Introduction

Parce que les risques en matière de sécurité n'ont cessé d'augmenter ces dernières années, il est important pour les entreprises de mettre en place une stratégie qui leur permette d'être préparé en cas d'incident et de réduire l'occurrence de ces éventuels incidents. Les enjeux de la mise en place d'une politique de sécurité informatique Du bon fonctionnement du système d'information de l'entreprise dépend la disponibilité des informations et des systèmes informatiques mais aussi la confidentialité des informations, avec le risque de voir le capital informationnel de l'entreprise compromis ou perdu. On sait désormais que le principal facteur de risque en matière de sécurité informatique c'est le facteur humain. Comment faire pour travailler sur cet aspect de la sécurité informatique ? Différentes stratégies sont possibles. Dans cet article nous allons aborder l'élaboration d'une politique de sécurité informatique au sein de l'entreprise, avec des conseils et des bonnes pratiques.

Définition

Qu'est-ce qu'une politique de sécurité informatique ?

Une politique de sécurité informatique est une stratégie visant à maximiser la sécurité informatique d'une entreprise. Elle est matérialisée dans un document qui reprend l'ensemble des enjeux, objectifs, analyses, actions et procédures faisant parti de cette stratégie.

I- Les bonnes pratiques d'une mise en place d'une sécurité informatique.

La mise en place d'une politique de sécurité informatique n'est que l'une des nombreuses mesures possibles pour assurer la sécurité du système d'information de l'entreprise. Elle représente l'ensemble des orientations suivies par une organisation en termes de sécurité. Elle est élaborée au niveau de système de pilotage (Direction), car elle concerne tous les utilisateurs du système. Ainsi, 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 aussi aller au-delà de cela tout en couvrant les champs ci-après :

- Mise en place des correctifs ;
- Définition de la police de sécurité ;
- Objectifs, Portée, Responsables ;
- Une stratégie de sauvegarde correctement planifiée ;
- Description de la sécurité (de l'infrastructure physique, des données informatiques, des applications, du réseau) ;
- Plan en cas de sinistre (Un plan de reprise après incident) ;
- Sensibilisation du personnel aux nouvelles procédures ;
- Sanctions en cas de manquements.

I-1 Les parties d'une mise en place d'une politique de sécurité

L'usage de la mise en place d'une politique de sécurité en entreprise repose généralement sur des incidents commune et récurrente qui sont généralement visible en entreprise et peut être découpée en plusieurs parties entre autre :

- **Défaillance matérielle :** Tout équipement physique est sujet à défaillance (usure, vieillissement, défaut…) ; L'achat d'équipements de qualité et standard accompagnés d'une bonne garantie avec support technique est essentiel pour minimiser les délais de remise en fonction. Seule une forme de sauvegarde peut cependant protéger les données.

- **Défaillance logicielle :** Tout programme informatique contient des bugs. La seule façon de se protéger efficacement contre ceux-ci est de faire des copies de l'information à risque. Une mise à jour régulière des logiciels et la visite des sites consacrés à ce type de problèmes peuvent contribuer à en diminuer la fréquence.

- **Accidents** (pannes, incendies, inondations…) : Une sauvegarde est indispensable pour protéger efficacement les données contre ces problèmes. Cette procédure de sauvegarde peut combiner plusieurs moyens fonctionnant à des échelles de temps différentes : Disques RAID pour maintenir la disponibilité des serveurs ; Copie de sécurité via le réseau (quotidienne) ; Copie de sécurité dans un autre bâtiment (hebdomadaire).

- **Erreur humaine :** Outre les copies de sécurité, seule une formation adéquate du personnel peut limiter ce problème.

- **Vol via des dispositifs physique (disques et bandes) :** Contrôler l'accès à ces équipements : ne mettre des unités de disquette, bandes… que sur les ordinateurs où c'est essentiel. Mettre en place des dispositifs de surveillances.

- **Virus provenant de disquettes :** Ce risque peut être réduit en limitant le nombre de lecteur de disquettes en service. L'installation de programmes antivirus peut s'avérer une protection efficace mais elle est coûteuse, diminue la productivité, et nécessite de fréquentes mises à jour.

- **Piratage et virus réseau** : Cette problématique est plus complexe et l'omniprésence des réseaux, notamment l'Internet, lui confère une importance particulière. Les problèmes de sécurité de cette catégorie sont particulièrement dommageables et font l'objet de l'étude qui suit.

MISE EN PLACE D'UNE SECURITE INFORMATIQUE

I-1-1Exemple de Quelques bonnes pratiques dans la Mise en place d'une politique de sécurité informatique :

La mise place d'une politique de sécurité informatique n'est pas universelle et respecte généralement les objectifs et la vision de la politique de l'entreprise qui souhaite la mettre en œuvre. Nous avons récolté ci-dessous quelques-unes des meilleures pratiques à observer lors de l'élaboration d'une politique de sécurité informatique :

- Désignation d'un responsable :
Designer responsable informatique est la première chose à prendre en compte dans l'élaboration de politique de sécurité car c'est lui qui sera en charge de toute l'infrastructure et qui supervisera celui en vue d'un bon fonctionnement.

- **Définir le périmètre et les objectifs**

La définition du champs d'action de la politique de sécurité informatique dans une entreprise à des fins d'efficience permet de ressortir les besoins nécessaires et les mesures adéquates en vue de bon résultats.

- **Effectuer un Audit**

L'analyse de l'existant matériel, logiciel, et humain est nécessaire ainsi que la mise à jour d'un registre de l'ensemble des éléments qui composent le système d'information. Ce registre est important lors des modifications des composants de la configuration informatique. En cas d'incident, il peut permettre aux équipes IT de trouver l'origine du problème.

- **Effectuer une analyse des risques**

Effectuez une analyse des risques informatiques, au regard du préjudice possible et de la probabilité d'occurrence de l'incident. Déterminer les moyens nécessaires pour la réduction des risques et la prise en charge des incidents, qu'il s'agisse de moyens matériels ou humains

- **Définir les procédures adaptées, notamment en matière de gestion des incidents, ou de gestion de la continuité d'activité**

- **Rédiger une charte informatique,**

La charte informatique, est un document de recommandations concernant la bonne utilisation des technologies informatiques, et qui est destiné aux employés de l'entreprise. Ce document est unique et personnalisé, car il est établi en tenant compte du fonctionnement, de l'environnement, de la composition du système d'information de l'entreprise et des enjeux et des risques informatiques qui lui sont propres à l'attention des collaborateurs.

- **Communiquer sur la politique de sécurité informatique auprès de l'ensemble de l'entreprise**

Une sensibilisation auprès des employés sur les bonnes pratiques et les mesures de sécurité est important.

Suite à cet exemple nous comprenons ainsi que mettre en place une politique de sécurité informatique n'est pas une mince affaire, car cela implique de nombreuses tâches et de nombreux acteurs. Cela demande également une analyse fine du système d'information de l'entreprise, et des compétences à la fois techniques, en gestion de projet, en documentation et en communication.

La politique de sécurité informatique de l'entreprise peut donc être réalisée en interne par des techniciens ou par le responsable informatique. Elle peut également être réalisée à la demande par une entreprise externe, qui sera en charge de la conduite du projet, de la réalisation des différents audits, de la mise en place des procédures et de la rédaction de la documentation associée.

II- Architecture sécurisée

La mise en place d'une politique de sécurité informatique nécessite de respecter un canevas bien précis ou une architecture sécurisée afin de réduire des éventuelles menaces.

Définition

L'architecture de sécurité de l'information a été décrite comme une architecture de sécurité permettant de contrôler le réseau supportant les communications locales, étendues et distantes, d'en comprendre le fonctionnement, et d'en assurer la surveillance.

L'architecture est la façon dont les composants d'une chose s'organisent. S'agissant d'un système d'information en réseau, l'objectif est d'organiser et d'exploiter ce système de manière à pouvoir contrôler le système et à détecter des activités inattendues, indésirables et malveillantes.

Dans la construction d'une architecture sécurisée en vue de la mise en place d'une sécurité informatique robuste, les éléments à prendre en compte sont :

Passerelle sécurisée

Si le trafic qui s'écoule dans, hors et au travers d'un réseau ne peut pas être vu, il ne peut pas être surveillé. Pour éviter cela, le trafic doit traverser un environnement de passerelle maîtrisé. Les grandes entreprises peuvent ne pas avoir une bonne gestion du nombre de points d'accès à Internet utilisés. Ce qui représente une vulnérabilité majeure pour le l'administration américaine. La situation idéale est d'avoir une seule passerelle pour concentrer et surveiller le trafic.

La passerelle Internet sécurisée devrait fournir les services suivants :

Pare-feu pour fournir inspection des paquets et contrôle d'accès ;

Du point de vue de l'architecture de la sécurité de l'information, un pare-feu peut être considéré comme un périphérique qui assure l'implémentation de la politique de sécurité, et en particulier la politique d'accès. La présupposition est qu'une politique de contrôle d'accès périmétrique

- si c'est là qu'est placé le pare-feu

- a été définie et documentée.

Sans une politique de contrôle d'accès définie qui sert de guide pour la configuration du pare-feu, l'implémentation du pare-feu risque de ne pas fournir le niveau de service de sécurité requis par l'organisation.

- **Système de détection/prévention d'intrusion (IDS/IPS) ;**

Disposer d'un IDS ou d'un IPS est essentiel dans une architecture de passerelle sécurisée. Généralement, l'IDS/IPS s'appuie sur une base de données de signatures pour détecter les intrusions potentielles ou les violations de la politique de sécurité, comme l'utilisation de protocoles non autorisés. La base de données de signatures dans un IDS est comparable à celle utilisée dans un système de détection de virus, notamment en cela qu'il ne produira aucune alerte pour une signature d'intrusion absente de sa base de données. Celle-ci doit donc être mise à jour régulièrement, tout comme avec un système de détection de logiciels malveillants.

- **Service proxy applicatif pour les protocoles http/https, smtp, ftp, etc. ;**

A chaque service, son proxy tous les protocoles applicatifs qui traversent la passerelle doivent passer par un service de proxy bidirectionnel complet afin d'être surveillés efficacement. Cela commence par le courrier électronique (smtp, imap, pop) et les protocoles Web (http, https). La majorité du trafic réseau devrait être couverte. Une analyse de bande passante permettra d'identifier d'autres protocoles applicatifs utilisés dans l'organisation, tels que ftp et ssh. Faire transiter ces protocoles via un service proxy bidirectionnel complet fournira une visibilité supplémentaire et la possibilité de surveiller les informations et les fichiers entrant et sortant du réseau. Ces services proxy incluent :

- Proxy de messagerie

Les proxys de messagerie peuvent filtrer le spam, effectuer des recherches de virus et contrôler les pièces jointes et les liens HTML. Le contenu actif et le code mobile peuvent également être filtrés par un service proxy. Le courrier électronique peut également être analysé dans une perspective de prévention des fuites de données.

- Proxy Web

Un service de proxy Web devrait fournir un filtrage bidirectionnel pour les protocoles http et https en fonction de l'adresse IP et/ou de l'URL, y compris le filtrage des liens et du code actif intégrés dans les pages Web. Le filtrage de contenu et de mots clés devrait également être utilisé dans le cadre d'un service proxy Web. L'accès à un courrier électronique externe via une interface Web - une option de choix pour l'exfiltration de données - peut être surveillé ou bloqué.

- **Antivirus, antimalware et blocage de spam**

Si elle n'est pas fournie ailleurs, dans le cadre d'un serveur proxy par exemple, la détection des virus et des logiciels malveillants, et le blocage des courriers indésirables, doivent être fournis dans la passerelle sécurisée. Bien qu'il soit possible d'effectuer une analyse antivirus et un blocage des courriers indésirables sur les postes de travail, identifier ces menaces aussi tôt que possible avant leur entrée dans l'environnement de confiance est préférable.

- **Analyse du trafic réseau**

L'analyse du trafic du réseau informatique repose sur la collecte et l'analyse des flux IP. Cette analyse est extrêmement utile pour comprendre le comportement du réseau : l'adresse source permet de comprendre qui produit le trafic ; l'adresse de destination indique qui reçoit le trafic ; les ports donnent des indications sur l'application liée au trafic ; la classe de service examine la priorité du trafic, etc.

À l'aide de ces informations, il est possible de déterminer des profils comportementaux qu'il sera possible de considérer comme normaux, pour ensuite identifier les comportements inattendus ou indésirables, y compris les comportements malveillants. Par exemple, si un utilisateur commence à transférer de grandes quantités de données par courrier électronique vers l'extérieur l'entreprise, il serait possible de détecter ce comportement avec l'analyse du trafic réseau.

- **L'usage des protocoles et des méthodes d'accès**

Dans une architecture sécurisée les protocoles et les méthodes d'accès sont aussi à prendre en compte a l'instar du protocole AAA (Authentification, Autorisation et Audit) qui permet de régulariser les accès entre un utilisateur et un système.

III- Principe de défense et de détection (segmentation, filtrage, relayage, imitation et contrôle d'accès)

La mise en place d'une politique de sécurité informatique dans une entreprise requière souvent de prendre en compte un certain nombre de principe de défense contre les éventuelles attaques informatiques et de prendre en compte différentes méthodes de détections de ces attaques.

III-1 Principe de détection

Un système de détection d'intrusion (ou IDS : Intrusion detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

Il existe deux grandes catégories d'IDS, les plus connues sont les détections par signatures (reconnaissance de programme malveillant) et les détections par anomalies (détecter les écarts par rapport à un modèle représentant les bons comportements, cela est souvent associé a de l'apprentissage automatique).

- **Systèmes de détection d'intrusion par signatures**

Les systèmes de détection d'intrusion par signature (ou SIDS : Signature-based Intrusion Detection System), reposent sur des bibliothèques de description des attaques (appelées signatures).

Au cours de l'analyse du flux réseau, le système de détection d'intrusion analysera chaque événement et une alerte sera émise dès lors qu'une signature sera détectée. Cette signature peut référencer un seul paquet, … ou un ensemble (dans le cas d'une attaque par déni de service par exemple). Cette méthodologie de détection se révèle être efficace uniquement si la base de signatures est maintenue à jour de manière régulière.

Dans ce cas, la détection par signatures produit peu de faux-positifs. Cependant, une bonne connaissance des différentes attaques est nécessaire pour les décrire dans la base de signature. Dans le cas d'attaques inconnues de la base, ce modèle de détection s'avérera inefficace et ne générera donc pas

d'alertes. La base de signature est donc très dépendante de l'environnement (système d'exploitation, version, applications déployées, …).

- **Systèmes de détection d'intrusion par anomalies**

Contrairement aux SIDS, les systèmes de détection d'intrusion par anomalies (ou AIDS : Anomaly-based Intrusion Detection System) ne se reposent pas sur des bibliothèques de description des attaques. Ils vont se charger de détecter des comportements anormaux lors de l'analyse du flux réseau. Pour cela, le système va reposer sur deux phases:

- Une phase d'apprentissage, au cours de laquelle ce dernier va étudier des comportements normaux de flux réseau. …
- Une phase de détection, le système analyse le trafic et va chercher à identifier les événements anormaux en se basant sur ses connaissances. Cette méthode de détection repose sur de nombreuses techniques d'apprentissage supervisé, telles que : Les réseaux de neurones artificiels, Le modèle de Markov caché, Les machines à vecteurs de support.

- **Hybride**

Cette méthodologie de détection consiste à reposer à la fois sur un système de détection par signatures et sur un système de détection par anomalies. Pour cela, les deux modules de détection, en plus de déclencher des alertes si une intrusion est détectée, peuvent communiquer leurs résultats d'analyse à un système de décision qui pourra lui-même déclencher des alertes … grâce à la corrélation des résultats remontés par les deux modules. L'avantage de cette méthodologie de détection est la combinaison du faible taux de faux-positifs générés par les systèmes de détection d'intrusion par signature, tout en possédant la capacité de détecter des attaques inconnues dans la base de signature grâce à la détection par anomalie

III-2 le principe de defenses

Dans tout système informatiques une politique de défense est toujours à prendre en compte pour protéger une entreprise contre des attaques. Parmi les principes de défense nous pouvons citer :

Système de détection d'intrusion (IDS)

– Un **système de détection d'intrusion** améliore la cyber sécurité en repérant un pirate informatique ou un logiciel malveillant sur un réseau afin que vous puissiez le supprimer rapidement pour éviter toute violation ou tout autre problème, et utiliser les données consignées à propos de l'événement pour mieux vous protéger contre des incidents d'intrusion similaires. A l'avenir. Investir dans un système IDS permettant de réagir rapidement aux attaques peut coûter beaucoup moins cher que de réparer les dommages causés par une attaque et de régler les problèmes juridiques ultérieurs.

- **Système de prévention des intrusions (IPS)**

  – Un **système de** protection **contre les intrusions** est une solution de sécurité réseau qui peut non seulement détecter les intrus, mais aussi les empêcher de lancer avec succès toute attaque connue. Les systèmes de prévention des intrusions combinent les capacités des pare-feu et des systèmes de détection des intrusions. Toutefois, la mise en œuvre d'un système IPS à une échelle efficace peut être coûteuse. Les entreprises doivent donc évaluer soigneusement leurs risques informatiques avant d'investir. En outre, certains systèmes de prévention des intrusions ne sont pas aussi rapides et robustes que certains pare-feu et systèmes de détection des intrusions. Par conséquent, cette solution peut ne pas être appropriée lorsque la vitesse est une exigence absolue.

- **Le contrôle d'accès réseau (NAC)** implique la limitation de la disponibilité des ressources réseau aux périphériques d'extrémité conformes à votre stratégie de sécurité. Certaines solutions NAC peuvent corriger automatiquement les nœuds non conformes pour garantir leur sécurité avant que l'accès ne soit autorisé. NAC est particulièrement utile lorsque l'environnement utilisateur est relativement statique et peut être contrôlé de manière rigide, comme dans les entreprises et les agences gouvernementales. Cela peut être moins pratique dans des environnements avec un ensemble varié d'utilisateurs et d'appareils qui changent fréquemment et sont courants dans les secteurs de l'éducation et de la santé.
- **Les filtres Web** sont des solutions qui empêchent les navigateurs des utilisateurs de charger certaines pages de sites Web particuliers. Il existe différents filtres Web conçus pour une utilisation individuelle, familiale, institutionnelle et professionnelle.
- **Les serveurs proxy** agissent en tant que négociateurs pour les demandes émanant du logiciel client recherchant des ressources auprès d'autres serveurs. Un client se connecte au serveur proxy pour demander un service (par exemple, un site Web); le serveur proxy évalue la demande puis l'autorise ou le refuse. Dans les organisations, les serveurs proxy sont généralement utilisés pour le filtrage du trafic et l'amélioration des performances.
- **Les** dispositifs **anti-DDoS** détectent les attaques par déni de service (DDoS) à leurs débuts, absorbent le volume de trafic et identifient la source de l'attaque.
- **Les équilibreurs de charge** sont des unités physiques qui dirigent des ordinateurs vers des serveurs individuels d'un réseau en fonction de facteurs tels que l'utilisation du processeur de serveur, le nombre de connexions à un serveur ou les performances globales du serveur. Les organisations utilisent des équilibreurs de charge pour minimiser les risques de saturation d'un

serveur en particulier et pour optimiser la bande passante disponible de chaque ordinateur du réseau.

- **Les filtres anti-spam** détectent les courriers indésirables et les empêchent d'accéder à la boîte aux lettres d'un utilisateur. Les filtres anti-spam jugent les e-mails en fonction de règles ou de modèles conçus par une organisation ou un fournisseur. Les filtres plus sophistiqués utilisent une approche heuristique qui tente d'identifier le spam par le biais de modèles de mots suspects ou de la fréquence de mots.
- **La segmentation** du réseau implique la séparation du réseau en unités logiques ou fonctionnelles appelées zones. Par exemple, vous pouvez avoir une zone pour les ventes, une zone pour le support technique et une autre zone pour la recherche, chacune ayant des besoins techniques différents. Vous pouvez les séparer à l'aide de routeurs ou de commutateurs ou à l'aide de réseaux locaux virtuels (VLAN), que vous créez en configurant un ensemble de ports sur un commutateur afin qu'il se comporte comme un réseau séparé. La segmentation limite les dommages potentiels d'un compromis à ce qui se trouve dans cette zone. Essentiellement, il divise une cible en plusieurs, laissant deux options aux attaquants : Traiter chaque segment comme un réseau séparé ou en compromettre un et tenter de franchir la division. Ni le choix est attrayant. Traiter chaque segment comme un réseau distinct représente une lourde charge de travail supplémentaire, car l'attaquant doit compromettre chaque segment individuellement. Cette approche augmente également de manière spectaculaire l'exposition de l'attaquant à la découverte.

CONCLUSION

Rendu au terme de notre exposé dont le thème parlait de la mise en place d'une sécurité informatique, nous pouvons dire que la mise en place d'une politique de sécurité informatique ne dois pas se prendre à la légère et que toute décision sur la mise en place de ce dernier nécessite la prise en compte d'un bon nombre de principes et de règles qui doivent être respecté afin d'assurer une sécurité optimale du système en mettre en place.

BIBLIOGRAPHIE

- Support de cours

SUPPORT DE COURS DE SÉCURITÉ DES SYSTEMES D'INFORMATIONS SEMINAIRE 1. Dr. KAMDEM Alain Bertrand, Ph.D.

- Reference web

www.soltic.com

www.Ivision.com

www.fr.wikipedia.com

Table des matières