Stratégie de sécurité de réseau : Livre blanc sur les pratiques recommandées

Contenu

Introduction

Sans politique de sécurité, la disponibilité de votre réseau peut être compromise. La politique commence par une évaluation des risques liés au réseau et la mise en place d'une équipe d'intervention. Le maintien de la politique requiert la mise en place d'une pratique de gestion des modifications relatives à la sécurité et le contrôle du réseau à la recherche de violations de sécurité. Pour finir, le processus de révision modifie la politique existante et s'adapte à l'expérience acquise.

Ce document est divisé en trois parties : préparation, prévention et réponse. Regardons en détail chacune de ces étapes.

Préparation

Avant de mettre en place une politique de sécurité, vous devez faire ce qui suit :

- Créer des instructions de politique d'utilisation.
- Réaliser une évaluation des risques.
- Établir une structure pour l'équipe chargée de la sécurité.

Créer des instructions de politique d'utilisation

Nous vous recommandons de créer des instructions de stratégie d'utilisation qui soulignent les

rôles et responsabilités des utilisateurs en ce qui concerne la sécurité. Vous pouvez commencer par un politique générale qui couvre tous les systèmes et données réseau au sein de votre société. Ce document doit fournir à la communauté d'utilisateurs en général une compréhension de la politique de sécurité, sa portée, des directives pour améliorer leurs pratiques de sécurité et des définitions de leurs responsabilités en matière de sécurité. Si votre société a identifié des actions spécifiques qui pourraient entraîner des mesures punitives ou disciplinaires à l'encontre d'un employé, ces actions et la façon de les éviter doivent être clairement articulées dans ce document.

L'étape suivante est de créer des instructions d'utilisation acceptable à fournir aux partenaires avec une entente quant aux informations qui sont à leur disposition, la façon dont ces informations doivent être utilisées, ainsi que le comportement des employés de votre société. Vous devez clairement expliquer tous les actes spécifiques qui ont été identifiés comme des attaques de sécurité et les mesures punitives qui seront prises si une attaque de sécurité est détectée.

Pour finir, créez des instructions d'utilisation d'administrateur acceptables pour expliquer les procédures pour la gestion de compte utilisateur, la mise en application de la politique et le contrôle des privilèges. Si votre société a des politiques spécifiques au sujet des mots de passe utilisateur ou de la gestion des données subséquentes, présentez également clairement ces politiques. Comparez la politique avec les instructions d'utilisation acceptable du partenaire et les instructions de politique d'utilisation acceptable d'utilisateur pour assurer l'uniformité. Assurez-vous que les exigences relatives à l'administrateur répertoriées dans la politique d'utilisation acceptable sont reflétées dans des plans de formation et des évaluations des performances.

Réaliser une évaluation des risques

Une évaluation des risques doit identifier les risques liés à votre réseau, aux ressources et aux données du réseau. Ceci ne signifie pas que vous devez identifier chaque point d'entrée possible au réseau, ni tous les moyens d'attaque possibles. L'évaluation des risques a pour but d'identifier des parties de votre réseau, d'évaluer les risques de menace pour chaque partie et d'appliquer un niveau de sécurité approprié. Ceci aide à maintenir un équilibre réalisable entre la sécurité et l'accès au réseau requis.

Attribuez à chaque ressource réseau l'un des trois niveaux de risque suivants :

- **Risque peu élevé** Systèmes ou données dont la compromission (données consultées par le personnel non autorisé, données corrompues ou données perdues) ne perturberait pas l'entreprise ou n'aurait pas de conséquences légales ou financières. Le système ou les données ciblés peuvent être facilement restaurés et ne permettent pas d'accéder à d'autres systèmes.
- **Risque moyen** Systèmes ou données dont la compromission (données consultées par le personnel non autorisé, données corrompues ou données perdues) perturberait peu l'entreprise, aurait des conséquences légales ou financières mineures, ou permet d'accéder à d'autres systèmes. Le système ou les données ciblés demandent un effort modéré de restauration ou le processus de restauration perturbe le système.
- **Risque élevé** Systèmes ou données dont la compromission (données consultées par le personnel non autorisé, données corrompues ou données perdues) perturberait beaucoup l'entreprise, aurait des conséquences légales ou financières importantes, ou menace la santé et la sécurité d'une personne. Le système ou les données ciblés demandent un effort de restauration important ou le processus de restauration perturbe l'entreprise ou d'autres systèmes.

Attribuez un niveau de risque à chacun des éléments suivants : périphériques réseau de base, périphériques réseau de distribution, périphériques réseau d'accès, périphériques de surveillance de réseau (moniteurs SNMP et agents RMON), périphériques de sécurité réseau (RADIUS et TACACS), systèmes de messagerie, serveurs de fichiers réseau, serveurs d'impression réseau, serveurs d'application réseau (DNS et DHCP), serveurs d'application de données (Oracle ou d'autres applications autonomes), ordinateurs de bureau et d'autres périphériques (serveurs d'impression et fax de réseau autonomes).

Les équipements réseau tels que des commutateurs, des routeurs, des serveurs DNS et des serveurs DHCP peuvent permettre un accès supplémentaire au réseau, et sont ainsi des périphériques de risque moyen ou élevé. Il est également possible que la corruption de ce matériel entraîne la panne du réseau lui-même. Une telle panne peut énormément perturber l'entreprise.

Une fois que vous avez attribué un niveau de risque, il est nécessaire d'identifier les types d'utilisateurs de ce système. Les cinq types d'utilisateurs les plus courants sont :

- **Administrateurs** Utilisateurs internes responsables des ressources réseau.
- **Privilégiés** Utilisateurs internes qui ont besoin d'un accès plus important.
- **Utilisateurs** Utilisateurs internes avec un accès général.
- **Partenaires** Utilisateurs externes qui ont besoin d'accéder à quelques ressources.
- **Autres** Utilisateurs externes ou clients.

L'identification du niveau de risque et du type d'accès requis de chaque système réseau forme la base du tableau suivant sur la sécurité. Le tableau sur la sécurité une référence rapide pour chaque système et un point de départ pour de nouvelles mesures de sécurité, telle que la création d'une stratégie appropriée pour restreindre l'accès aux ressources réseau.

Système	Description	Niveau de risque	Types d'utilisateurs
Commutateurs ATM	Équipement réseau de base	Haute	Administrateurs pour la configuration des périphériques (personnel de support seulement) ; Tous les autres pour utilisation comme transport
Routeurs réseau	Périphérique réseau de distribution	Haute	Administrateurs pour la configuration des périphériques (personnel de support seulement) ; Tous les autres pour utilisation comme transport
Commutateurs en armoire	Périphérique réseau d'accès	Support	Administrateurs pour la configuration des périphériques (personnel de support seulement) ; Tous les autres pour utilisation comme transport
Serveurs ISDN ou	Périphérique réseau	Support	Administrateurs pour la configuration des périphériques (personnel de support

commutés	d'accès		seulement) ; Partenaires et utilisateurs privilégiés pour un accès spécial
Pare-feu	Périphérique réseau d'accès	Haute	Administrateurs pour la configuration des périphériques (personnel de support seulement) ; Tous les autres pour utilisation comme transport
Serveurs DNS et DHCP	Applications réseau	Support	Administrateurs pour la configuration ; Utilisateurs généraux et privilégiés pour l'usage
Serveur de messagerie électronique externe	Application réseau	Bas	Administrateurs pour la configuration ; Tous les autres pour le transport de messagerie entre le serveur Internet et le serveur de messagerie interne
Serveur de messagerie électronique interne	Application réseau	Support	Administrateurs pour la configuration ; Tous autres utilisateurs internes pour l'usage
Base de données Oracle	Application réseau	Moyen ou élevé	Administrateurs pour l'administration de système ; Utilisateurs privilégiés pour des mises à jour de données ; Utilisateurs généraux pour l'accès aux données ; Tous les autres pour l'accès aux données partiel

Établir une structure pour l'équipe chargée de la sécurité

Créez une équipe de sécurité interfonctionnelle menée par un Responsable de sécurité avec des participants de chacune des zones opérationnelles de votre société. Les représentants de l'équipe doivent connaître la politique de sécurité et les aspects techniques de la conception et de la mise en œuvre de la sécurité. Ceci requiert souvent une formation complémentaire pour les membres de l'équipe. L'équipe chargée de la sécurité a trois domaines de responsabilité : élaboration des politiques, pratique et réponse.

L'élaboration des politiques se concentre sur la création la révision des politiques de sécurité pour la société. Passez au moins en revue l'évaluation des risques et la politique de sécurité sur une base annuelle.

La pratique est l'étape pendant laquelle l'équipe chargée de la sécurité réalise l'évaluation des risques, l'approbation de la modification de la sécurité demande, passe en revue des alertes sécurité des deux constructeurs et la liste de diffusion de CERT, et transforme des conditions requises de stratégie de sécurité de langage clair en réalisations techniques spécifiques.

Le dernier domaine de responsabilité est la réponse. Tandis que la surveillance de réseau identifie souvent la violation de la sécurité, ce sont les membres de l'équipe chargée de la sécurité qui se chargent de diagnostiquer et de corriger une telle violation. Chaque membre de l'équipe chargée de la sécurité doit connaître en détail les fonctions de sécurité fournies par le matériel dans son domaine opérationnel.

Tandis que nous avons défini les responsabilités de l'équipe dans son ensemble, vous devez définir les différents rôles et responsabilités des membres de l'équipe chargée de la sécurité dans votre politique de sécurité.

Prévention

La prévention peut être divisée en deux parties : approuver les modifications de la sécurité et contrôler la sécurité de votre réseau.

Approuver les modifications de sécurité

Les modifications de la sécurité sont définies comme modifications de l'équipement réseau qui ont une incidence possible sur la sécurité globale du réseau. Votre politique de sécurité doit identifier les conditions requises spécifiques en matière de configuration de la sécurité dans des termes non techniques. En d'autres termes, au lieu de définir une condition requise sous la forme « Aucune connexion FTP externe ne sera autorisée par le pare-feu », définissez la condition requise sous la forme « Les connexions externes ne doivent pas pouvoir récupérer des fichiers depuis le réseau interne ». Vous devrez définir un seul ensemble de conditions requises pour votre organisation.

L'équipe chargée de la sécurité doit examiner la liste de conditions requises en langage clair afin d'identifier les problèmes spécifiques de configuration de réseau ou de conception qui répondent aux exigences. Une fois que l'équipe a créé les changements de configuration du réseau requis pour mettre en place la politique de sécurité, vous pouvez appliquer ces derniers à toutes les futures modifications de configuration. L'équipe chargée de la sécurité peut passer en revue toutes les modifications, mais ce processus leur permet de passer en revue seulement les modifications qui présentent des risques suffisants pour justifier un traitement spécial.

Nous recommandons que l'équipe chargée de la sécurité passe en revue les types de modifications suivants :

- Toute modification de la configuration de pare-feu.
- Toute modification des listes de contrôle d'accès (ACL).
- Toute modification de la configuration du Protocole de gestion de réseau simple (SNMP).
- Toute modification ou mise à jour logicielle qui diffère de la liste de niveau de révision de logiciel approuvée.

Nous recommandons également l'adhésion aux directives suivantes :

- Modifiez couramment les mots de passe des périphériques réseau.
- Restreignez l'accès aux équipements réseau à une liste de personnel approuvée.
- Assurez-vous que les niveaux actuels de révision de logiciel de l'équipement réseau et des environnements du serveur sont conformes aux conditions requises en matière de configuration de la sécurité.

Outre ces directives d'approbation, demandez à un représentant de l'équipe chargée de la

sécurité de participer au comité d'approbation de la gestion des modifications, afin de contrôler toutes les modifications que le comité passe en revue. Le représentant de l'équipe chargée de la sécurité peut refuser n'importe quelle modification considérée comme une modification de la sécurité jusqu'à son approbation par l'équipe chargée de la sécurité.

Contrôler la sécurité de votre réseau

Le contrôle de la sécurité est semblable à la surveillance de réseau, sauf qu'il se concentre sur la détection des changements du réseau qui indiquent une violation de la sécurité. Le point de départ pour le contrôle de la sécurité est de déterminer ce qui constitue une violation. Dans Conduire une évaluation des risques, nous avons identifié le niveau de la surveillance requis en fonction de la menace pour le système. Dans Approuver les modifications de sécurité, nous avons identifié des menaces spécifiques pour le réseau. En observant ces deux paramètres, nous développerons une image claire de ce que vous devez contrôler et à quelle fréquence.

Dans le Tableau d'évaluation des risques, le pare-feu est considéré un périphérique réseau à haut risque, ce qui indique que vous devez le contrôler en temps réel. Dans la section Approuver les modifications de sécurité , vous observez que vous devez contrôler toutes les modifications du pare-feu. Ceci signifie que l'agent de sondage SNMP doit contrôler notamment les échecs de tentative de connexion, le trafic inhabituel, les modifications du pare-feu, l'accès accordé au pare-feu et les connexions configurées via le pare-feu.

D'après cet exemple, créez une politique de surveillance pour chaque zone identifiée dans votre évaluation des risques. Nous vous recommandons de contrôler le matériel à faible risque toutes les semaines, le matériel à risque moyen tous les jours et le matériel à haut risque toutes les heures. Si vous avez besoin d'une détection plus rapide, contrôlez sur une période une plus courte.

Pour finir, votre politique de sécurité doit aborder la façon de signaler les violations de sécurité à l'équipe chargée de la sécurité. Souvent, votre logiciel de surveillance réseau sera le premier à détecter la violation. Il doit déclencher une notification au centre des opérations, qui à son tour doit informer l'équipe chargée de la sécurité, à l'aide d'un pager si nécessaire.

Réponse

La réponse peut être divisée en trois parties : violations de la sécurité, restauration et révision.

Violation de la sécurité

Quand une violation est détectée, la capacité de protéger l'équipement réseau, de déterminer l'étendue de l'intrusion et de revenir à un fonctionnement normal dépend de décisions rapides. Prendre ces décisions d'avance facilite la gestion des intrusions.

La première action suivant la détection d'une intrusion est d'en informer l'équipe chargée de la sécurité. Sans procédure en place, les personnes adéquates interviendront beaucoup plus tard. Définissez dans votre politique de sécurité une procédure disponible 24 heures sur 24, 7 jours par semaine.

Vous devez ensuite définir le niveau d'autorité donné à l'équipe chargée de la sécurité pour apporter des modifications, et dans quelle ordre les modifications doivent être apportées. Les actions correctives possibles sont :

- Mettre en place des modifications pour empêcher l'accès à la violation.
- Isoler les systèmes violés.
- Contacter le fournisseur ou l'ISP afin d'essayer de tracer l'attaque.
- Utiliser des périphériques d'enregistrement pour recueillir des preuves.
- Déconnecter les systèmes violés ou la source de violation.
- Contacter la police ou d'autres agences gouvernementales.
- Arrêter les systèmes violés.
- Restaurer les systèmes selon une liste prioritaire.
- Informer le personnel de direction et juridique interne.

S'assurer de détailler toutes les modifications qui peuvent être apportées à la politique de sécurité sans l'approbation de la direction.

Pour finir, il y a deux raisons pour collecter et conserver des informations pendant une attaque de sécurité : pour déterminer à quel point les systèmes ont été compromis par une attaque de sécurité et poursuivre des violations externes. Le type d'informations et la manière dont vous les collectez diffèrent selon votre objectif.

Pour déterminer l'étendue de la violation, procédez comme suit :

- Enregistrez l'événement en obtenant des tracés de l'analyseur de réseau, des copies des fichiers journal, des comptes utilisateurs actifs et des connexions réseau.
- Limitez la compromission en désactivant les comptes, en déconnectant l'équipement réseau du réseau et en vous déconnectant d'Internet.
- Sauvegarder le système compromis pour faciliter une analyse détaillée des dommages et de la méthode d'attaque.
- Recherchez d'autres signes de compromission. Souvent quand un système est compromis, d'autres systèmes ou comptes sont impliqués.
- Mettez à jour et examinez les fichiers journal de périphérique de sécurité et les fichiers journal de surveillance réseau, car ils fournissent souvent des indices à la méthode d'attaque.

Si vous souhaitez prendre des mesures judiciaires, demandez à votre département juridique d'examiner les procédures pour recueillir des preuves et impliquer les autorités. Un tel examen augmente l'efficacité des preuves lors des procédures légales. Si la violation était de nature interne, contactez votre département des ressources humaines.

Restauration

La restauration des opérations réseau normales est l'objectif final de n'importe quelle réponse de violation de la sécurité. Définissez dans la politique de sécurité comment vous réalisez, sécurisez et mettez à disposition des sauvegardes normales. Comme chaque système a ses propres moyens et procédures de sauvegarde, la politique de sécurité doit agir en tant que méta-politique, détaillant pour chaque système les conditions de sécurité qui requièrent la restauration depuis la sauvegarde. Si l'approbation est requise avant de pouvoir effectuer toute restauration, incluez également le processus pour obtenir l'approbation.

Examen

Le processus de révision est l'effort final pour créer et maintenir une politique de sécurité. Il y a trois choses que vous devrez passer en revue : politique, position et pratique.

La politique de sécurité doit être un document vivant qui s'adapte à un environnement toujours changeant. La révision de la politique existante par rapport aux meilleures pratiques connues maintient le réseau à jour. En outre, vérifiez le site Web de CERT pour les conseils, les pratiques, les améliorations de la sécurité, et les alertes utiles qui peuvent être incorporées à votre stratégie de sécurité.

Vous devez également passer en revue la position du réseau en comparaison avec la position de sécurité désirée. Une entreprise extérieure qui se spécialise dans la Sécurité peut essayer de pénétrer le réseau et de tester non seulement la position du réseau, mais également la réponse de sécurité de votre organisation. Pour des réseaux à haute disponibilité, nous recommandons d'effectuer un tel test tous les ans.

En conclusion, la pratique est définie comme un entraînement ou un test du personnel de support afin d'assurer qu'ils ont une bonne compréhension de ce qu'ils doivent faire pendant une violation de la sécurité. Généralement, cet entraînement n'est pas annoncé par la direction et est effectué en conjonction avec le test de position de réseau. Cette révision identifie des lacunes dans les procédures et la formation du personnel de sorte que des mesures correctives puissent être prises.

Informations connexes

- Plus de livres blancs des meilleures pratiques
- Support technique - Cisco Systems