Prosit 03 – Security

Table des matières

1. Mise en contexte

1.1 Contexte

On cherche à sécuriser un réseau informatique.

1.2 Mots-clés

- **DMZ :** En sécurité informatique, une zone démilitarisée (ou DMZ) fait référence à un sous-réseau qui héberge les services exposés et accessibles de l'extérieur d'une entreprise. Elle agit comme une zone tampon avec les réseaux non sécurisés tels qu'Internet.
- **Proxy :** Un serveur proxy joue le rôle de passerelle entre Internet et vous. C'est un serveur intermédiaire qui sépare les utilisateurs, des sites Web sur lesquels ils naviguent. Un proxy établit lui-même la communication avec le site Web.
- **ACL :** Les ACL sont un outil de configuration polyvalent sur votre routeur. En règle générale, les listes de contrôle d'accès sont considérées comme un outil de filtrage, filtrant le trafic entrant ou sortant de votre routeur.
- **Sandbox (bac à sable) :** Une sandbox (bac à sable en français) est un terme de sécurité informatique qui désigne un mécanisme utilisé pour améliorer la sécurité d'un logiciel et de pages web. Pour un système d'exploitation, il diminue les risques lors de l'exécution d'un logiciel. Dans l'univers du Web, ce terme évoque l'environnement qui permet de tester des logiciels ou des sites Web.
- **Vecteur d'attaque :** Un vecteur d'attaque est une voie ou un moyen qui permet à un pirate informatique d'accéder à un ordinateur ou à un serveur pour envoyer une charge utile (payload) ou obtenir un résultat malveillant. Les vecteurs d'attaque permettent aux pirates d'exploiter les failles des systèmes, notamment humaines.

2. Analyse du besoin

2.1 Besoin / Livrable

Réaliser un schéma d'infrastructure et l'infrastructure sécurisée.

2.2 Contraintes

- Prendre en compte le schéma donné dans le prosit
- Prendre en compte les aspects fonctionnels et budgétaires.

2.3 Pistes de solutions

- Bloquer les ports.
- Mettre en place une zone démilitarisée (entre le routeur et le réseau).
- Mettre en place un proxy et un pfsense.

2.4 Généralisation

Sécuriser une infrastructure réseau.

2.5 Problématique

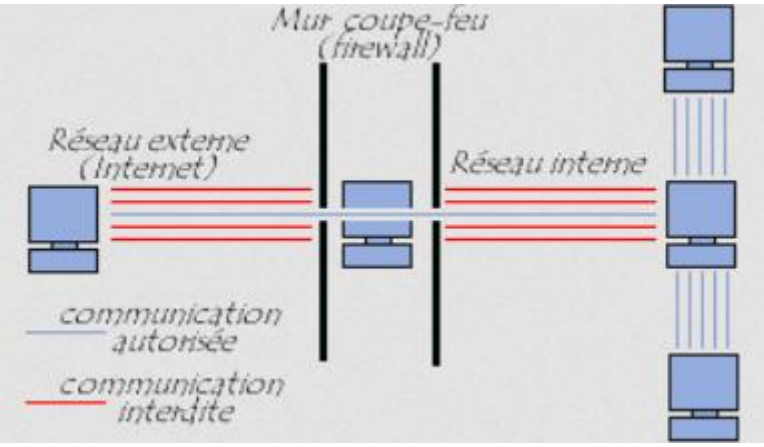
Comment sécuriser une infrastructure en réseau local connectée à internet en prenant en compte des aspects de management et de budget ?

3. Plan d'actions

3.1 Firewall

Un pare-feu, est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- Une interface pour le réseau à protéger (réseau interne).
- Une interface pour le réseau externe.



3.1.1 Fonctionnement d'un pare-feu

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (allow).
- De bloquer la connexion (deny).
- De rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité.

Filtrage simple de paquets :

Un système pare-feu fonctionne sur le principe du filtrage simple de paquets (en anglais « stateless packet filtering »). Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine extérieure.

Ainsi, les paquets de données échangée entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

- Adresse IP de la machine émettrice.
- Adresse IP de la machine réceptrice.
- Type de paquet (TCP, UDP, etc.).
- Numéro de port (rappel : un port est un numéro associé à un service ou une application réseau).

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

Filtrage dynamique :

Les applications utilisent des ports sources dont on ne peut connaître à l'avance la valeur (le port source est choisi aléatoirement entre 1024 et 65535 dans le cas d'un flux TCP, par exemple). Le filtrage dynamique de paquets, ou stateful, permet de suivre l'état des sessions et d'adapter de manière dynamique les règles du pare-feu.

L'amélioration par rapport au filtrage simple réside dans la conservation de la trace des sessions et des connexions dans des tables d'états internes au firewall. Le firewall prend alors ses décisions en fonction des états de connexions.

La conservation des données permet au Firewall de vérifier dynamiquement si toutes les réponses reçues correspondent bien à ce qui est attendue dans ce cas la communication peut avoir lieu sinon la communication est coupée.

Ce filtrage permet aussi de se protéger face à certains types d'attaques DoS.

Filtrage applicatif :

Dans le filtrage de niveau applicatif, également appelé proxy, le pare-feu agit comme un filtre au niveau applicatif, c'est-à-dire au niveau 7 du modèle OSI.

Les requêtes sont traitées par des processus dédiés, par exemple une requête de type HTTP sera filtrée par un processus proxy HTTP. Le pare-feu rejettera toutes les requêtes qui ne sont pas conformes aux spécifications du protocole. Cela implique que le pare-feu proxy connaisse toutes les règles protocolaires des protocoles qu'il doit filtrer.

3.2 ACL

L'objectif à atteindre est de disposer d'une fonction de filtrage prenant en compte l'historique des connexions en cours afin de ne pas accepter du trafic qui n'aurait pas été demandé à partir d'une zone précise du réseau.

Les listes de contrôle d'accès (en anglais Access Control List ou ACL) semblent avoir toujours existé sur les routeurs Cisco et rares sont les configurations où elles n'apparaissent pas. Les ACL servent principalement au filtrage des paquets sur les interfaces physiques cependant leur mode de définition est employé pour catégoriser les réseaux en vue, entre autres, de les injecter dans un protocole de routage ou de les soumettre à une règle de qualité de service. Les types d'ACL proposés sont les suivants :

- Les ACL standards qui filtrent sur l'adresse source.
- Les ACL étendues qui filtrent sur l'adresse source, l'adresse destination ainsi que les ports sources et destination.
- Les ACL lock and Key se mettent en place après authentification de l'utilisateur (en telnet).
- Les named ACL sont des ACL étendues qui reçoivent un nom au lieu d'un numéro.

- Les ACL reflexives utilisent les informations de session pour laisser entrer les paquets de retour correspondant aux paquets envoyés.
- Les time-based ACL sont actives sur une plage de temps donnée.
- Les ACL Context-based access control utilisent...

3.2.1 Filtrage

Les listes de contrôle d'accès sont un groupe de commandes qui vous permettent de contrôler le trafic entrant ou sortant d'une interface. Lorsque les listes de contrôle d'accès filtrent le trafic, elles sont généralement appelées filtres. Les décisions que vous pouvez appliquer au trafic incluent l'autorisation ou l'abandon du trafic en fonction des conditions (règles) que vous définissez sur votre routeur. Les conditions peuvent rechercher des correspondances sur le contenu d'un paquet, notamment :

- Adresse source ou destination
- Informations de protocole de couche 2, telles que le type de trame Ethernet
- Protocoles de couche 3, tels que IP, IPX et AppleTalk
- Informations de protocole de couche 3, telles que IP, ICMP, OSPF, TCP, UDP et autres dans la suite de protocoles TCP/IP
- Informations de protocole de couche 4, telles que les numéros de port TCP et UDP

En règle générale, les ACL filtrent les informations des couches 3 et 4, mais comme vous pouvez le voir dans la liste précédente, vous pouvez également les utiliser pour filtrer les informations de la couche 2. Lorsque je discute des listes de contrôle d'accès réflexives au chapitre 8, « Listes d'accès réflexives » et du contrôle d'accès basé sur le contexte (CBAC) au chapitre 9, « Contrôle d'accès basé sur le contexte », vous verrez que les listes de contrôle d'accès peuvent également garder une trace des informations de la couche 5, ou des informations sur la session, et plus.

3.2.2 Type de listes de contrôles d'accès

Les listes de contrôle d'accès peuvent être utilisées dans n'importe quelle situation pour contrôler le trafic entre les appareils, les services, les réseaux ou une combinaison de ceux-ci. Comme le montre la Figure 6-1, vous pouvez utiliser des listes de contrôle d'accès pour implémenter une solution de pare-feu sur un routeur, ou vous pouvez les utiliser pour restreindre l'utilisation interne des ressources, comme un serveur de comptabilité. En fait, il est très courant de voir un routeur de périmètre avec des listes de contrôle d'accès restreignant le type de trafic autorisé sur le réseau. Dans la Figure 6-1, le routeur de périmètre autorise uniquement le trafic Web destiné au serveur Web interne, ainsi que tout trafic de retour initié par les utilisateurs internes.

Vous pouvez utiliser de nombreux types d'ACL pour implémenter des solutions de filtrage. Chacun est destiné à accomplir une fonction spécifique, et chacun a ses

propres avantages et inconvénients. Certains types d'ACL sont destinés aux solutions de pare-feu ; d'autres non. Les types suivants d'ACL IP sont traités dans ce livre :

ACL IP standard ?

Ce type d'ACL ne peut filtrer que les informations de la couche 3. Ces listes de contrôle d'accès sont utilisées pour filtrer les paquets en fonction de l'adresse source dans l'en-tête du paquet. Le chapitre 7, « Listes d'accès de base », couvre les listes de contrôle d'accès IP standard. Les listes de contrôle d'accès standard sont généralement utilisées pour restreindre l'accès VTY à un routeur Cisco.

Listes de contrôle d'accès IP étendues ?

Ce type d'ACL peut filtrer les informations des couches 3 et 4. Ces listes de contrôle d'accès sont utilisées pour filtrer les paquets en fonction de l'adresse IP source et de destination, du protocole IP (tel que ICMP, IP, OSPF, TCP, UDP et autres) et des informations de protocole (telles que les types de message ICMP ou le port TCP ou UDP Nombres). Le chapitre 7 traite des listes de contrôle d'accès IP étendues. Les listes de contrôle d'accès étendues sont généralement utilisées pour filtrer le trafic, en particulier le trafic lorsqu'il entre dans votre réseau.

Turbo ACL ?

Il s'agit d'une fonction ACL qui vous permet de compiler des ACL standard et étendues, ce qui les rend plus efficaces pour le traitement du routeur et accélère les temps de recherche. Le chapitre 7, « Listes d'accès de base », couvre les ACL turbo.

ACL IP chronométrées ?

Il s'agit d'une liste de contrôle d'accès IP étendue qui peut filtrer les informations des couches 3 et 4. Contrairement aux listes de contrôle d'accès IP étendues normales, les listes de contrôle d'accès temporisées peuvent être activées en fonction de l'heure du jour, du jour de la semaine ou du jour du mois. Ils peuvent être configurés pour filtrer sur une période récurrente ou sur une seule période. Le chapitre 7 traite des listes de contrôle d'accès IP temporisées.

ACL IP réflexives ?

Ce type d'ACL peut filtrer les informations des couches 3, 4 et 5. Certaines personnes pensent que les ACL réflexives implémentent une fonction de pare-feu avec état ; ils ne le font pas, comme vous le verrez au chapitre 8, « Listes d'accès réflexives », mais ils s'en rapprochent beaucoup. J'aime les appeler le "pare-feu du pauvre".

ACL de contrôle d'accès basé sur le contexte (CBAC) ?

Ce type d'ACL peut filtrer les informations de la couche 3 à la couche 7. Il s'agit de la fonction de pare-feu dynamique de Cisco dans son Cisco IOS. Le chapitre 9, « Contrôle d'accès basé sur le contexte », couvre les listes de contrôle d'accès CBAC.

ACL verrouillable et clé ?

Ce type d'ACL filtre les informations de la couche 3 et parfois de la couche 4. Ces ACL implémentent une double authentification, dans laquelle, lors de la connexion via PPP, l'utilisateur s'authentifie d'abord via PAP ou CHAP, puis au niveau de la couche application avant que le routeur n'autorise la connexion. Le chapitre 13, « Listes d'accès verrou et clé », traite des listes de contrôle d'accès verrou-et-clé. Comme vous le verrez ici, les listes de contrôle d'accès verrouillables peuvent être utilisées pour restreindre tout type d'accès à votre réseau

3.3 Proxy

Un serveur proxy est une machine qui traduit le trafic entre les réseaux ou les protocoles. Il s'agit d'un **serveur intermédiaire** séparant les clients finaux des destinations qu'ils parcourent. Les serveurs proxy offrent différents niveaux de fonctionnalités, de sécurité et de confidentialité en fonction de votre cas d'utilisation, de vos besoins ou de la politique de l'entreprise.

Si vous utilisez un serveur proxy, le trafic transite par le serveur proxy jusqu'à l'adresse que vous avez demandée. La demande revient ensuite via ce même serveur proxy (il existe des exceptions à cette règle), puis le serveur proxy vous transmet les données reçues du site Web.

3.3.1 Fonctionnement

Un serveur proxy HTTP, est ce que l'on peut appeler un intermédiaire entre votre ordinateur et internet. Ce serveur agit en prenant la demande de l'internaute pour la transférer avec **sa propre adresse IP** vers le site cible de ce dernier. Grâce au serveur proxy, il n'y a donc **aucun contact direct entre l'internaute et son site cible.** C'est donc un mandataire qui protège l'internaute des menaces qui peuvent provenir des sites web qu'il visite. Il existe d'ailleurs deux sortes de serveurs proxy en fonction de son utilisation.

- **Le serveur proxy :** Le serveur proxy, va s'intercaler entre l'ordinateur et internet. Votre navigateur sera configuré de sorte qu'il sache que vous utilisez un proxy et qu'il en connaisse l'adresse.
  A partir de là, votre navigateur enverra vos requêtes au serveur proxy, mais c'est ce proxy qui se rendra sur internet pour chercher ce que vous lui demandez. Quand il aura une réponse, il l'enverra vers votre poste.
- **Le serveur proxy cache** : Un serveur proxy cache c'est un serveur proxy qui va servir de cache. C'est-à-dire que lorsque vous allez chercher à vous rendre sur un site, le proxy va d'abord vérifier que vous ne vous y êtes pas déjà rendu. S'il voit que vous avez déjà consulté ce site, il vous l'envoi directement car il en a conservé une copie.
- **Le serveur proxy inverse :** avec ce type de serveur, ce sont les serveurs qui sont protégés des contenus venant de vous et du réseau public. Avant de pouvoir vous connecter à internet, **le proxy inverse examine que vous ne représentez aucun danger** pour le site que vous voulez visiter avant de vous mettre en contact. Si toutefois un doute subsiste, vos données sont redistribuées vers les serveurs en arrière-plan pour plus de vérification.

Un serveur proxy est donc très utile pour vous connecter à internet en toute sécurité. Toutefois, le proxy marche également dans le sens inverse dans la protection du site que vous voulez visiter contre les attaques qui peuvent émaner de vous ou de votre réseau.

3.3.2 Avantages et Inconvénients

Avantages :

- Anonymat presque total car c'est l'IP du proxy qui est utilisé et non la vôtre.
- Échapper aux géo-restrictions avec un serveur proxy étranger.
- Filtrage des requêtes du réseau, souvent utilisé par les écoles et les entreprises.
- Sécurité, ce n'est pas vous qui êtes en contact direct avec internet, vous êtes donc un peu mieux protégé.
- Système de cache qui vous permet d'afficher les pages déjà consulté plus rapidement.

Principal Inconvénient :

Le proxy présente un inconvénient assez important. En effet, étant votre intermédiaire à internet, toutes ce que vous faites sur internet passe par celui-ci. Le propriétaire du serveur, s'il est mal intentionné, peut donc avoir accès et enregistrer toutes les informations que vous renseignez en l'utilisant.

3.4 NAT/PAT

NAT (Network Address Translation) et PAT (Port Address Translation) sont les protocoles utilisés pour mapper l'adresse privée (locale) non enregistrée d'un réseau interne vers une adresse publique enregistrée d'un réseau externe avant de transférer le paquet. La principale différence entre eux est que NAT est utilisé pour mapper des adresses IP publiques à des adresses IP privées, il peut s'agir d'une relation un-à-un ou plusieurs-à-un. Tandis que, PAT est un type de NAT où les adresses IP privées multiples sont mappées en une seule IP publique (plusieurs-à-un) en utilisant des ports.

Un utilisateur réseau interne ayant une adresse IP privée (non enregistrée) n'a pas pu se connecter à Internet ou au réseau externe car chaque périphérique d'un réseau doit avoir une adresse IP unique. Le NAT fonctionne sur un routeur connectant deux réseaux ensemble, et il traduit l'adresse privée du réseau interne dans l'adresse publique légale.

De plus, il a été conçu pour conserver les adresses IP. Comme les utilisateurs d'Internet étaient confrontés à un problème de rareté d'adresses IP, où le nombre d'utilisateurs a été augmenté plus que la plage limitée d'adresses IP. Pour cette raison les protocoles NAT et PAT sont utilisés.

3.4.1 NAT

Le NAT est la traduction d'adresses réseau qui relie deux réseaux et mappe les adresses privées en adresses publiques. Ici, le terme adresses privées signifie que l'adresse de l'hôte appartient à un réseau local et n'est pas assignée par le fournisseur de services. Et l'adresse publique signifie que l'adresse est une adresse assignée par le fournisseur de service et il représente également une ou plusieurs adresses locales internes au monde extérieur.

3.2 PAT

Le PAT est la traduction d'adresse de port est un type de NAT dynamique grâce auquel la traduction d'adresse peut être configurée au niveau du port, et l'utilisation de l'adresse IP est optimisée. PAT met en correspondance plusieurs adresses locales et ports sources avec une adresse IP publique et un port à partir d'une liste d'adresses IP routables sur le réseau de destination. Ici, l'adresse IP de l'interface est utilisée en combinaison avec le numéro de port et plusieurs hôtes peuvent avoir la même adresse IP avec un numéro de port unique.

3.5 SIEM

Le SIEM (Security Information and Event Management) est une approche du management de la sécurité. Il combine les fonctions du SIM (Security Information Management) et le SEM (Security Event Management) en un seul système de management de sécurité. Et l'acronyme SIEM se prononce « sim » avec un e silencieux.

3.5.1 Fonctionnement

Les principes sous-jacents de chaque système SIEM est d'agréger des data pertinentes, de plusieurs sources différentes. Et d'identifier les écarts possibles par rapport à la moyenne / norme, afin de prendre les actions appropriées. Par exemple, lorsqu'un problème potentiel est détecté, le SIEM peut enregistrer des informations supplémentaires. Puis générer une alerte, et ordonner à d'autres contrôles de sécurité d'arrêter la progression de leur activité.

À son niveau le plus basique, un système SIEM peut être basé sur des règles. Ou utiliser un moteur de corrélation statistique pour établir des relations entre les entrées du journal de log. De plus, les SIEMs avancés ont évolué pour inclure l'analyse du comportement de l'utilisateur et des entités (UEBA). Ainsi que l'orchestration de la sécurité et la réponse automatisée (SOAR).

La compliance aux standards de sécurité des données de l'industrie des cartes de paiement (PCI DSS) a conduit à l'adoption du SIEM dans les grandes entreprises. Néanmoins, les inquiétudes concernant les menaces persistantes ont conduit de plus petites entreprises à privilégier les avantages d'un SIEM géré par un fournisseur de services de sécurité (MSSP). En effet, cela permet de visualiser toutes les data en lien avec la sécurité d'un seul point de vue. Donc, pour toute entreprise, de facilement repérer les modèles qui sortent de l'ordinaire

3.6 IPS / IDS

La principale différence entre les systèmes de détection d'intrusion (IDS) et les systèmes de prévention d'intrusion (IPS) est que les IDS sont des systèmes de surveillance et les IPS sont des systèmes de contrôle. L'IDS ne modifiera pas le trafic réseau tandis que l'IPS empêche la livraison des paquets en fonction du contenu du paquet, de la même manière qu'un pare-feu empêche le trafic par adresse IP.

Les IDS sont utilisés pour surveiller les réseaux et envoyer des alertes lorsqu'une activité suspecte sur un système ou un réseau est détectée tandis qu'un IPS réagit aux cyberattaques en temps réel dans le but de les empêcher d'atteindre les systèmes et réseaux ciblés.

En bref, IDS et IPS ont la capacité de détecter les signatures d'attaque, la principale différence étant leur réponse à l'attaque. Cependant, il est important de noter qu'IDS et IPS peuvent implémenter les mêmes méthodes de surveillance et de détection.

Dans cet article, nous décrivons les caractéristiques d'une intrusion, les différents vecteurs d'attaque que les cybercriminels peuvent utiliser pour compromettre la sécurité du réseau, la définition d'IDS/IPS et comment ils peuvent protéger votre réseau et améliorer la cybersécurité.

3.6.1 Fonctionnement IDS

Il existe trois variantes de détection courantes utilisées par IDS pour surveiller les intrusions :

- Détection basée sur les signatures : détecte les attaques en recherchant des modèles spécifiques, tels que des séquences d'octets dans le trafic réseau ou des signatures d'utilisation (séquences d'instructions malveillantes

connues) utilisées par les logiciels malveillants. Cette terminologie provient d'un logiciel antivirus qui fait référence à ces modèles en tant que signatures. Alors que les IDS basés sur les signatures peuvent facilement détecter les cyberattaques connues, ils ont du mal à détecter les nouvelles attaques lorsqu'aucun modèle n'est disponible.

- Détection basée sur les anomalies : un système de détection d'intrusion pour détecter à la fois les intrusions sur le réseau et l'ordinateur et les abus en surveillant l'activité du système et en la classant comme normale ou anormale. Ce type de système de sécurité a été développé pour détecter les attaques inconnues, en partie en raison du développement rapide des logiciels malveillants. L'approche de base consiste à utiliser l'apprentissage automatique pour créer un modèle d'activité digne de confiance et comparer le nouveau comportement au modèle. Étant donné que ces modèles peuvent être entraînés en fonction de configurations d'application et de matériel spécifiques, ils ont des propriétés mieux généralisées par rapport aux IDS traditionnels basés sur les signatures. Cependant, ils souffrent également de plus de faux positifs.
- Détection basée : Reconnaît les potentielles en cybermenaces sur la réputation fonction des scores de réputation.

3.6.2 IPS

Les systèmes de prévention des intrusions (IPS) fonctionnent en analysant tout le trafic réseau via une ou plusieurs des méthodes de détection suivantes :

Détection basée sur les signatures : l'IPS basé sur les signatures surveille les paquets dans un réseau et les compare aux modèles d'attaque préconfigurés et prédéterminés appelés signatures.

Détection statistique basée sur les anomalies : un IPS basé sur les anomalies surveille le trafic réseau et le compare à une base de référence établie. Cette ligne de base est utilisée pour identifier ce qui est « normal » dans un réseau, par exemple la quantité de bande passante utilisée et les protocoles utilisés. Bien que ce type de détection d'anomalies soit utile pour identifier de nouvelles menaces, il peut également générer des faux positifs lorsque les utilisations légitimes de la bande passante dépassent une ligne de base ou lorsque les lignes de base sont mal configurées.

Détection d'analyse de protocole avec état : cette méthode identifie les écarts dans les états du protocole en comparant les événements observés avec des profils prédéterminés de définitions généralement acceptées d'activité bénigne.

Une fois détecté, un IPS effectue une inspection des paquets en temps réel sur chaque paquet qui circule sur le réseau et s'il est jugé suspect, l'IPS effectuera l'une des actions suivantes :

- Terminer la session TCP qui a été exploitée
- Empêchez l'adresse IP ou le compte utilisateur incriminé d'accéder à toute application, hôte ou ressource réseau
- Reprogrammez ou reconfigurez le pare-feu pour empêcher qu'une attaque similaire ne se produise à une date ultérieure
- Supprimez ou remplacez le contenu malveillant qui reste après une attaque en reconditionnant la charge utile, en supprimant les informations d'en-tête ou en détruisant les fichiers infectés

Lorsqu'il est déployé correctement, cela permet à un IPS d'éviter de graves dommages causés par des paquets malveillants ou indésirables et une gamme d'autres cybermenaces, notamment :

- Déni de service distribué (DDOS)
- Exploits
- Vers informatiques
- Virus
- Attaques par force brute

3.7 UTM

La gestion unifiée des menaces est plus connue sous l'acronyme UTM, signifiant Unified Threat Management. Concrètement, il existe plusieurs solutions UTM permettant aux entreprises (quelle que soit leur envergure) de maîtriser simplement et efficacement les risques informatiques. Cette synchronisation de toutes les politiques de prévention, également utile pour anticiper les coûts, accroît considérablement leur protection.

De plus en plus développés, les programmes UTM réunissent de nombreuses fonctions en une seule et même solution :

- Le logiciel antivirus
- Les programmes anti-espions
- Les filtres contre les spams
- Le pare-feu pour le réseau.

- L'analyse de toutes les requêtes web en temps réel
- La prévention et l'identification des intrusions
- Le filtrage des contenus
- La protection contre les fuites d'informations
- La génération de rapports

Ces appliances UTM, que l'on appelle parfois également pare-feu de nouvelle génération, simplifient considérablement la sécurisation d'un environnement informatique. Le fait de cumuler plusieurs protections permet de faire face aux menaces les plus sophistiquées, sachant que les pirates du web ne cessent de perfectionner leurs méthodes d'action !

3.8 SOC

Un SOC est une installation abritant une unité de sécurité chargée de surveiller et d'analyser en permanence le dispositif de sécurité d'une entreprise. L'objectif du SOC est **de détecter, analyser et intervenir en cas d'incidents lié à la cybersécurité**. Pour cela, il utilise une combinaison de dispositifs technologiques ainsi qu'un ensemble de processus pour détecter et remonter le moindre incident afin que les équipes puissent réagir rapidement. Avec l'augmentation du nombre de cyberattaque, le SOC devient un élément de plus en plus important pour la sécurité de votre entreprise.

3.8.1 Fonctionnement

Plutôt que de se concentrer sur l'élaboration d'une stratégie de prévention, la conception d'une architecture de sécurité ou la mise en œuvre de mesures de protection, l'équipe SOC est responsable de la face opérationnelle et permanente de la sécurité des informations de l'entreprise.

Le personnel du SOC est principalement composé d'analystes qui travaillent de concert pour détecter, analyser, réagir, signaler et prévenir les incidents liés à la cybersécurité. Certains SOC offrent des capacités supplémentaires, avec des analyses avancées, comme avec la cryptanalyse ou du reverse ingeneering des logiciels malveillants afin de détecter les failles dans l'enreprise en essayant de cracker les mots de passe de l'entreprise ou les clés, pour ensuite analyser les incidents.

Lors de la mise en place d'un SOC au sein d'une structure, la première étape consiste à définir clairement une stratégie qui tient compte des objectifs des divers services de l'entreprise ainsi que des observations des dirigeants. La stratégie se base sur les

services les plus sensibles de l'entreprise, les divisions qui ont le plus de donnée même si elles ne sont pas sensibles, les liens entres les différents départements afin de ne pas avoir de canard boiteux qui permettrait l'accès aux autres services de l'entrepris. Une fois la stratégie élaborée, l'infrastructure requise pour la soutenir doit être mise en œuvre

Selon Pierluigi Paganini, l'infrastructure typique d'un SOC comprend des pare-feux, des IPS/IDS, des solutions de détection des brèches, des sondes et un système de gestion des informations et événements de sécurité (SIEM).

La technologie devra être prête à recueillir les données par le biais des flux de données, de la télémétrie, de la saisie de paquets, du syslog et d'autres méthodes afin que leur activité puisse être corrélée et analysée par le personnel de SOC.

Le SOC surveille également les vulnérabilités des réseaux et des terminaisons afin de protéger les données sensibles et de se conformer aux réglementations industrielles ou gouvernementales.

3.8.2 Avantages

Le principal avantage d'avoir un SOC **est l'amélioration de la détection des incidents de sécurité** par la surveillance **et l'analyse continues de l'activité des données**. En analysant les réseaux, les terminaux, les serveurs et les bases de données d'une société 24h/24, l'équipe du SOC assure une détection et une intervention rapides en cas d'incident de sécurité.

La surveillance permanente assurée par un SOC donne aux entreprises l'avantage de pouvoir se défendre contre les incidents et les intrusions, quels que soient leur source, l'heure de la journée ou le type d'attaque.

4. Bibliographie

DMZ :

https://www.techtarget.com/searchsecurity/definition/DMZ

Pare-feu :

https://www.frameip.com/firewall/

UTM :

https://www.ipe.fr/une-solution-de-securite-informatique-complete-quest-ce-que-lutm/

IP/IDS :

https://blog.varonis.fr/ids-et-ips-en-quoi-sont-ils-differents/#:~:text=Comment%20fonctionnent%20les%20syst%C3%A8mes%20de,de%20pr%C3%A9vention%20des%20intrusions%20(IPS)&text=La%20principale%20diff%C3%A9rence%20entre%20les,est%20un%20syst%C3%A8me%20de%20contr%C3%B4le.

ACL :

http://etutorials.org/Networking/Router+firewall+security/Part+III+Nonstateful+Filtering+Technologies/Chapter+6.+Access+List+Introduction/Access+List+Overview/

NAT/PAD :

https://waytolearnx.com/2018/07/difference-entre-nat-et-pat.html#:~:text=NAT%20traduit%20les%20adresses%20locales,%C3%AAtre%20affect%C3%A9s%20avec%20la%20m%C3%AAme

Proxy :

https://www.proxyvpn.fr/qu-est-ce-qu-un-proxy

SIEM :

https://www.expert-com.com/siem-definition/

SOC :

https://actualiteinformatique.fr/cybersecurite/definition-soc-security-operation-center