# Politique de sécurité réseau : Livre blanc sur les meilleures pratiques

## Table des matières

[Introduction](#)
[Préparation](#)
[Créer des instructions de stratégie d'utilisation](#)
[Réaliser une analyse des risques](#)
[Établir une structure d'équipe de sécurité](#)
[Prévention](#)
[Approuver les modifications de sécurité](#)
[Surveillance de la sécurité de votre réseau](#)
[Réponse](#)
[Violations de sécurité](#)
[Restauration](#)
[Révision](#)
[Informations connexes](#)

## Introduction

Sans stratégie de sécurité, la disponibilité de votre réseau peut être compromise. La politique commence par l'évaluation des risques pour le réseau et la constitution d'une équipe pour y répondre. La poursuite de la stratégie nécessite la mise en oeuvre d'une pratique de gestion des modifications de sécurité et la surveillance du réseau à la recherche de violations de sécurité. Enfin, le processus d'examen modifie la politique existante et s'adapte aux enseignements tirés.

Ce document se divise en trois parties : préparation, prévention et intervention. Examinons chacune de ces étapes en détail.

## Préparation

Avant d'implémenter une stratégie de sécurité, vous devez procéder comme suit :

- Créez des instructions de stratégie d'utilisation.
- Réaliser une analyse des risques.
- Établir une structure d'équipe de sécurité.

### Créer des instructions de stratégie d'utilisation

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

rôles et responsabilités des utilisateurs en matière de sécurité. Vous pouvez commencer par une politique générale qui couvre tous les systèmes et données réseau de votre entreprise. Ce document doit fournir à la communauté générale des utilisateurs une compréhension de la politique de sécurité, de son objectif, des directives pour améliorer leurs pratiques de sécurité et des définitions de leurs responsabilités de sécurité. Si votre entreprise 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 expliquées dans ce document.

L'étape suivante consiste à créer une déclaration d'utilisation acceptable pour les partenaires afin de leur permettre de comprendre les informations dont ils disposent, la disposition prévue de ces informations, ainsi que la conduite des employés de votre entreprise. Vous devez expliquer clairement tout acte spécifique qui a été identifié comme une attaque de sécurité et les mesures punitives qui seront prises si une attaque de sécurité est détectée.

Enfin, créez une instruction d'utilisation acceptable par l'administrateur pour expliquer les procédures d'administration des comptes d'utilisateurs, d'application des stratégies et de révision des privilèges. Si votre entreprise a des politiques spécifiques concernant les mots de passe utilisateur ou le traitement ultérieur des données, présentez clairement ces politiques également. Vérifiez la politique par rapport aux énoncés de politique d'utilisation acceptable par le partenaire et par l'utilisateur pour assurer l'uniformité. Assurez-vous que les exigences de l'administrateur répertoriées dans la politique d'utilisation acceptable sont prises en compte dans les plans de formation et les évaluations de performances.

## Réaliser une analyse des risques

Une analyse des risques doit identifier les risques pour votre réseau, vos ressources réseau et vos données. Cela ne signifie pas que vous devez identifier tous les points d'entrée possibles sur le réseau, ni tous les moyens d'attaque possibles. L'objectif d'une analyse des risques est d'identifier des parties de votre réseau, d'attribuer une évaluation des menaces à chaque partie et d'appliquer un niveau de sécurité approprié. Cela permet de maintenir un équilibre fonctionnel entre la sécurité et l'accès réseau requis.

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

- Risque faible Systèmes ou données qui, s'ils étaient compromis (données consultées par un personnel non autorisé, données corrompues ou données perdues), ne perturberaient pas l'activité ou n'auraient pas de conséquences juridiques 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 un personnel non autorisé, données corrompues ou données perdues) entraînerait une perturbation modérée de l'activité, des conséquences juridiques ou financières mineures ou fournirait un accès supplémentaire à d'autres systèmes. Le système ou les données ciblés nécessitent un effort modéré de restauration ou le processus de restauration perturbe le système.

- Risque élevé Systèmes ou données qui, s'ils étaient compromis (données consultées par un personnel non autorisé, données corrompues ou données perdues), provoqueraient une perturbation extrême de l'activité, auraient des conséquences juridiques ou financières majeures ou menaceraient la santé et la sécurité d'une personne. Le système ou les données ciblés nécessitent un effort important de restauration ou le processus de restauration perturbe l'activité ou d'autres systèmes.

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

Les équipements de réseau tels que les commutateurs, les routeurs, les serveurs DNS et les serveurs DHCP peuvent permettre un accès plus étendu au réseau et sont donc des périphériques à risque moyen ou élevé. Il est également possible que la corruption de cet équipement entraîne l’effondrement du réseau. Un tel échec peut être extrêmement perturbateur pour 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.
- Utilisateurs internes privilégiés nécessitant un accès plus étendu.
- Utilisateurs Utilisateurs internes avec accès général.
- Partenaires Utilisateurs externes ayant besoin d'accéder à certaines ressources.
- Autres Utilisateurs ou clients externes.

L'identification du niveau de risque et du type d'accès requis de chaque système réseau constitue la base de la matrice de sécurité suivante. La matrice de sécurité fournit une référence rapide pour chaque système et un point de départ pour d'autres mesures de sécurité, telles que la création d'une stratégie appropriée pour restreindre l'accès aux ressources réseau.

| système | Description | Niveau de risque | Types d'utilisateurs |
|---|---|---|---|
| Commutateurs ATM | Périphérique réseau principal | Élevé | Administrateurs pour la configuration des périphériques (personnel d'assistance |

| | | | |
|---|---|---|---|
| | | | uniquement) ; Tous les autres devant servir de moyen de transport |
| Routeurs réseau | Dispositif de réseau de distribution | Élevé | Administrateurs pour la configuration des périphériques (personnel d'assistance uniquement) ; Tous les autres devant servir de moyen de transport |
| Commutateurs de placard | Périphérique réseau d'accès | Moyen | Administrateurs pour la configuration des périphériques (personnel d'assistance uniquement) ; Tous les autres devant servir de moyen de transport |
| Serveurs RNIS ou commutés | Périphérique réseau d'accès | Moyen | Administrateurs pour la configuration des périphériques (personnel d'assistance uniquement) ; Partenaires et utilisateurs privilégiés pour un accès spécial |
| Pare-Feu | Périphérique réseau d'accès | Élevé | Administrateurs pour la configuration |

| | | | |
|---|---|---|---|
| | | | des périphériques (personnel d'assistance uniquement) ; Tous les autres devant servir de moyen de transport |
| Serveurs DNS et DHCP | Applications réseau | Moyen | Administrateurs pour la configuration ; Utilisateurs généraux et privilégiés à utiliser |
| Serveur de messagerie externe | Application réseau | Faible | Administrateurs pour la configuration ; Tous les autres pour le transport du courrier entre Internet et le serveur de messagerie interne |
| Serveur de messagerie interne | Application réseau | Moyen | Administrateurs pour la configuration ; Tous les autres utilisateurs internes à utiliser |
| base de données Oracle | Application réseau | Moyenne ou élevée | Administrateurs pour l'administration système ; Utilisateurs privilégiés pour les mises à jour de données ; Utilisateurs généraux pour l'accès aux données ; Tous |

| | | | |
|---|---|---|---|
| | | | les autres pour un accès partiel aux données |

### Établir une structure d'équipe de sécurité

Créez une équipe de sécurité interfonctionnelle dirigée par un responsable de la sécurité avec des participants de chaque domaine d'activité de votre entreprise. Les représentants de l'équipe doivent connaître la politique de sécurité et les aspects techniques de la conception et de la mise en oeuvre de la sécurité. Souvent, cela nécessite une formation supplémentaire pour les membres de l'équipe. L'équipe de sécurité a trois domaines de responsabilité : l'élaboration de politiques, les pratiques et les interventions.

Le développement des politiques est axé sur l'établissement et la révision des politiques de sécurité de l'entreprise. Révisez au minimum l'analyse des risques et la stratégie de sécurité sur une base annuelle.

La mise en pratique est l'étape au cours de laquelle l'équipe de sécurité effectue l'analyse des risques, l'approbation des demandes de modification de sécurité, examine les alertes de sécurité des fournisseurs et de la liste de diffusion CERT , et transforme les exigences de la stratégie de sécurité en langage clair en implémentations techniques spécifiques.

Le dernier domaine de responsabilité est la réponse. Bien que la surveillance du réseau identifie souvent une violation de la sécurité, ce sont les membres de l'équipe de sécurité qui procèdent au dépannage et à la résolution d'une telle violation. Chaque membre de l'équipe de sécurité doit connaître en détail les dispositifs de sécurité fournis par l'équipement dans sa zone opérationnelle.

Bien que nous ayons défini les responsabilités de l'équipe dans son ensemble, vous devez définir les rôles et responsabilités individuels des membres de l'équipe de sécurité dans votre stratégie de sécurité.

## Prévention

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

### Approuver les modifications de sécurité

Les modifications de sécurité sont définies comme des modifications apportées à l'équipement réseau qui peuvent avoir un impact sur la sécurité globale du réseau. Votre stratégie de sécurité doit identifier les exigences spécifiques de configuration de la sécurité en termes non techniques. En d'autres termes, au lieu de définir une exigence comme « Aucune source externe de connexions FTP ne sera autorisée à travers le pare-feu », définissez l'exigence comme « Les connexions externes ne devraient pas pouvoir récupérer des fichiers à partir du réseau interne ». Vous devrez définir un ensemble unique d'exigences pour votre organisation.

L'équipe de sécurité doit examiner la liste des exigences en langage clair afin d'identifier les

problèmes de configuration ou de conception spécifiques du réseau qui répondent à ces exigences. Une fois que l'équipe a créé les modifications de configuration réseau requises pour mettre en oeuvre la stratégie de sécurité, vous pouvez les appliquer à toute modification de configuration future. Bien qu'il soit possible pour l'équipe de sécurité d'examiner toutes les modifications, ce processus ne lui permet d'examiner que les modifications qui présentent un risque suffisant pour justifier un traitement spécial.

Nous recommandons à l'équipe de sécurité d'examiner les types de modifications suivants :

- Toute modification de la configuration du pare-feu.
- Toute modification apportée aux listes de contrôle d’accès (ACL).
- Toute modification apportée à la configuration du protocole SNMP (Simple Network Management Protocol).
- Toute modification ou mise à jour du logiciel qui diffère de la liste de niveau de révision du logiciel approuvé.

Nous vous recommandons également de respecter les directives suivantes :

- Modifiez régulièrement les mots de passe des périphériques réseau.
- Restreignez l'accès aux périphériques réseau à une liste de personnel approuvée.
- S'assurer que les niveaux actuels de révision logicielle des équipements réseau et des environnements de serveurs sont conformes aux exigences de configuration de la sécurité.

En plus de ces directives d'approbation, demandez à un représentant de l'équipe de sécurité de siéger au conseil d'approbation de la gestion des modifications afin de surveiller toutes les modifications examinées par le conseil. Le représentant de l'équipe de sécurité peut refuser toute modification considérée comme une modification de sécurité tant qu'elle n'a pas été approuvée par l'équipe de sécurité.

## Surveillance de la sécurité de votre réseau

La surveillance de la sécurité est similaire à la surveillance du réseau, sauf qu'elle se concentre sur la détection des modifications du réseau qui indiquent une violation de la sécurité. Le point de départ de la surveillance de la sécurité consiste à déterminer ce qu'est une violation. Dans Effectuer une analyse des risques, nous avons identifié le niveau de surveillance requis en fonction de la menace pour le système. Dans Approuver les modifications de sécurité, nous avons identifié des menaces spécifiques au réseau. En examinant ces deux paramètres, nous obtiendrons une image claire de ce que vous devez surveiller et à quelle fréquence.

Dans la matrice d'analyse des risques, le pare-feu est considéré comme un périphérique réseau à haut risque, ce qui indique que vous devez le surveiller en temps réel. Dans la section Approbation des modifications de sécurité, vous voyez que vous devez surveiller les modifications apportées au pare-feu. Cela signifie que l'agent d'interrogation SNMP doit surveiller des éléments tels que les tentatives de connexion infructueuses, le trafic inhabituel, les modifications apportées

au pare-feu, l'accès accordé au pare-feu et les connexions configurées via le pare-feu.

Dans cet exemple, créez une stratégie de surveillance pour chaque zone identifiée dans votre analyse des risques. Nous vous recommandons de surveiller les équipements à faible risque chaque semaine, les équipements à risque moyen chaque jour et les équipements à haut risque toutes les heures. Si vous avez besoin d'une détection plus rapide, effectuez une surveillance sur une période plus courte.

Enfin, votre stratégie de sécurité doit indiquer comment informer l'équipe de sécurité des violations de la sécurité. Souvent, votre logiciel de surveillance du réseau sera le premier à détecter la violation. Il doit déclencher une notification au centre d'opérations, qui à son tour doit avertir l'équipe de 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.

## Violations de sécurité

Lorsqu'une violation est détectée, la capacité à protéger l'équipement réseau, à déterminer l'étendue de l'intrusion et à rétablir le fonctionnement normal dépend de décisions rapides. Le fait de prendre ces décisions à l'avance rend la réponse à une intrusion beaucoup plus facile à gérer.

La première action qui suit la détection d'une intrusion est la notification de l'équipe de sécurité. Sans une procédure en place, il y aura beaucoup de retard dans l'obtention des bonnes personnes pour appliquer la bonne réponse. Définissez dans votre stratégie de sécurité une procédure disponible 24 heures sur 24, 7 jours sur 7.

Vous devez ensuite définir le niveau d'autorité accordé à l'équipe de sécurité pour effectuer les modifications, et dans quel ordre elles doivent être effectuées. Les mesures correctives possibles sont les suivantes :

- Mise en oeuvre des modifications pour empêcher un accès ultérieur à la violation.
- Isoler les systèmes violés.
- Contacter l'opérateur ou le FAI pour tenter de tracer l'attaque.
- Utilisation d'appareils d'enregistrement pour recueillir des preuves.
- Déconnexion des systèmes enfreints ou de la source de la violation.
- Communiquer avec la police ou d'autres organismes gouvernementaux.
- Arrêt des systèmes violés.
- Restauration des systèmes selon une liste de priorités.
- Informer le personnel de gestion et le personnel juridique internes.

Veillez à détailler toutes les modifications pouvant être apportées sans l'approbation de la direction dans la stratégie de sécurité.

Enfin, la collecte et la mise à jour d'informations lors d'une attaque de sécurité ont deux raisons : pour déterminer la mesure dans laquelle les systèmes ont été compromis par une attaque de sécurité et pour poursuivre les 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 traces de l'analyseur du réseau, des copies des fichiers journaux, des comptes d'utilisateurs actifs et des connexions réseau.
- Limitez les risques supplémentaires en désactivant les comptes, en déconnectant l'équipement réseau du réseau et en vous déconnectant d'Internet.
- Sauvegardez le système compromis pour faciliter une analyse détaillée des dommages et de la méthode d'attaque.
- Recherchez d'autres signes de compromission. Souvent, lorsqu'un système est compromis, d'autres systèmes ou comptes sont impliqués.
- Tenir à jour et examiner les fichiers journaux des périphériques de sécurité et les fichiers journaux de surveillance du réseau, car ils fournissent souvent des indices sur la méthode d'attaque.

Si vous souhaitez intenter une action en justice, demandez à votre service juridique de revoir les procédures de collecte des preuves et d'implication des autorités. Un tel examen accroît l'efficacité de la preuve dans les procédures judiciaires. Si la violation était de nature interne, contactez votre service des ressources humaines.

## Restauration

La restauration du fonctionnement normal du réseau est l'objectif final de toute réponse aux violations de sécurité. Définissez dans la stratégie de sécurité la manière dont vous effectuez, sécurisez et rendez disponibles les sauvegardes normales. Comme chaque système dispose de ses propres moyens et procédures de sauvegarde, la stratégie de sécurité doit agir comme une méta-stratégie, détaillant pour chaque système les conditions de sécurité qui nécessitent une restauration à partir d'une sauvegarde. Si une approbation est requise avant que la restauration puisse être effectuée, inclure également le processus d'obtention de l'approbation.

## Révision

Le processus d'examen est le dernier effort de création et de gestion d'une stratégie de sécurité. Il y a trois choses que vous aurez besoin de revoir : la politique, la posture et la pratique.

La politique de sécurité doit être un document vivant qui s'adapte à un environnement en constante évolution. L'examen de la politique existante par rapport aux meilleures pratiques

connues permet de maintenir le réseau à jour. Consultez également le site Web du CERT pour obtenir des conseils, des pratiques, des améliorations en matière de sécurité et des alertes qui peuvent être incorporés à votre stratégie de sécurité.

Vous devez également comparer la position du réseau à la position de sécurité souhaitée. Une entreprise externe spécialisée dans la sécurité peut tenter de pénétrer le réseau et tester non seulement la position du réseau, mais également la réponse de votre entreprise en matière de sécurité. Pour les réseaux à haute disponibilité, nous vous recommandons d'effectuer ce test chaque année.

Enfin, la pratique est définie comme un exercice ou un test effectué par le personnel d'assistance pour s'assurer qu'il comprend clairement ce qu'il faut faire en cas de violation de la sécurité. Souvent, cette exploration n'est pas annoncée par la direction et est effectuée conjointement avec le test de la position du réseau. Cet examen permet de relever les lacunes dans les procédures et la formation du personnel afin que des mesures correctives puissent être prises.

## Informations connexes

- Autres livres blancs sur les meilleures pratiques
- Support technique - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.