de l'entreprise, les clients doivent être informés par une communication directe et des annonces officielles. La communication crée la transparence, ce qui est crucial dans ce type de situation.
* Soyez sincère et responsable si l'entreprise est responsable.
* Fournissez des détails. Expliquez les raisons de la situation et ce qui a été compromis. Il est également prévu que l'entreprise prenne en charge les coûts des services de protection d'usurpation d'identité pour les clients concernés.
* Essayez de comprendre ce qui a causé la faille et l'a facilitée. Si nécessaire, embauchez des enquêteurs en informatique pour rechercher et étudier les détails.
* Appliquez ce qui a été appris au cours de l'enquête pour vous assurer que des failles similaires ne se produisent plus à l'avenir.
* Vérifiez que tous les systèmes sont sains, qu'aucune porte dérobée n'est installée et que rien d'autre n'a été compromis. Les agresseurs tenteront souvent de laisser une porte dérobée pour faciliter les failles futures. Assurez-vous que cela ne se produise pas.
* Formez les employés, les partenaires et les clients sur la méthode de prévenir des failles futures.

# Conclusion

Ce chapitre a traité les moyens utilisés par les professionnels de la cybersécurité pour analyser les faits survenus suite à une cyberattaque. Cela explique les vulnérabilités des logiciels et du matériel de sécurité, ainsi que les différentes catégories de vulnérabilité de la sécurité.

Les différents types de logiciels malveillants (appelés malware) et les symptômes des malwares ont été expliqués. Certains des malwares abordés incluent les virus, les vers, les chevaux de Troie, les logiciels espions, les publiciels, etc.

Les différents moyens utilisés par les agresseurs pour infiltrer un système ont été abordés, notamment le piratage psychologique, le décryptage de mot de passe Wi-Fi, l’hameçonnage et l’exploitation d’une vulnérabilité. Les différents types d’attaques par déni de service ont également été expliqués.

Les attaques mixtes utilisent différentes techniques pour infiltrer et pour attaquer un système. Un grand nombre des vers informatiques les plus néfastes comme Nimbda, CodeRed, BugBear, Klez et Slammer sont davantage catégorisés comme des attaques mixtes. Lorsqu’une attaque ne peut être évitée, il incombe au professionnel de la cybersécurité de réduire l’impact de cette attaque.

Si vous souhaitez découvrir plus en détail les concepts de ce chapitre, référez-vous à la page des [ressources et activités supplémentaires](https://contenthub.netacad.com/legacy/I2CS/2.1/fr/course/files/IntroCybersecurity%20-%20Additional%20Resources%20and%20Activities.pdf) dans les Ressources des étudiants.