ESTIAM / PARIS

Rapport de cours Jour 3 suite

Victoria SAUTEREAU

Cybersécurité

ESTIAM

École d'informatique et du numérique

2ème année

2022/2023

Sommaire

Partie 1 Les mesures pour améliorer la disponibilité

. Gestion des actifs

Avant de savoir quels doivent être les paramètres de configuration, une entreprise doit savoir quels sont le matériel et le logiciel présents. La gestion des ressources implique un inventaire complet du matériel et des logiciels.

L'entreprise doit connaître tous les composants qui peuvent courir des risques en matière de sécurité, notamment :

- Chaque système matériel
- Chaque système d'exploitation
- Chaque appareil réseau matériel
- Chaque système d'exploitation des appareils réseau
- Chaque application logicielle
- Tous les micrologiciels
- Tous les environnements d'exécution
- Toutes les bibliothèques individuelles

Une entreprise peut opter pour une solution automatisée pour effectuer le suivi des ressources. Un administrateur doit examiner tout changement de configuration, car cela peut signifier que la configuration n'est pas à jour ou bien que quelqu'un effectue des modifications non autorisées.

La classification des ressources regroupe toutes les ressources d'une entreprise sur la base de caractéristiques communes. Une entreprise doit mettre en place un système de classification des ressources (documents, dossiers de données, fichiers de données et disques). Les informations essentielles doivent se voir attribuer le niveau de protection le plus élevé, voire faire l'objet d'un traitement spécial.

Une entreprise peut adopter un système de marquage en fonction de l'importance, de la confidentialité ou du caractère « critique » des informations. Suivez la procédure ci-dessous pour identifier et classer les ressources d'une entreprise :

1. Déterminez avec précision la catégorie d'identification des ressources.

2. Établissez la traçabilité des ressources en identifiant le propriétaire de toutes les ressources d'informations et de tous les logiciels d'application.

3. Déterminer les critères de classement.

4. Mettez en place un schéma de classification.

La gestion des ressources porte sur le cycle de vie et l'inventaire des ressources technologiques, y compris les appareils et les logiciels. Dans le cadre d'un système de gestion des ressources informatiques, l'entreprise indique les ressources qui répondent à ses objectifs. Cette pratique réduit effectivement le nombre de types de ressources. Ainsi, une entreprise n'installera que les applications qui respectent ses directives. En

éliminant les applications non conformes, les administrateurs contribuent à une réelle amélioration de la sécurité.

Les standards relatifs aux ressources identifient les produits matériels et logiciels spécifiques qu'une entreprise utilise et prend en charge. Lorsqu'une défaillance survient, une action rapide permet de maintenir en conditions opérationnelles l'accès et la sécurité. Si une entreprise ne standardise pas sa procédure de sélection de matériel, il se peut que le personnel éprouve quelques difficultés à trouver un composant de rechange. Outre des coûts de maintenance et d'inventaire plus élevés, la gestion des environnements non standard requiert des compétences plus poussées. Cliquez ici pour savoir comment l'armée a migré vers du matériel standard pour établir ses communications militaires.

La procédure d'identification des menaces commence par la création d'un identifiant CVE pour les vulnérabilités de cybersécurité connues du public. Chaque identifiant CVE comprend les éléments suivants :

- Le numéro d'identifiant CVE
- Une brève description de la vulnérabilité de sécurité
- Toute référence présentant un intérêt

L'analyse des risques est un processus qui consiste à analyser les dangers que représentent les événements d'origine humaine et naturelle pour les ressources d'une entreprise.

Un utilisateur identifie les ressources pour savoir lesquelles protéger. Les objectifs de l'analyse des risques sont au nombre de quatre :

- Identifier les ressources et leur importance
- Identifier les vulnérabilités et les menaces
- Quantifier la probabilité et l'impact des menaces identifiés
- Mettre en balance l'impact de la menace et le coût de mise en œuvre de la contre-mesure

L'atténuation des risques consiste à réduire la gravité de la perte ou la probabilité que cet événement survienne. De nombreux contrôles techniques réduisent les risques, comme les systèmes d'authentification, les autorisations de fichiers et les pare-feu. L'entreprise et les professionnels de la sécurité doivent être conscients que l'atténuation des risques peut avoir des effets positifs et négatifs sur l'entreprise. Une atténuation des risques efficace trouve l'équilibre entre, d'une part, les effets négatifs des contre-mesures et des contrôles et, d'autre part, les bénéfices associés à la réduction des risques. Quatre méthodes sont souvent utilisées pour réduire les risques :

- Accepter les risques et procéder à une réévaluation périodique
- Réduire les risques en mettant en place des contrôles
- Éviter les risques en adoptant une approche totalement différente
- Transférer le risque à un tiers

Une stratégie à court terme consiste à accepter les risques, ce qui nécessite l'élaboration de plans d'urgence. Les utilisateurs et les entreprises doivent accepter les risques au quotidien. Les technologies modernes réduisent les risques en développant des

logiciels de manière incrémentielle, et en fournissant des mises à jour et des correctifs pour remédier aux vulnérabilités et aux erreurs de configurations.

Externaliser des services, souscrire une assurance ou souscrire un contrat de maintenance sont quelques exemples de transfert de risques. Confier l'exécution des tâches essentielles à des spécialistes afin de réduire les risques peut s'avérer judicieux. Cela peut, en outre, donner de meilleurs résultats avec un investissement moindre à long terme. Un plan de réduction des risques efficace peut inclure plusieurs stratégies.

. Défense approfondie

Opter pour une protection avancée ne garantit pas à l'entreprise que son système de défense sera impénétrable. Cependant, cela l'aide à réduire les risques en gardant une longueur d'avance sur les cybercriminels.

Si un seul moyen de défense est mis en place pour protéger les données et les informations, il suffira aux cybercriminels de contourner un seul obstacle. Pour être sûre que les données et informations restent disponibles, l'entreprise doit créer plusieurs couches de protection.

Cette approche est celle qui offre la protection la plus complète. Si les cybercriminels parviennent à pénétrer un niveau, ils doivent encore faire face à plusieurs autres couches, chacune d'elles étant plus complexe que la précédente.

Les diverses couches créent une barrière de protections multiples qui se coordonnent pour éviter les attaques. Une entreprise peut, par exemple, stocker ses documents top secret sur un serveur installé dans un bâtiment entouré d'une barrière électronique.

Limiter l'accès aux données et informations réduit les risques de subir une attaque. Il est conseillé aux entreprises de restreindre l'accès aux utilisateurs et de ne leur permettre que d'accéder aux ressources dont ils ont besoin pour accomplir leur mission. Par exemple, les membres du service marketing n'ont pas besoin d'avoir accès aux documents de paie dans le cadre de leur mission.

L'application de solutions technologiques, telles que l'utilisation d'autorisations de fichiers, est un moyen de limiter l'accès ; une entreprise doit également instaurer des mesures procédurales. Il est nécessaire de mettre en place une procédure pour interdire à un employé de supprimer des documents sensibles sur site.

Si toutes les couches protégées étaient identiques, il serait aisé pour les cybercriminels de mener à bien leur attaque. Par conséquent, elles doivent être différentes. Si les cybercriminels pénètrent une couche, la même technique ne fonctionnera pas pour toutes les autres. Une attaque qui touche une seule couche de sécurité ne compromet pas l'intégralité du système. Une entreprise peut utiliser divers algorithmes de chiffrement ou systèmes d'authentification afin de protéger les données à différents états.

Pour mettre en place une solution diversifiée, les entreprises peuvent utiliser des produits de sécurité conçus par différentes sociétés en vue d'une authentification multifacteur. Par exemple, le serveur contenant les documents top secret se trouve dans une salle fermée, dont l'accès est protégé par un système de carte magnétique et une solution d'authentification biométrique fournis par deux sociétés différentes.

La méthode de dissimulation permet également de protéger les données et les informations. Une entreprise ne doit pas dévoiler d'informations que les cybercriminels peuvent utiliser pour déterminer le système d'exploitation qu'un serveur exécute ou le type d'équipement qu'il utilise. Par exemple, les messages d'erreur ne doivent contenir aucune information que les cybercriminels pourraient utiliser pour déterminer les vulnérabilités existantes. En masquant certains types d'informations, vous compliquez singulièrement la tâche des cybercriminels qui envisagent de pirater un système.

La complexité n'est pas nécessairement un gage de sécurité. Le déploiement de systèmes difficiles à faire fonctionner et à dépanner peut, en réalité, se retourner contre l'entreprise qui les met en place. Si les employés ne savent pas comment configurer correctement des systèmes complexes, compromettre leur sécurité peut être un jeu d'enfant pour les cybercriminels. Pour maintenir la disponibilité des systèmes, une solution de sécurité doit être simple à l'intérieur, mais complexe à l'extérieur.

. Redondance

La redondance N+1 garantit la disponibilité du système en cas de défaillance d'un composant. Les composants (N) doivent comporter au moins un composant de secours (+1). C'est le cas, par exemple, d'une voiture à quatre roues (N) disposant d'une roue de secours dans le coffre en cas de crevaison (+1).

Dans un data center, la redondance N+1 signifie que la conception du système peut résister à la perte d'un composant. Le « N » fait référence aux divers éléments qui composent le data center (serveurs, alimentations, commutateurs, et routeurs). Le « +1 » désigne un composant ou système supplémentaire, prêt à être utilisé en cas de besoin.

La technologie RAID (Redundant Array of Independent Disks) regroupe plusieurs disques durs physiques au sein d'une seule unité logique afin de fournir une redondance de données et d'améliorer les performances. Le système RAID prend les données normalement stockées sur un seul disque et les répartit sur plusieurs disques. Si l'un des disques est défaillant, l'utilisateur peut récupérer les données à partir des autres disques sur lesquels elles résident également.

Le système RAID permet également d'accélérer la récupération des données. L'utilisation de plusieurs lecteurs permet de récupérer les données demandées plus rapidement que si la tâche était effectuée avec un seul disque.

La redondance améliore la disponibilité de l'infrastructure en supprimant le risque de points de défaillance uniques dans un réseau ; par exemple, une panne d'un commutateur ou d'un câble du réseau. L'établissement d'une redondance physique dans un réseau

entraîne l'apparition de boucles et de trames en double. Ceux-ci ont des conséquences désastreuses pour un réseau commuté.

Le protocole STP (Spanning Tree Protocol) permet de résoudre ces problèmes. La fonction de base de STP est d'empêcher les boucles dans un réseau lorsque plusieurs chemins connectent les commutateurs entre eux. STP garantit que les liaisons physiques redondantes sont dépourvues de boucles. Il permet qu'il n'y ait qu'un seul chemin logique entre toutes les destinations du réseau. STP bloque intentionnellement les chemins d'accès redondants susceptibles d'engendrer une boucle.

Le blocage des chemins redondants est essentiel pour empêcher la formation de boucles sur le réseau. Les chemins physiques sont préservés pour assurer la redondance, mais STP les désactive afin d'empêcher la création de boucles. En cas de défaillance d'un commutateur ou d'un câble réseau, le protocole STP recalcule les chemins et débloque les ports nécessaires pour autoriser l'activation du chemin redondant.

La passerelle par défaut est généralement le routeur, qui assure l'accès des appareils au reste du réseau ou à Internet. Si un seul routeur sert de passerelle par défaut, il constitue un point de défaillance unique. L'entreprise peut choisir d'installer un routeur de secours supplémentaire.

La capacité d'un réseau à effectuer une reprise dynamique après la défaillance d'un périphérique jouant le rôle de passerelle par défaut est appelée « redondance au premier saut ».

La liste suivante indique les options disponibles pour la redondance de routeur en fonction du protocole qui définit la communication entre les appareils réseau :

- Protocole HSRP (Hot Standby Router Protocol) : ce protocole garantit la disponibilité du réseau en fournissant une redondance de routage au premier saut. Un groupe de routeurs utilise le protocole HSRP pour sélectionner un appareil actif et un appareil de secours. Dans un groupe d'interfaces d'appareil, l'appareil actif est celui qui achemine les paquets ; l'appareil de secours est celui qui prend le relais en cas de défaillance de l'appareil actif. La fonction du routeur en veille HSRP est de surveiller l'état de fonctionnement du groupe HSRP et de prendre rapidement la responsabilité du réacheminement des paquets lorsque le routeur actif est défaillant.

- Protocole VRRP (Virtual Router Redundancy Protocol) : un routeur VRRP exécute le protocole VRRP avec un ou plusieurs autres routeurs connectés à un réseau local. Dans une configuration VRRP, le routeur choisi est le routeur virtuel principal, les autres routeurs servant de routeurs de secours en cas de défaillance de celui-ci.

- Protocole GLBP (Gateway Load Balancing Protocol) : ce protocole protège le trafic de données en provenance d'un routeur ou d'un circuit défaillant, tel que HSRP et VRRP,

tout en permettant un équilibrage de la charge (également appelé partage de charge) au sein d'un groupe de routeurs redondants.

Une entreprise peut, dans certains cas, envisager la mise en œuvre de la redondance d'emplacements. Vous trouverez, ci-dessous, trois formes de redondance d'emplacements.

Synchrone

- Synchronise les deux emplacements en temps réel.
- Nécessite une bande passante élevée.
- Les emplacements doivent être proches les uns des autres pour réduire la latence.

Réplication asynchrone

- La synchronisation ne s'effectue pas en temps réel, mais presque.
- Nécessite moins de bande passante.
- Les sites peuvent être plus éloignés, car la latence est un facteur moins important.

Réplication ponctuelle

- Met à jour régulièrement l'emplacement des données de sauvegarde.
- Option la moins gourmande en termes de bande passante, car elle ne nécessite pas une connexion permanente.
- L'option la mieux adaptée à l'entreprise dépendra du bon compromis entre coût et disponibilité.

. Résilience du système

LA résilience regroupe les méthodes et configurations utilisées pour rendre un système ou un réseau tolérant aux pannes. Par exemple, un réseau peut disposer de liaisons redondantes entre des commutateurs exécutant le protocole STP. Bien que le protocole STP fournisse un autre chemin sur le réseau en cas de défaillance d'une liaison, il se peut que le basculement ne soit pas immédiat si la configuration n'est pas optimale.

Les protocoles de routage offrent également une résilience, mais un réglage précis peut améliorer le basculement, de telle sorte que cette opération passe inaperçue pour les utilisateurs du réseau. Les administrateurs doivent essayer des configurations personnalisées dans un réseau de test afin de déterminer si elles permettent d'améliorer les délais de rétablissement.

La redondance ne suffit pas pour parvenir à une conception résiliente. Il est essentiel de bien comprendre les besoins de l'entreprise, puis d'intégrer la redondance afin de créer un réseau résilient.

Partie 2 : Haute disponibilité

Les cinq neuf

L'expression cinq neuf signifie que les systèmes et les services sont disponibles 99,999 % du temps. Elle signifie également que les interruptions planifiées et non planifiées représentent moins de 5,26 minutes par an. Le graphique illustré ici permet de comparer les interruptions observées pour divers pourcentages de disponibilité.

La haute disponibilité fait référence à un système ou un composant qui est opérationnel sans interruption sur une période donnée. Pour assurer la haute disponibilité il est important de :

- Supprimer les points de défaillance uniques
- Concevoir un système assurant la fiabilité
- Détecter les défaillances avant qu'elles ne surviennent

Préserver une haute disponibilité conformément au standard des cinq neuf peut s'avérer coûteux et consommer de nombreuses ressources. L'augmentation des coûts est due à l'achat de matériel supplémentaire, tel que des serveurs et des composants. De plus, plus une entreprise ajoute de composants, plus cela augmente la complexité de la configuration et, partant, les facteurs de risque. Plus le nombre de pièces est important, plus la probabilité de panne est grande au niveau des composants.

Même si préserver la haute disponibilité peut être coûteux dans certains secteurs, plusieurs environnements ont besoin d'atteindre ces 99,999 %.

- Au sein du secteur financier, il est essentiel de maintenir une haute disponibilité pour éviter toute interruption des échanges, assurer une conformité continue et conserver la confiance des clients. Cliquez ici pour en savoir plus sur la panne qui a immobilisé la Bourse de New York pendant quatre heures en 2015.

- La haute disponibilité est indispensable dans le secteur de la santé pour soigner les patients 24 h/24. Cliquez ici pour en savoir plus sur les coûts induits par une panne du data center dans le secteur de la santé.

- Le secteur de la sécurité publique compte des agences qui assurent la sécurité d'une ville, d'une région ou d'un pays. Cliquez ici pour en savoir plus sur la panne de réseau dont a été victime le service de police du Pentagone.

- Le secteur du commerce dépend de l'efficacité des chaînes d'approvisionnement et de la livraison de produits aux clients. Toute interruption peut être catastrophique, notamment pendant les périodes de forte affluence, comme les fêtes.

- Le public attend des médias qu'ils le tiennent informé des événements en temps réel. Aujourd'hui, l'actualité est un bien qui se consomme 24 heures sur 24, 7 jours sur 7.

Les menaces suivantes font peser un risque élevé sur la disponibilité des données et des informations :

- Un utilisateur non autorisé réussit à accéder à la base de données principale d'une entreprise et en compromet la sécurité.
- Une attaque DoS a un impact significatif sur les activités d'une entreprise.
- Une entreprise subit une perte importante de données confidentielles.
- Une application critique cesse de fonctionner.
- Une compromission de l'utilisateur racine ou administrateur se produit.
- Détection d'un script intersite (XSS) ou d'un partage de serveur de fichiers illégal.
- Le vandalisme sur le site web d'une entreprise nuit aux relations publiques.
- Événement climatique majeur, tel qu'un ouragan ou une tornade.
- Événement catastrophique, tel qu'une attaque terroriste, un attentat à la bombe dans un bâtiment ou un incendie.
- Panne de longue durée d'un opérateur télécoms ou d'un service public.
- Dégâts des eaux causés par une inondation ou la rupture d'une canalisation.

Catégoriser le niveau d'impact de chaque menace permet à une entreprise d'évaluer son impact financier.

La haute disponibilité intègre trois principes majeurs pour garantir un accès ininterrompu aux données et aux services :

1. L'élimination ou la réduction des points de défaillance uniques
2. La résilience du système
3. La tolérance aux pannes

.

est important de bien comprendre les différentes méthodes de résolution d'un point de défaillance unique. Un point de défaillance unique peut être un commutateur ou un routeur central, un service réseau et même un membre hautement qualifié du personnel informatique. Le fait est qu'un événement affectant le système, le processus ou la personne peut perturber gravement l'ensemble du système. Il est donc essentiel de disposer de processus, de ressources et de composants qui réduisent les points de

défaillance uniques. Pour garantir la redondance, une méthode consiste à utiliser des clusters à haute disponibilité. Ces clusters se composent d'un groupe d'ordinateurs ayant accès au même stockage partagé et présentant des configurations réseau identiques. Tous les serveurs participent simultanément au traitement d'un service. De l'extérieur, le groupe de serveurs apparaît comme un seul appareil. En cas de défaillance d'un serveur du cluster, les autres serveurs continuent de traiter le même service.

La résilience d'un système est sa capacité à maintenir la disponibilité des données et des processus opérationnels malgré une attaque ou un événement perturbateur. En règle générale, cela n'est possible qu'en utilisant des systèmes redondants, tant sur le plan de l'alimentation que du traitement, de sorte que si un système tombe en panne, l'autre puisse prendre le relais sans interruption du service. La résilience d'un système va au-delà du renforcement des appareils. En effet, cela exige que les données et les services restent disponibles alors même que le système subit l'attaque.

La tolérance de panne permet à un système de continuer à fonctionner en cas de défaillance d'un ou plusieurs composants. L'émulation des données est un exemple de tolérance de panne. Si une défaillance se produit, entraînant par là même une perturbation au niveau d'un appareil tel qu'un contrôleur de disque, le système en miroir fournit les données demandées sans que l'utilisateur constate la moindre interruption du service.

Partie 3 : Traitement des incidents

• Phases de gestion des incidents

La gestion des incidents désigne les procédures suivies par une entreprise à la suite d'un événement en dehors de la plage de fonctionnement normale. Une violation de données divulgue des informations dans un environnement non sécurisé. Cela peut se produire à la suite d'un acte accidentel ou intentionnel. Une violation de données se produit lorsqu'une personne non autorisée accède à des informations sensibles, les copie, les transmet, les consulte ou les vole.

Lorsqu'un incident se produit, l'entreprise doit savoir comment y répondre. Une entreprise doit élaborer un plan de gestion des incidents et mettre sur pied une équipe CSIRT (Computer Security Incident Response Team) pour gérer la réponse. Cette équipe effectue les opérations suivantes :

- Gérer le plan de gestion des incidents
- Veiller à ce que ses membres connaissent bien le plan
- Tester le plan
- Faire approuver le plan par la direction

La détection commence lorsque quelqu'un découvre l'incident. Les entreprises peuvent s'équiper des systèmes de détection les plus sophistiqués, mais si les administrateurs ne consultent pas les journaux et ne surveillent pas les alertes, ces systèmes ne servent à rien. Une détection appropriée doit indiquer non seulement la manière dont l'incident s'est produit, mais aussi les données et les systèmes concernés. La violation est transmise aux

cadres supérieurs et aux responsables des données et systèmes afin de les impliquer dans le processus de correction et de réparation. La détection et l'analyse comprennent les étapes suivantes :

- Alertes et notifications
- Surveillance et suivi

L'analyse des incidents permet d'identifier la source, l'étendue, les conséquences et les détails de la violation des données. Le cas échéant, l'entreprise peut décider de faire appel à une équipe d'experts pour mener l'enquête.

Les opérations de confinement comprennent les actions effectuées immédiatement, comme déconnecter un système du réseau afin de stopper la fuite d'informations.

Après avoir identifié la faille, l'entreprise doit la contenir et l'éliminer. Cela peut se traduire par une interruption supplémentaire pour les systèmes. La phase de reprise comprend les mesures que l'entreprise doit prendre pour remédier à la violation et rétablir le fonctionnement des systèmes concernés. Une fois la correction appliquée, l'entreprise doit rétablir tous les systèmes dans l'état dans lequel ils se trouvaient avant la faille.

Une fois le fonctionnement normal rétabli, l'entreprise doit examiner la cause de l'incident et se poser les questions suivantes :

- Quelles mesures prendre pour éviter que l'incident se reproduise ?
- Quelles mesures préventives doivent être renforcées ?
- Comment améliorer la surveillance du système ?
- Comment minimiser les interruptions pendant les phases de confinement, d'élimination et de reprise ?
- Comment la gestion peut-elle atténuer les effets sur l'entreprise ?

Une analyse des enseignements tirés de cet événement peut aider l'entreprise à mieux se préparer en améliorant son plan de gestion des incidents.

Technologies de gestion des incidents

L'objectif du contrôle de l'accès au réseau (NAC) est de permettre aux utilisateurs autorisés disposant de systèmes conformes d'accéder au réseau. Un système conforme satisfait à toutes les exigences de la politique de l'entreprise.

Un cadre NAC peut utiliser l'infrastructure de réseau et les logiciels tiers existants pour appliquer la conformité avec la politique de sécurité à l'ensemble des terminaux. Une appliance NAC peut, tour à tour, contrôler l'accès réseau, évaluer la conformité et appliquer la politique de sécurité. Les vérifications courantes des systèmes NAC sont les suivantes :

1. Détection des virus mise à jour

2. Mises à jour et correctifs des systèmes d'exploitation

3. Application de mots de passe complexes

Les systèmes de détection d'intrusion (IDS) surveillent passivement le trafic sur un réseau. En cas de fonctionnement avec une copie du trafic, le système IDS n'a pas d'incidence négative sur le flux de paquets du trafic transféré. Il s'agit là du principal avantage de cette méthode. En revanche, il est impossible pour le système IDS de bloquer les attaques à un seul paquet avant qu'elles atteignent leur cible. Pour répondre à une attaque, le système IDS a généralement besoin de l'aide d'autres appareils réseau, tels que des routeurs et des pare-feu.

Une meilleure solution consiste à utiliser un appareil capable de détecter et de bloquer immédiatement une attaque. C'est précisément ce que fait un système de prévention des intrusions (IPS).

L'IPS repose sur la technologie IDS. Toutefois, un appareil IPS fonctionne en mode inline. Cela signifie que tout le trafic entrant et sortant doit transiter par celui-ci. Un système de protection contre les intrusions surveille le trafic réseau. Il analyse le contenu et la charge utile des paquets à la recherche d'attaques intégrées plus sophistiquées susceptibles de contenir des données malveillantes. Certains systèmes utilisent une combinaison de technologies de détection d'intrusions ; détection basée sur l'analyse des protocoles, sur les profils ou encore sur les signatures. Cette analyse plus approfondie leur permet d'identifier, d'arrêter et de bloquer les attaques qui franchiraient les limites d'un pare-feu classique. Lorsqu'un paquet entre par une interface sur un système de protection contre les intrusions, l'interface de sortie ou approuvée ne le reçoit pas tant qu'il n'a pas été analysé.

L'avantage du mode inline est que le système IPS peut empêcher les attaques à un seul paquet d'atteindre le système cible. En revanche, si le système IPS est mal configuré, cela peut avoir une incidence négative sur le flux de paquets du trafic transféré.

La principale différence entre les systèmes IDS et IPS est la suivante : alors que le système IPS agit immédiatement et bloque le trafic malveillant, le système IDS le laisse passer avant de résoudre le problème.

NetFlow est une technologie Cisco IOS qui fournit des statistiques sur les paquets traversant un routeur ou un commutateur multicouche Cisco. NetFlow est la norme pour la collecte de données opérationnelles à partir de réseaux L'IETF (Internet Engineering Task Force) s'est appuyé sur NetFlow Version 9 de Cisco pour l'exportation des informations du flux IP (IP Flow Information Export - IPFIX).

IPFIX est un format standard conçu pour exporter, vers des appareils de collecte de données, des informations basées sur le routeur concernant les flux de trafic réseau. IPFIX fonctionne sur les routeurs et applications de gestion qui prennent en charge le protocole. Les gestionnaires réseau peuvent exporter les informations relatives au trafic réseau à partir d'un routeur et les utiliser dans le but d'optimiser les performances du réseau.

Les applications prenant en charge IPFIX peuvent afficher des statistiques de n'importe quel routeur compatible avec ce standard. La collecte, le stockage et l'analyse des données agrégées fournies par les appareils compatibles IPFIX offrent les bénéfices suivants :

- Protection du réseau contre les menaces internes et externes
- Résolution rapide et précise des pannes affectant le réseau
- Analyse des flux réseau en vue de la planification de la capacité

Les threat intelligence avancées peuvent aider les entreprises à détecter une cyberattaque pendant l'une des phases de l'attaque et parfois même avant qu'elle ne survienne.

Les entreprises peuvent repérer les alertes de sécurité suivantes dans les journaux et rapports système afin de détecter les indicateurs d'attaque :

- Blocages de compte
- Tous les événements de base de données
- Création et suppression de ressources
- Modification de la configuration des systèmes

Partie 4 : Reprise après sinistre

Plan de reprise après sinistre

L'entreprise met en action son plan de reprise après sinistre (DRP) alors que la catastrophe est en cours et que les employés s'efforcent de maintenir les systèmes critiques en activité. Ce plan comprend les mesures prises par l'entreprise pour évaluer, récupérer, réparer et restaurer les installations ou les biens endommagés.

Pour créer le plan de reprise après sinistre, vous devez répondre aux questions suivantes :

- Qui est responsable de ce processus ?
- Quels sont les éléments nécessaires pour effectuer ce processus ?
- Où la personne responsable exécute-t-elle ce processus ?
- Quel est le processus ?
- En quoi ce processus est-il considéré comme critique ?

Un plan de reprise après sinistre doit identifier les processus les plus critiques au sein de l'entreprise. Lors du processus de récupération, l'entreprise rétablit d'abord ses systèmes essentiels.

Dans le domaine informatique, il existe trois types de contrôles de reprise après sinistre :

- Mesures préventives : il s'agit des contrôles qui empêchent un sinistre de se produire. Ces mesures cherchent à identifier les risques.
- Mesures de détection : ces contrôles détectent les événements indésirables. Ces mesures permettent de découvrir de nouvelles menaces potentielles.
- Mesures correctives : il s'agit de contrôles qui rétablissent le fonctionnement du système à la suite d'un sinistre ou d'un événement.

- ## Planification de la continuité d'activité

  Les contrôles de continuité de l'activité ne se limitent pas à la sauvegarde de données et à la mise à disposition de matériel redondant. Les entreprises ont besoin que les employés configurent et utilisent correctement les systèmes. Les données peuvent être inutiles jusqu'à ce qu'elles fournissent des informations. L'entreprise doit prêter une attention particulière aux points suivants :

  - Mettre les bonnes personnes aux bons endroits
  - Documentation des configurations
  - Établir d'autres canaux de communication pour la voix et les données
  - Garantir l'approvisionnement en électricité
  - Identifier toutes les dépendances pour les applications et les processus de manière à garantir une bonne comprehension
  - Comprendre comment mener à bien manuellement des tâches automatisées