ROYAUME DU MAROC

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail

POLITQUE DE SECURITE
www.ofppt.info

OFPPT

DIRECTION **R**ECHERCHE ET **I**NGENIERIE DE **F**ORMATION

SECTEUR NTIC

Sommaire

1.Introduction

Le terme « système informatique » désigne ici tout système dont le fonctionnement fait appel, d'une façon ou d'une autre, à l'électricité et destiné à élaborer, traiter, stocker, acheminer ou présenter de l'information. Les systèmes d'information s'appuient en règle général sur des systèmes informatiques pour leur mise en oeuvre.

De tels systèmes se prêtent à des menaces de types diverses, susceptibles d'altérer ou de détruire l'information (on parle d'« intégrité de l'information »), ou de la révéler à des tiers qui ne doivent pas en avoir connaissance (on parle de « confidentialité de l'information »), ou bien par exemple de porter atteinte à sa disponibilité (on parle alors de « disponibilité du système »).

Certaines de ces menaces peuvent aussi, indirectement, causer d'importants dommages financiers. Par exemple, bien qu'il soit relativement difficile de les estimer, des sommes de l'ordre de plusieurs milliards de dollars US ont été avancées suite à des dommages causés par des programmes malveillants comme le ver Code Red. D'autres dommages substantiels, comme ceux reliés au vol de numéros de cartes de crédit, ont été déterminés plus précisément.

Outre les aspects financiers, des bris de sécurité informatique peuvent causer du tort à la vie privée d'une personne en diffusant des informations confidentielles sur elle (entre autres ses coordonnées postales ou bancaires), et peuvent pour cette raison être sanctionnés lorsqu'une négligence de l'hébergeur est établie : si, par exemple, celui-ci n'a pas appliqué un correctif dans des délais raisonnables.

Indirectement aussi, certaines menaces peuvent nuire à l'image même du propriétaire du système d'information. Des techniques répandues de « defacing » (une refonte d'un site web) permettent à une personne mal intentionnée de mettre en évidence des failles de sécurité sur un serveur web. Ces personnes peuvent aussi profiter de ces vulnérabilités pour diffuser de fausses d'informations sur son propriétaire (on parle alors de désinformation).

2. Politique de sécurité

2.1. Définition

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.

2.2. Définition selon RFC 2196

« Une politique de sécurité est une déclaration formelle des règles auxquelles doivent se conformer les personnes recevant un droit d'accès au capital technologique et informatif d'une entreprise «

2.3. Politique de sécurité d'entreprise

Une politique de sécurité doit être mise en œuvre avec la participation du personnel clé de l'entreprise concerné, à savoir :

- Les membres de la direction générale
- Le personnel technique
- Le personnel juridique, éventuellement

Une politique de sécurité d'entreprise apporte les avantages suivants:

- Un cadre fonctionnel (« un cadre fonctionnel (« le voir comme un CPS ou ou un Texte de Loi») permettant d'implémenter des Procédures de sécurité dans l'infrastructure de réseau
- Un processus permettant l'audit de la sécurité un processus permettant l'audit de la sécurité actuelle du réseau

- une sécurité globale

- Une base pour toute action juridique éventuelle

Enfin, Pour réussire à la mettre en œuvre , il faut :

- Elle doit pouvoir être implémentée. sur le. sur le plan technique
- Elle doit pouvoir être implémentée sur le plan organisationnel.
- Elle doit pouvoir être imposée soit techniquement ou sinon par des sanctions administratives
- Elle doit être souple et et adaptable aux changements et évolutions au sein de l'entreprise

Et, C'est la nature des activités qui doit dicter la politique de sécurité à suivre. Et non pas l'inverseDéfinir une politique peut sembler difficile, mais la penser avant de choisir l es méthodes de sécurité peut éviter à une entreprise de devoir revoir ces dernières une fois qu'elles sont déjà en place.

2.4. 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.
Les mécanismes de sécurité mis en place peuvent néanmoins provoquer une gêne au niveau des utilisateurs et les consignes et règles deviennent de plus en plus compliquées au fur et à mesure que le réseau s'étend. 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 oeuvre se fait selon les quatre étapes suivantes :

- Identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;
- Elaborer des règles et des procédures à mettre en oeuvre 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 terme 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 terme 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

3. Gestion de risques :

La gestion des risques permet de répondre à 3 questions essentielles à la mise en place d'une **Politique de sécurité :**

- Comment résoudre les problèmes de sécurité
- A quel endroit les résoudre
- Quels types et niveaux de contrôles de sécurité appliquer

3.1. Comparaison des approches de la gestion des risques

La plupart des entreprises se penchent sur la gestion des risques de sécurité lorsqu'elles doivent faire face à un incident de sécurité relativement bénin. Cette situation se présente par exemple lorsque l'ordinateur d'un employé est infecté par un virus et qu'un responsable de l'entreprise s'improvise expert informaticien et cherche à éliminer le virus sans endommager l'ordinateur ou les données qu'il contient. Quel que soit l'incident initial, lorsque les problèmes de sécurité se multiplient au point d'affecter les performances commerciales, la plupart des entreprises se lassent d'avoir à faire face à de telles successions de crises. Elles recherchent alors une approche alternative à cette démarche réactive, afin de réduire la probabilité d'occurrence des incidents de sécurité. Les entreprises qui appliquent la gestion des risques s'orientent vers une approche proactive.

3.1.1. Approche réactive

Lorsqu'un problème de sécurité survient, la plupart des professionnels de l'informatique ne trouvent que le temps de contenir le problème, analyser l'événement et intervenir le plus rapidement possible sur les systèmes affectés. Certains essaient parfois d'identifier la cause du problème, mais pour ceux qui sont soumis à de fortes contraintes, cette démarche est purement accessoire. Bien que l'approche réactive puisse s'avérer efficace pour résoudre des incidents de sécurité liés à l'exploitation de risques de sécurité, il est possible de l'améliorer en lui imposant une certaine rigueur afin d'aider les entreprises à optimiser l'utilisation de leurs ressources.
En s'appuyant sur des incidents de sécurité récents, une entreprise peut prévoir et anticiper les problèmes potentiels. Ainsi, si une entreprise prend le temps de traiter les incidents de sécurité de manière pondérée et rationnelle et d'en déterminer les raisons sous-jacentes, il lui sera plus facile de se protéger d'incidents similaires à l'avenir et elle pourra traiter ces problèmes plus rapidement.

3.1.2. Approche proactive

Plutôt que d'attendre que les problèmes se présentent avant d'y répondre, le principe de cette approche est de minimiser la possibilité qu'ils se produisent dès le départ. Pour protéger les ressources importantes de votre entreprise, vous devez mettre en place des contrôles visant à réduire les risques d'exploitation des vulnérabilités par des programmes ou des personnes malveillants ou par un usage accidentel. L'analogie suivante

illustre bien ce concept. La grippe est une maladie respiratoire mortelle qui affecte des millions de personnes chaque année. Une première approche pour lutter contre cette maladie consiste à ne rien faire tant que vous n'êtes pas affecté et à vous soigner si vous tombez malade. La seconde approche consiste à vous faire vacciner avant que la saison de la grippe ne commence.
Bien entendu, les entreprises ne doivent pas complètement renoncer à l'approche réactive. En effet, bien qu'une approche proactive efficace permette de diminuer considérablement les risques d'incidents de sécurité, il est peu probable que ces derniers disparaissent complètement

3.2. Approches du classement des risques

Il existe de nombreuses méthodologies de classement et d'évaluation des risques. Cependant, la plupart d'entre elles s'appuient sur une gestion **quantitative** ou **qualitative** des risques ou sur une combinaison de ces approches.

3.2.1. Évaluation quantitative des risques

L'objectif de cette approche est de calculer des valeurs numériques objectives pour tous les composants collectés lors de l'évaluation des risques et de l'analyse coût/bénéfices. Par exemple, cela consiste à évaluer la valeur réelle des ressources de l'entreprise en fonction du coût de leur remplacement, du coût occasionné par la perte de productivité, du coût en matière de réputation et diverses autres valeurs directes et indirectes.

3.2.2. Valorisation des ressources

L'estimation de la valeur monétaire d'une ressource joue un rôle important dans la gestion des risques. Les directeurs d'entreprise se basent souvent sur la valeur d'une ressource pour déterminer le temps et l'argent qu'ils peuvent consacrer à sa protection. La liste des **VR** (valeurs des ressources) figure dans les plans de continuité des opérations de la plupart des entreprises. Vous pourrez cependant remarquer que les chiffres donnés sont des estimations subjectives : il n'existe pas de méthode ni d'outil objectif pour déterminer la valeur d'une ressource. Pour déterminer la valeur d'une ressource, calculez les trois facteurs suivants :

- **Valeur globale de la ressource pour l'entreprise**. Calculez ou estimez la valeur financière directe de la ressource. Calculez par exemple l'impact d'une perturbation temporaire de l'activité d'un site Web de commerce électronique accessible 7 jours sur 7 et 24 heures sur 24, dont les commandes client génèrent des recettes moyennes de 2 000 euros par heure. Vous pouvez affirmer avec certitude que la valeur annuelle du site Web en termes de recettes équivaut à 17 520 000 euros.

- **Impact financier immédiat de la perte de la ressource**. Simplifiez l'exemple ci-dessus et considérez que le site Web génère un revenu horaire constant. Si ce même site Web est inaccessible pendant 6 heures, l'exposition calculée correspond à 0,000685 % par an. En multipliant ce pourcentage par la valeur annuelle de la ressource, vous pouvez prédire que les pertes directement imputables à l'indisponibilité du site s'élèveront à 12 000 euros.

- **Impact commercial indirect lié à la perte de la ressource**. Gardons le même exemple : la société estime devoir dépenser 10 000 euros à l'occasion d'une campagne de marketing visant à revaloriser une image de marque ternie par l'indisponibilité du site. Par ailleurs, elle s'attend également à une perte de 0,01 (1 %) des ventes annuelles, soit 17 520 euros. En additionnant les dépenses publicitaires supplémentaires et la perte de recettes, elle prévoit dans ce cas précis une perte indirecte totale de 27 520 euros.

Détermination de la PEU (Perte estimée annuelle)

Il s'agit du montant total de recettes perdues à la suite d'une occurrence unique du risque. La **PEU** est le montant monétaire attribué à un événement unique représentant le montant des pertes potentielles qu'essuierait la société si une menace spécifique se concrétisait. Le résultat obtenu correspond à l'impact d'une analyse qualitative du risque. Pour calculer la PEU, multipliez la valeur de la ressource par le **FE** (Facteur d'exposition). Ce dernier représente le pourcentage de perte qu'une menace concrétisée peut avoir sur une ressource donnée. Si une batterie de serveurs Web a une valeur de 150 000 euros et qu'un incendie provoque des dommages estimés à 25 % de sa valeur, alors la PEU s'élève à 37 500 euros. Notez cependant que cet exemple est simplifié à l'extrême. Il est en effet probable que d'autres dépenses doivent également être prises en compte.

Détermination du TAO (Taux annuel d'occurrences)

Ce taux correspond au nombre de fois qu'un risque peut raisonnablement se réaliser au cours d'une année.

Calcul de la PEA (Perte estimée annuelle).

Il s'agit de la somme totale que l'entreprise perdra en un an si rien n'est fait pour atténuer le risque. Calculez cette valeur en multipliant la valeur de la PEU par le TAO. La perte estimée annuelle correspond au classement relatif obtenu par une analyse qualitative du risque.
Par exemple, si un incendie ravage la batterie de serveurs Web de l'entreprise évoquée ci-dessus, provoquant des dommages estimés à 37 500 euros et que la probabilité (ou taux annuel d'occurrence) d'un incendie est de 0,1 % (une fois en 10 ans), alors la valeur de la PEA est de 3 750 euros (37 500 euros × 0,1 = 3 750 euros).

RIPS (Retour sur investissement pour la sécurité)

Estimez le coût des contrôles à l'aide de l'équation suivante :

(PEA avant le contrôle) – (PEA après le contrôle) – (coût annuel du contrôle) = RIPS

Par exemple, la PEA d'une menace d'attaque visant à paralyser un serveur Web s'élève à 12 000 euros et elle est ramenée à 3 000 euros après l'implémentation de la mesure de protection suggérée. Le coût annuel de maintenance et de fonctionnement de cette mesure de protection est de 650 euros. Le RIPS s'élève donc à 8 350 euros par an, selon l'équation suivante : 12 000 euros - 3 000 euros - 650 euros = 8 350 euros.

Résultats de l'analyse quantitative des risques
Les informations issues des analyses quantitatives du risque fournissent des résultats et des objectifs clairement définis. Les éléments suivants sont généralement obtenus d'après les résultats des étapes précédentes :

- Valeurs monétaires attribuées aux ressources
- Liste complète des menaces significatives
- Probabilité de voir chaque menace se réaliser
- Potentiel de perte pour la société, pour chaque menace et pour une période de 12 mois
- Mesures de protection, contrôles et actions recommandés

3.2.3. Évaluation qualitative des risques

Ce qui différencie l'évaluation qualitative des risques de l'évaluation quantitative des risques, c'est que dans le cas de la première, il n'est pas nécessaire d'affecter des valeurs financières concrètes aux ressources, aux pertes estimées ou au coût des contrôles. Il s'agit plutôt de calculer des valeurs relatives. L'analyse des risques est généralement menée à l'aide d'une combinaison de questionnaires et d'ateliers de collaboration impliquant des personnes appartenant à plusieurs services au sein de l'entreprise, comme des experts en sécurité informatique, des responsables et employés du service informatique, les propriétaires et les utilisateurs des ressources de l'entreprise ainsi que des hauts responsables. Le cas échéant, les questionnaires sont généralement distribués quelques jours ou quelques semaines avant le premier atelier. Ils sont conçus pour déterminer les ressources et les contrôles déjà déployés. Les informations ainsi collectées peuvent se révéler très utiles lors des ateliers suivants. Lors des ateliers, les participants identifient les ressources et estiment leurs valeurs relatives. Ensuite, ils essaient de déterminer les menaces pouvant affecter chaque ressource, avant d'essayer d'imaginer quels types de vulnérabilités ces mêmes menaces pourraient exploiter à l'avenir. Habituellement, les experts du groupe de sécurité informatique et les administrateurs système développent des contrôles visant à minimiser les risques, les soumettent au groupe et estiment le coût de chaque contrôle. Enfin, les résultats sont soumis à la direction durant une analyse coût/bénéfices.

4. Évaluation des risques

La classification des données selon des niveaux variés d'importance peut être une étape préliminaire dans la procédure de valorisation. Un simple système d'évaluation avec les mentions ***élevé. Moyen*** **ou** ***faible*** peut déjà représenter un point de départ pour évaluer les risques. Les données peuvent appartenir à diverses catégories

Données administratives. La correspondance ou autres informations relatives aux biens de l'entreprise ainsi que les renseignements de personnel qui sont généralement consultables.

Données financières. Les informations sur les budgets et les dépenses relatives aux opérationsde l' entreprise**.**

Données de clientèle. Les informations de nature personnelle relatives aux clients ou des renseignements issus de tests. d'observations ou de missions de conseil**.**

Données propriétaires/recherches..
Les informations qui ne peuvent pas être divulguées au public sans la permission du propriétaire

Exemple : Valorisation des Exemple :Valorisation des ressources non tangibles ressources non tangibles

Type de données	*Classification*	*Gravité d'une perte*
Résultats de tests	Recherche	Elevée
Tendances de marché	Recherche	faible
Brevets en cours	Propriétaire	Elevee
Mémos d'entreprise	Administration	Faible
Fichier d'employés	Administration,	Faible'
		Moyenne
Nouvelles fonctionnalités de produits	Propriétaire	Elevée
Sècrets commerciaux	Propriétaire	
Données d' acquisition	Finances	Elevée
	Finances	Moyenne

4.1. Evaluation des Menaces et vulnérabilités

Une menace peut être une personne, un objet ou un événement pouvant potentiellement provoquer des dommages au réseau ou à ses équipements.

Les menaces peuvent être intentionnelles, comme la modification malveillante d'informations sensibles, ou accidentelles, suite à une erreur de calcul ou la suppression fortuite d'un fichier.

Une vulnérabilité est une faiblesse sur un réseau qui peut être exploitée par une menace (ex password)
Par exemple. un accès, non autorisé (la menace) au réseau peut être commis par un attaquant qui devine un mot de passe trop évident.
La vulnérabilité exploitée ici est un choix médiocre de mot de passe de la part d'un utilisateur.
La réduction ou l'élimination des points faibles du réseau peut réduire ou éliminer le risque de voir les menaces se concrétiser.

Par exemple, un outil qui peut aider des utilisateurs à choisir des mots de passe plus robustes

Les menaces sont généralement classées de la façon suivante:

- écoute clandestine ou vol d'informations:
- blocage de l'accès aux ressources du réseau (DoS)
- Accès non autorisé

4.2. Les Conséquences des Menaces

Les conséquences de ce type de menaces peuvent être déclinés en 3 grands domaines :

1-Compromission de la sécurité des données

- Vol d'information parun accès non autorisé à un système ou par écoute passive des échanges (sniffer)

2-Perte d'intégrité des données

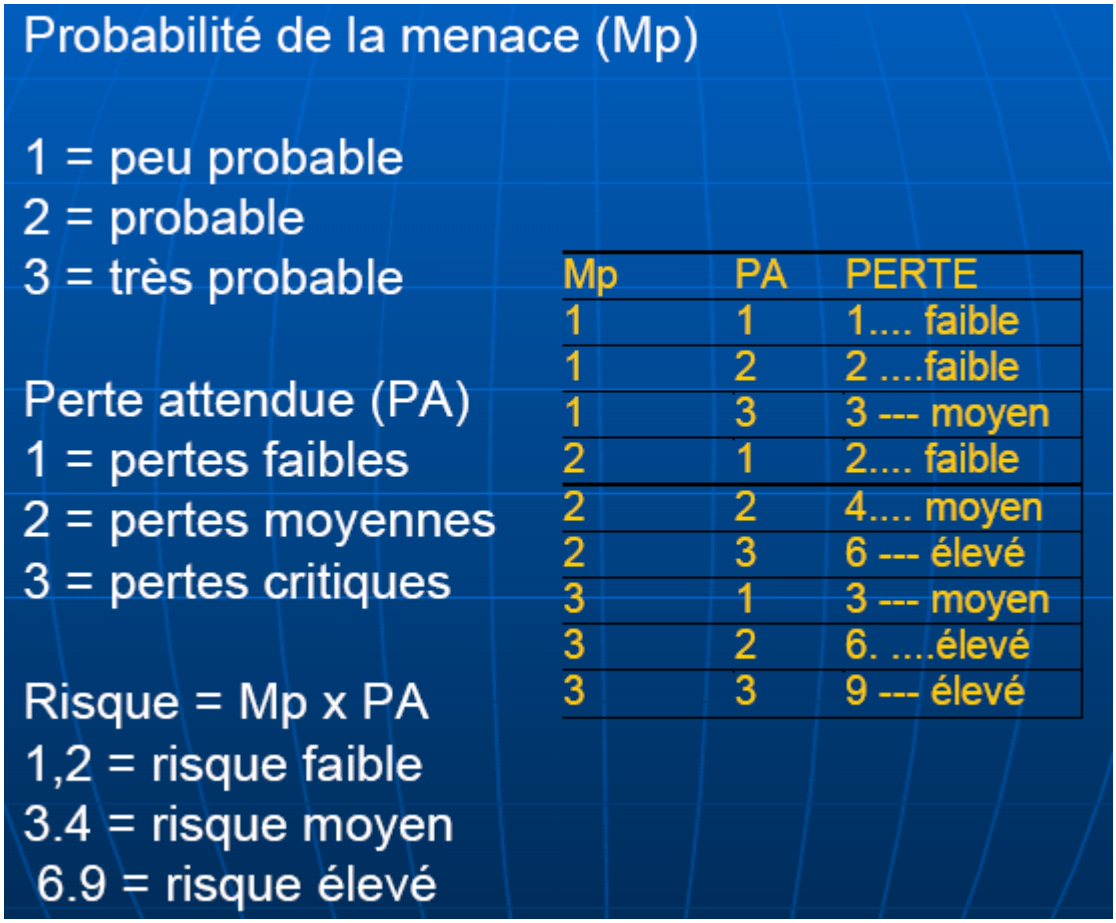
- Les données ne sont plus fiables ou bien ne peuvent plus être restaurés les données actives sont-elles physiquement sécurisées et sauvegardées (Où , quand et comment)?
- Qui dispose d'un accès physique au média contenant vos données?

3-Indisponibilité des ressources

- Dans les environnements actuels où les entreprises s'appuient de plus en plus sur des transactions réalisées en réseau, l'inaccessibilité à des systèmes vitaux peut se traduire rapidement par des pertes importantes en temps et en argent (manque à gagner)
- Ce domaine de problèmes est étroitement lié à celui de la fiabilité et de la redondance d'un système, raison pour laquelle une politique de sécurité doit etre définie pendant la conception du réseau.

Comment évaluer le Risque de sécurité informatique ?

En voici un Exemple de Calcul simple de risques.



4.3. Réduction des risques et du coût de la sécurité

Lorsque tous les risques ont été évalués, l'entreprise doit déterminer le niveau de risque qu'elle peut accepter et le niveau de protection à accorder à ses ressources. Donc, **La *réduction des risques*** est le processus de sélection des contrôles appropriés pour ramener les risques à un niveau acceptable. Ce niveau est déterminé en comparant le risque d'exposition de la brèche de sécurité au coût de l'implémentation et de l'application de la politique de sécurité.

Pour développer une politique de sécurité APPLICABLE, il faut considérer le niveau des coûts et des performances acceptables

Exemple : Les procédures de chiffrement et de déchiffrement consomment du temps et de la puissance de traitement. Une décision spontanée de chiffrer tout le trafic peut résulter en une dégradation des performances

En effet, Il faut comprendre que les mesures de sécurité ne rendent impossibles ni un accès frauduleux aux informations ni l'exécution de tâches non autorisées sur un système du réseau. Donc, Les mesures de sécurité ne peuvent qu'augmenter les difficultés pour y parvenir. Même si l'entreprise n'implémente que des filtres ACL pour accepter le trafic extérieur provenant de certains réseaux Cela peut être suffisamment dissuasif pour certains intrus pas vraiment déterminés, cherchant simplement à occuper leur temps libre.. .

Item a
Item b

Mettre l’accent sur un point particulier

Note d’attention particulière.

Pour approfondir le sujet….

Proposition de références utiles permettant d'approfondir le thème abordé

Sources de référence

Citer les auteurs et les sources de référence utilisées pour l'élaboration du support