CHAPITRE 1 : INFORMATIONS GENRALES SUR LA SECURITE INFORMATIQUE

Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information. Il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.

Introduction à la sécurité

Le **risque** en termes de sécurité est généralement caractérisé par l'équation suivante :

$$\text{Risque} = \frac{\text{Menace x Vulnérabilité}}{\text{Contre-mesure}}$$

La **menace** (en anglais « threat ») représente le type d'action susceptible de nuire dans l'absolu.

La **vulnérabilité** (en anglais « *vulnerability* », appelée parfois *faille* ou *brèche*) représente le niveau d'exposition face à la menace dans un contexte particulier.

La **contre-mesure** est l'ensemble des actions mises en œuvre en prévention de la menace.

Les contre-mesures à mettre en œuvre ne sont pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un ensemble de règles clairement définies.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'ennemi. Le but étant de donner un aperçu des motivations éventuelles des pirates, de catégoriser ces derniers, et enfin de donner une idée de leur façon de procéder afin de mieux comprendre comment il est possible de limiter les risques d'intrusions.

Objectifs de la sécurité informatique

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger.

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

La sécurité informatique vise généralement cinq principaux objectifs :

- L'**intégrité**, c'est-à-dire garantir que les données sont bien celles que l'on croit être ;
- La **confidentialité**, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ;
- La **disponibilité**, permettant de maintenir le bon fonctionnement du système d'information ;
- La **non répudiation**, permettant de garantir qu'une transaction ne peut-être niée ;
- L'**authentification**, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

La confidentialité

La **confidentialité** consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.

L'intégrité

Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).

La disponibilité

L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources.

La non-répudiation

La **non-répudiation** de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.

L'authentification

L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot

de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.

Nécessité d'une approche globale

La sécurité d'un système informatique fait souvent l'objet de métaphores. En effet, on la compare régulièrement à une chaîne en expliquant que le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue.

Cela signifie que la sécurité doit être abordée dans un contexte global et notamment prendre en compte les aspects suivants :

- **La sensibilisation des utilisateurs aux problèmes de sécurité** ;
- **La sécurité logique**, c'est-à-dire la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation ;
- **La sécurité des télécommunications : technologies réseau, serveurs de l'entreprise, réseaux d'accès, etc.**
- **La sécurité physique**, soit *la sécurité au niveau des infrastructures matérielles* : salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail des personnels, etc.

Mise en place d'une politique de sécurité

La sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés.

Ainsi, la sécurité informatique doit être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance.

C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une **politique de sécurité**, dont la mise en œuvre se fait selon les quatre étapes suivantes :

- Identifier les besoins en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;

- Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ;
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

La politique de sécurité est donc l'ensemble des orientations suivies par une organisation (à prendre au sens large) en termes de sécurité. A ce titre elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système.

A cet égard, il ne revient pas aux seuls administrateurs informatiques de définir les droits d'accès des utilisateurs mais aux responsables hiérarchiques de ces derniers. Le rôle de l'administrateur informatique est donc de s'assurer que les ressources informatiques et les droits d'accès à celles-ci sont en cohérence avec la politique de sécurité définie par l'organisation.

De plus, étant donné qu'il est le seul à connaître parfaitement le système, il lui revient de faire remonter les informations concernant la sécurité à sa direction, éventuellement de conseiller les décideurs sur les stratégies à mettre en œuvre, ainsi que d'être le point d'entrée concernant la communication à destination des utilisateurs sur les problèmes et recommandations en termes de sécurité.

La sécurité informatique de l'entreprise repose sur une bonne connaissance des règles par les employés, grâce à des actions de formation et de sensibilisation auprès des utilisateurs, mais elle doit aller au-delà et notamment couvrir les champs suivants :

- Un dispositif de sécurité physique et logique, adapté aux besoins de l'entreprise et aux usages des utilisateurs ;
- Une procédure de management des mises à jour ;
- Une stratégie de sauvegarde correctement planifiée ;
- Un plan de reprise après incident ;
- Un système documenté à jour.

Les causes de l'insécurité

On distingue généralement deux types d'insécurités :

- **L'état actif d'insécurité**, c'est-à-dire la non connaissance par l'utilisateur des fonctionnalités du système, dont certaines pouvant lui être nuisibles

(par exemple le fait de ne pas désactiver des services réseaux non nécessaires à l'utilisateur).

- **L'état passif d'insécurité**, c'est-à-dire la méconnaissance des moyens de sécurité mis en place, par exemple lorsque l'administrateur (ou l'utilisateur) d'un système ne connaît pas les dispositifs de sécurité dont il dispose.

Définition des besoins en termes de sécurité de l'information

Phase de définition

La phase de définition des besoins en termes de sécurité est la première étape vers la mise en œuvre d'une politique de sécurité.

L'objectif consiste à déterminer les besoins de l'organisation en faisant un véritable état des lieux du système d'information, puis d'étudier les différents risques et la menace qu'ils représentent afin de mettre en œuvre une politique de sécurité adaptée.

La phase de définition comporte ainsi trois étapes :

- L'identification des besoins ;
- L'analyse des risques ;
- La définition de la politique de sécurité.

Identification des besoins

La phase d'identification des besoins consiste dans un premier temps à faire l'inventaire du système d'information, notamment pour les éléments suivants :

- Personnes et fonctions ;
- Matériels, serveurs et les services qu'ils délivrent ;
- Cartographie du réseau (plan d'adressage, topologie physique, topologie logique, etc.);
- Liste des noms de domaine de l'entreprise ;
- Infrastructure de communication (routeurs, commutateurs, etc.) ;
- Données sensibles.

Analyse des risques

L'étape d'analyse des risques consiste à répertorier les différents risques encourus, d'estimer leur probabilité et enfin d'étudier leur impact.

La meilleure approche pour analyser l'impact d'une menace consiste à estimer le coût des dommages qu'elle causerait (par exemple attaque sur un serveur ou détérioration de données vitales pour l'entreprise).

Sur cette base, il peut être intéressant de dresser un tableau des risques et de leur potentialité, c'est-à-dire leur probabilité de se produire, en leur affectant des niveaux échelonnés selon un barème à définir, par exemple :

- Sans objet (ou improbable) : la menace n'a pas lieu d'être ;
- Faible : la menace a peu de chance de se produire ;
- Moyenne : la menace est réelle ;
- Haute : la menace a de grandes chances de se produire.

Définition de la politique de sécurité

La politique de sécurité est le document de référence définissant les objectifs poursuivis en matière de sécurité et les moyens mis en œuvre pour les assurer.

La politique de sécurité définit un certain nombre de règles, de procédures et de bonnes pratiques permettant d'assurer un niveau de sécurité conforme aux besoins de l'organisation.

Un tel document doit nécessairement être conduit comme un véritable projet associant des représentants des utilisateurs et conduit au plus haut niveau de la hiérarchie, afin qu'il soit accepté par tous. Lorsque la rédaction de la politique de sécurité est terminée, les clauses concernant le personnel doivent leur être communiquées, afin de donner à la politique de sécurité le maximum d'impact.

Méthodes

Il existe de nombreuses méthodes permettant de mettre au point une politique de sécurité. Voici une liste non exhaustive des principales méthodes :

- **MEHARI** (*Méthode Harmonisée d'Analyse de Risques*) développée et distribuée en mode Open Source par le CLUSIF;
    - https://www.clusif.asso.fr/fr/production/mehari/

- **EBIOS** (*Expression des Besoins et Identification des Objectifs de Sécurité*), mise au point par la DCSSI (*Direction Centrale de la Sécurité des Systèmes d'Information*) ;
    - http://www.ssi.gouv.fr/fr/confiance/ebios.html

Mise en œuvre de moyens de sécurisation

Phase de mise en œuvre

La phase de mise en œuvre consiste à déployer des moyens et des dispositifs visant à sécuriser le système d'information ainsi que de faire appliquer les règles définies dans la politique de sécurité.

Les principaux dispositifs permettant de sécuriser un réseau contre les intrusions sont les systèmes pare-feu. Néanmoins ce type de dispositif ne protège pas la confidentialité des données circulant sur le réseau.

Ainsi, la plupart du temps il est nécessaire de recourir à des applications implémentant des algorithmes cryptographiques permettant de garantir la confidentialité des échanges.

La mise en place de tunnels sécurisés (VPN) permet d'obtenir un niveau de sécurisation supplémentaire dans la mesure où l'ensemble de la communication est chiffré.

Audits de sécurité

Notion d'audit

Un **audit de sécurité** (en anglais *security audit*) consiste à s'appuyer sur un tiers de confiance (généralement une société spécialisée en sécurité informatique) afin de valider les moyens de protection mis en œuvre, au regard de la politique de sécurité.

L'objectif de l'audit est ainsi de vérifier que chaque règle de la politique de sécurité est correctement appliquée et que l'ensemble des dispositions prises forme un tout cohérent.

Un audit de sécurité permet de s'assurer que l'ensemble des dispositions prises par l'entreprise sont réputées sûres.

Quelques terminologies importantes en sécurité

- **Menace** : c'est une action ou un événement. C'est la violation potentielle des mesures de sécurité d'un réseau. Une menace peut affecter l'intégrité ou la disponibilité d'une information ;
- **Vulnérabilité** : elle représente, une faiblesse ou une brèche au sein du système d'information d'une entreprise. Elle est due à une erreur de conception ou d'implémentation qui une fois exploitée, permet de compromettre la sécurité du système ;
- **Attaque** : toute action qui consiste à s'introduire au sein du système informatique à travers une vulnérabilité. C'est donc toute action qui va violer les mesures de sécurités mises en place afin de prendre le contrôle d'un système ;
- Un **système informatique** est l'ensemble d'équipements informatiques mis en commun dans le but de traiter l'information ;
- Un **système d'information** est l'ensemble des éléments participant à la gestion, au traitement, au transport, au stockage et à la diffusion de l'information au sein d'une organisation.

Protection - Introduction à la sécurité des réseaux

Qu'est-ce que la sécurité d'un réseau ?

La sécurité d'un réseau est un niveau de garantie que l'ensemble des machines du réseau fonctionnent de façon optimale et que les utilisateurs desdites machines possèdent uniquement les droits qui leur ont été octroyés.

Il peut s'agir :

- D'empêcher des personnes non autorisées d'agir sur le système de façon malveillante ;
- D'empêcher les utilisateurs d'effectuer des opérations involontaires capables de nuire au système ;
- De sécuriser les données en prévoyant les pannes ;
- De garantir la non-interruption d'un service.

Les causes de l'insécurité

On distingue généralement deux types d'insécurité :

- **L'état actif d'insécurité**, c'est-à-dire la non-connaissance par l'utilisateur des fonctionnalités du système, dont certaines pouvant lui être nuisibles (par exemple la non-désactivation de services réseaux non nécessaires à l'utilisateur)
- **L'état passif d'insécurité**, c'est-à-dire lorsque l'administrateur (ou l'utilisateur) d'un système ne connaît pas les dispositifs de sécurité dont il dispose.

Le but des agresseurs

Les motivations des agresseurs que l'on appelle communément "pirates" peuvent être multiples :

- L'attirance de l'interdit ;
- Le désir d'argent (violer un système bancaire par exemple) ;
- Le besoin de renommée (impressionner des amis) ;
- L'envie de nuire (détruire des données, empêcher un système de fonctionner).

Procédé des agresseurs

Le but des agresseurs est souvent de prendre le contrôle d'une machine afin de pouvoir réaliser les actions qu'ils désirent. Pour cela il existe différents types de moyens :

- L'obtention d'informations utiles pour effectuer des attaques ;
- L'utilisation des failles d'un système ;
- L'utilisation de la force pour casser un système.

Comment se protéger ?

- Se tenir au courant ;
- Connaître le système d'exploitation ;
- Réduire l'accès au réseau (firewall) ;
- Réduire le nombre de points d'entrée (ports) ;
- Définir une politique de sécurité interne (mots de passe, lancement d'exécutables) ;
- Déployer des utilitaires de sécurité (journalisation).

Détection des incidents de sécurité

Phase de détection d'incidents

Afin d'être complètement fiable, un système d'information sécurisé doit disposer de mesures permettant de détecter les incidents.

Il existe ainsi des systèmes de détection d'intrusion (notés *IDS* pour *Intrusion Detection Systems*) chargés de surveiller le réseau et capables de déclencher une alerte lorsqu'une requête est suspecte ou non conforme à la politique de sécurité.

La disposition de ces sondes et leur paramétrage doivent être soigneusement étudiés car ce type de dispositif est susceptible de générer de nombreuses fausses alertes.

Tests d'intrusion

- Tests d'intrusion

Tests d'intrusion

Les **tests d'intrusion** (en anglais *penetration tests*, abrégés en *pen tests*) consistent à éprouver les moyens de protection d'un système d'information en essayant de s'introduire dans le système en situation réelle.

On distingue généralement deux méthodes distinctes :

- La méthode dite « boîte noire » (en anglais « *black box* ») consistant à essayer d'infiltrer le réseau sans aucune connaissance du système, afin de réaliser un test en situation réelle ;
- La méthode dite « boîte blanche » (en anglais « *white box* ») consistant à tenter de s'introduire dans le système en ayant connaissance de l'ensemble du système, afin d'éprouver au maximum la sécurité du réseau.

Une telle démarche doit nécessairement être réalisée avec l'accord (par écrit de préférence) du plus haut niveau de la hiérarchie de l'entreprise, dans la mesure où elle peut aboutir à des dégâts éventuels et étant donné que les méthodes mises en œuvre sont interdites par la loi en l'absence de l'autorisation du propriétaire du système.

Un test d'intrusion, lorsqu'il met en évidence une faille, est un bon moyen de sensibiliser les acteurs d'un projet. A contrario, il ne permet pas de garantir la sécurité du système, dans la mesure où des vulnérabilités peuvent avoir échappé aux testeurs.

Les audits de sécurité permettent d'obtenir un bien meilleur niveau de confiance dans la sécurité d'un système étant donné qu'ils prennent en compte des aspects organisationnels et humains et que la sécurité est analysée de l'intérieur.

Plusieurs outils existent actuellement afin d'effectuer ces tests. On retiendra particulièrement le projet Metasploit développé par HD Moore.

La sécurité vise donc à sécuriser:

- **L'émetteur** : il s'agit de l'objet qui initie la communication. Cet objet peut être un processus, un système d'exploitation, un utilisateur, un navigateur, une application etc.
- **Le récepteur :** il s'agit de l'objet qui reçoit la communication. Cet objet peut être un processus, un système d'exploitation, un utilisateur, un serveur etc..

- **Le canal de communication :** il s'agit du moyen par lequel l'émetteur et le récepteur communique. Il s'agit d'un canal sans fil, d'un canal filaire, de la mémoire, etc…
- **Des protocoles de communication :** Il s'agit d'un ensemble convenu de règles de communication entre les deux communicateurs. Comme exemple, on peut avoir le protocole HTTP (HyperText Transfer Protocol).
  - De prévenir un système d'information des attaques multiformes (gestion des risques)
  - D'empêcher qu'une attaque prenne effet (supervision (IDS))
  - De maintenir un système informatique en état de fonctionner normalement dans le but de restreindre l'accès à certaines informations aux utilisateurs autorisés à les consulter.

Démarche de la sécurité

Elle renvoie à une chaine de valeurs constituée des utilisateurs, des informations et du matériel qui doivent être protégés afin de garantir la sécurité du système d'information. Pour atteindre ce but, nous devons faire appel à une démarche clairement définie.

La sécurité d'un système d'information obéit à des règles, logiques ou méthodes qu'on peut résumer en cinq étapes à savoir : la protection, la supervision, la détection, l'analyse et la réponse.

- **La protection :** Le processus visant à empêcher les intrus d'accéder aux ressources du système. Les barrières incluent les pares-feux, les zones démilitarisées (DMZ) et l'utilisation d'éléments d'accès comme les clés, les cartes d'accès, la biométrie et autres pour ne permettre l'accès aux ressources qu'aux utilisateurs autorisés ;
- **La supervision :** examiner et récolter n'importe quelle information relative aux anomalies au sein du réseau informatique telles que les attaques, les accès non autorisés
- **La détection :** la détection se produit lorsque l'intrus a réussi ou est en train d'accéder au système. Les alertes à l'existence d'un intrus représentent sont exploitées comme signal de détection. Parfois, ces

alertes peuvent être en temps réel ou stockées pour une analyse approfondie par le personnel de sécurité. Les systèmes de détection d'intrusion en général et les antivirus en particulier sont des exemples ;

- **L'analyse :** elle implique différentes actions et méthodes qui ont pour but de confirmer un incident, de trouver la cause initiale et de pouvoir planifier les différentes actions à prendre face à cet incident

- **La réponse :** Il s'agit d'un mécanisme post-effet qui tente de répondre à l'échec des quatre premiers mécanismes. Cela fonctionne en essayant d'arrêter et / ou empêcher de futurs dommages ou l'accès à une installation. La réponse est très importante pour ralentir la contamination de l'infiltration.

Quelques outils de sécurité

Pour sécuriser un réseau interne, on utilise généralement les outils de sécurité tels :

- Les antivirus;
- Les outils de détection d'intrusion dont le rôle est de détecter une attaque et d'alerter l'administrateur, ou de détecter toute autre activité normale ou anormale du réseau;
- Les pare feu dans lesquels sont écrites des règles de sécurité visant à protéger le réseau contre les accès externes;
- Les outils de prévention d'intrusion dont le rôle est de détecter, bloquer une attaque et d'alerter l'administrateur ;
- Les listes de contrôle d'accès qui sont des règles écrites dans un routeur pour gérer le réseau interne.

Les antivirus

Un logiciel antivirus est une application indépendante ou suite de programmes capables de détecter et supprimer des virus présents sur des ordinateurs et réseaux. Les logiciels antivirus modernes protègent aussi vos appareils contre tout type de logiciel malveillant, notamment des vers informatiques, chevaux de Troie, publiciels, logiciels espion, pirates de navigateur, enregistreurs de frappe et rootkits.

Fonctionnement :

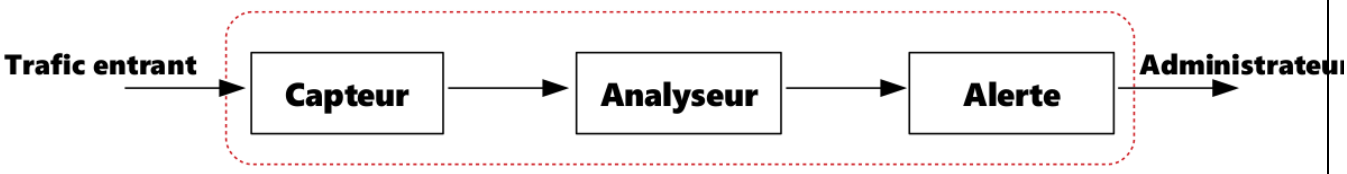
Lorsque vous effectuez un scan à la recherche d'un virus, votre programme antivirus balaye votre disque dur ainsi que tous les appareils de stockage externes qui y sont reliés. Le programme inspecte chaque fichier individuel et compare simultanément ses résultats dans sa base de données de virus connus pour détecter une menace potentielle.

Le cas échéant, en fonction de la gravité de la menace, il peut supprimer, mettre en quarantaine ou réparer le fichier infecté. Le programme surveille aussi le comportement de tous les logiciels installés sur votre ordinateur à la recherche de signes indicateurs de danger.

La détection d'intrusions (IDS/IPS)

La détection des intrusions regroupe les méthodes et les systèmes capables de détecter les actes de malveillance ou tout simplement des actes qui ne sont pas conformes à la « politique de sécurité. Un outil de détection d'intrusion (IDS) permet donc à un administrateur réseau de déceler tout comportement anormal ou trafic suspect. On en distingue trois variantes :

- **Le système** : l'IDS a alors pour but d'analyser le fonctionnement du système. On parle de HIDS (Host Intrusion Detection System) ;
- **Le réseau :** l'IDS anayse le trafic réseau afin de détecter des communications non autorisées. On parle de NIDS (Network Intrusion Detection System) ;
- **Les systèmes et les réseaux :** on parle d'IDS hybrides ; Ils combinent des HIDS et des NIDS.



Fonctionnement d'un IDS

- **Collecte d'informations** : elle peut être réalisée par divers dispositifs d'acquisition de données tels que les sondes ;
- **Analyse des informations collectées :** ces dernières sont comparées à des données déjà connues (données de référence) permettant de juger du caractère hostile du trafic ou du processus
- **Réaction :** en cas de détection d'une anomalie, l'IDS peut déclencher une alerte (logs, SMS, mail, téléphone, etc.) et apporter une réponse s'il y en a une qui est prévue.
- Après comparaison avec des données de référence, l'analyse doit permettre de dire si le fonctionnement anormal est détecté ou pas.

Dans certains cas, le système peut se tromper et générer :

- ✓ **Des faux-positifs** : une anomalie ou une attaque est détectée alors qu'il n'en est rien (on est face à une situation non hostile, mais peut-être peu habituelle) ;
- ✓ **Des faux-négatifs** : l'IDS ne déclenche pas d'alerte alors qu'on est en présence d'un risque pour le système (présence d'une attaque par exemple).

Différence entre IDS et IPS

- Les IDS et IPS sont des dispositifs de sécurité qui s'intéressent aux intrusions ayant traversé les pares-feux ;
- Ils sont donc localisés à l'intérieur du réseau l'IDS détecte des instruisons ou des anomalies dans le système ou le réseau et envoie des notifications ou alertes ;
- L'IPS, en plus de réaliser une IDS peut réagir activement en bloquant par exemple un trafic.

Exemples d'IDS/IPS : SNORT, BRO, OSSEC, SURICATA

Les pares feux

Rôles d'un pare-feu

Le pare-feu (en anglais firewall) est une protection située à l'entrée du réseau et sur les ordinateurs, visant à empêcher toute intrusion sur le réseau. Un pare-feu surveille

simplement le trafic entrant et sortant sur un appareil, en recherchant tout signe d'activité malveillante. S'il détecte quelque chose de suspect, il le bloque instantanément pour l'empêcher d'atteindre sa destination. Il joue un rôle capital dans un réseau informatique :

- **Les intrusions** : Les pare-feu empêchent les utilisateurs non autorisés d'accéder à votre ordinateur ou à votre serveur à distance et de faire ce qu'ils veulent.
- **Les logiciels malveillants (malware) :** Les attaquants qui parviennent à s'infiltrer peuvent envoyer des logiciels malveillants pour vous infecter ou infecter votre serveur. Les logiciels malveillants peuvent voler des informations personnelles, se propager à d'autres utilisateurs ou endommager votre ordinateur de toute autre manière.
- **Des attaques par force brute :** Tentatives de pirates informatiques pour essayer des centaines de combinaisons d'identifiants et de mots de passe afin de découvrir vos informations de connexion d'administrateur (ou d'autres utilisateurs).
- **Attaques DDoS :** Les pare-feu (en particulier les pares-feux d'applications web) peuvent tenter de détecter l'afflux de faux trafic qui se produit lors d'une attaque DDoS.

Les fonctionnalités d'un pare-feu

Selon les fonctionnalités prises en charge par le pare-feu, le trafic peut être autorisé ou bloqué par diverses techniques qui offrent différents niveaux de protection : ***Filtrage des entrées de la carte réseau, Filtrage statique de paquets, Traduction d'adresses réseau (NAT), Inspection dynamique, Analyse des circuits, Filtrage applicatif.***

Le contrôle d'accès

Définitions

« Un modèle de contrôle d'accès est un formalisme (souvent mathématique) permettant d'exprimer les droits d'accès des sujets (ou acteurs) sur les objets ». Une politique de contrôle d'accès permet de définir les règles à respecter afin de garantir un accès sécurisé aux informations confidentielles. Le contexte comprend :

- **Authentification** : composant qui vérifie que les Identifiants de l'utilisateur sont valides ;
- **Autorisation (gestion des) :** vérifications des droits ou autorisations à exécuter des opérations sur les ressources du système ;
- **Audit :** Composante qui garde des traces des opérations effectuées (Sujets, Objets,Date). L'audit est important en ce sens qu'il permet de faire Une évaluation du contrôle d'accès, Une détection de violation de mesures de sécurité, Une recommandation d'améliorations futures

Les politiques de contrôle d'accès

On distingue plusieurs politiques de contrôle d'accès. Dans le cadre de ce cours, nous allons voir les politiques de contrôle d'accès DAC, MAC, RBAC et ABAC.

La méthode d'accès DAC (Discretionary Access Control)

La politique de contrôle d'accès discrétionnaire est basée sur l'identité du sujet et les règles d'autorisation qui lui sont prédéfinies, les autorisations d'accès à chaque objet sont manipulées librement par le responsable de l'objet (généralement le propriétaire), les autorisations peuvent être accordées, selon sa volonté, par ce responsable à tout autre sujet. ***Exemples de cas d'utilisations : les SGBD, les OS, les ACLs.***

Avantages

- Facile à manipuler
- Flexible
- Adoptée par la majorité des systèmes commerciaux de nos jours (SGBD, Systèmes d'exploitation, etc.)

Inconvénients

Manque de contrôle de fuite d'informations confidentielles (vulnérables aux attaques par chevaux de Troie et aux utilisateurs malveillants).

La méthode d'accès MAC (Mandatory Access Control)

La politique de contrôle d'accès mandataire est définie par ***MAC = DAC + (Règles (contraintes) obligatoire),*** elle impose des règles d'autorisation incontournables qui

s'ajoutent aux règles discrétionnaires, spécifie l'accès en se basant sur des classifications associées aux sujets et aux objets. On s'y réfère souvent par Sécurité à Multi niveaux (MLS) et est utilisée pour protéger les informations dotées d'une importance élevée (***domaine militaire).***

Exemple : ***Un utilisateur sera autorisé à manipuler une information dans le système s'il possède le droit de lecture sur l'information (contrôle discrétionnaire) et s'il a un niveau de sécurité plus élevé que celui de l'information en question (contrôle obligatoire).***

Avantages

- Adopté dans les domaines militaires
- Sécurité et confidentialité renforcées
- Lutter contre les fuites d'informations

Inconvénients

- Difficile à manipuler
- Couteuse au niveau de l'implémentation

La méthode d'accès RBAC (Role Based Access Control)

Un des problèmes majeurs des politiques discutées précédemment revient à gérer un grand nombre d'objets et de sujets (nombre d'autorisations qui augmente, la manipulation des autorisations devient compliquée) d'où la nécessité d'adopter une politique de contrôle d'accès facile à manipuler mais en même temps flexible et adéquate, en l'occurrence la politique de contrôle d'accès à base de rôles.

Fonctionnement :

- Un rôle représente de façon abstraite une fonction identifiée dans l'organisation (Employé, directeur technique, directeur, etc.)
- L'association des permissions (autorisations) se fait pour chaque rôle et non pour chaque utilisateur
- Chaque utilisateur est associé à un (ou plusieurs) rôle(s) englobant ses fonctions au sein de l'organisation

Avantages

- La manipulation des autorisations est facile
- Le modèle sert à grouper les règles d'autorisation selon les positions (job) dans une organisation

Inconvénient

- Un grand nombre de rôles implique tout de même une complexité de gestion.

La méthode d'accès ABAC (Attribute-Based Access Control)

Politique de contrôle basée sur les attributs des utilisateurs, des ressources et des conditions de l'environnement. Politique d'accès définie par des conditions sur les attributs des sujets ou objets (ressources).

Avantages

- Utilisation des autorisations facile
- Plus sécurisante

Inconvénient

- Difficile à mettre en place

Les listes de contrôle d'accès

Une ACL est une liste de règles permettant de filtrer ou d'autoriser du trafic sur une ressource (une ressource peut être un réseau, un ordinateur, un protocole, un serveur, une donnée ou n'importe quel autre service réseau) en fonction de certains critères (IP source, IP destination, port source, port destination, protocole, …).

Une ACL permet de soit autoriser du trafic (permit) ou de le bloquer (deny). Il est possible d'appliquer au maximum une ACL par interface et par sens (input/output). Une ACL est analysée par l'IOS de manière séquentielle. Dès qu'une règle correspond au trafic, l'action définie est appliquée, le reste de l'ACL n'est pas analysé. Donc tout trafic ne correspondant à aucune règle d'une ACL est rejeté.

On distingue trois types d'ACL : les ACL standards, les ACL étendues et les ACL nommées

Une ACL est dite standard lorsque le filtre se fait uniquement sur l'adresse IP source. Elle est dite étendue lorsqu'en plus de l'adresse IP source, on filtre également l'adresse IP de destination, le protocole utilisé ainsi que les numéros de port des applications qui communiquent en réseau.

On utilise les numéros pour distinguer les ACL dans un routeur. Les numéros allant de **1 à 99** et de **1300** à **1999** sont utilisés pour les ACL standards et ceux allant de **100 à 199 et de 200 à 2699** pour les ACL étendues.

Les ACL nommées

Comme vous le savez, toutes les listes d'accès doivent être identifiées par un nom ou un numéro. Ce type de liste d'accès est plus pratique, car on peut spécifier un nom significatif qui est facile à retenir et associer à une règle. Les ACL nommées peuvent correspondre aux mêmes champs qu'une ACL standard et étendue, cependant, elles présentent trois grandes différences par rapport aux listes de contrôles d'accès numérotées, voyons cela ensemble :

- L'utilisation de noms au lieu de chiffres pour identifier la liste ACL facilite la mémorisation et l'identification de l'ACL.
- Utilisation de sous-commandes ACL, et non de commandes globales, pour définir l'action et les paramètres correspondants.
- Utilisation des fonctionnalités d'édition de l'ACL qui permettent de supprimer des lignes individuelles de l'ACL et d'insérer de nouvelles instructions à une liste d'accès nommée.

Les ACL sont configurées par protocole, par direction, par adresse et par interface. Pour bien configurer une ACL, on doit être capable de répondre aux quatre questions suivantes :

1) De quel type d'ACL s'agit-il ?
2) Dans quel routeur doit-on écrire cette ACL ?
3) Sur quelle interface doit-on appliquer l'ACL ?
4) Quelle est la direction du Traffic

NB1 : on écrit une ACL standard dans le routeur le plus proche de la destination et une ACL étendue dans le routeur le plus proche de la source.

NB2 : un Traffic est dit entrant dans un routeur, lorsque le message qui est transmis part d'un hôte pour le routeur. Il est dit sortant lorsqu'il part du routeur pour l'hôte.

NB3 : la commande « in » est utilisée lorsque le Traffic est entrant et « out » lorsque le traffic est sortant

NB4 : les ACL s'exécutent séquentiellement c'est-à-dire de la première à la dernière instruction. Ainsi, il faut toujours écrire les règles les plus spécifiques avant les règles les plus génériques. À travers la commande « **implicit deny** », les ACL rejettent par défaut tout ce qui n'a pas été autorisé par l'administrateur réseau.