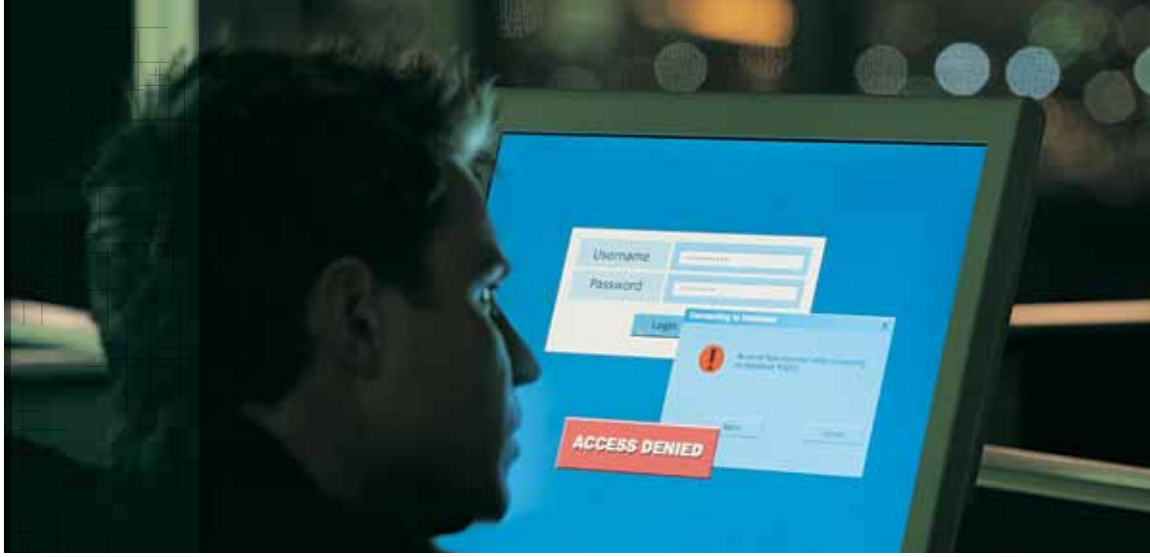
McAfee
An Intel Company

GESTION DE LA SÉCURITÉ ET DES RISQUES

Guide de solution



Security Connected

Le cadre d'implémentation McAfee Security Connected permet l'intégration de plusieurs produits, services et partenariats dans le but d'assurer une réduction des risques efficace et centralisée. Fondée sur plus de vingt ans de pratiques éprouvées en matière de sécurité, l'approche Security Connected apporte une assistance précieuse à toutes les entreprises, indépendamment de leur taille, de leur secteur d'activités ou de leur situation géographique. Ainsi, elle permet d'améliorer l'état de sécurisation général, d'optimiser les systèmes de protection pour une meilleure rentabilité de l'investissement en sécurité et d'aligner les stratégies de sécurité avec les initiatives d'ordre commercial. L'architecture de référence McAfee Security Connected vous mène des idées jusqu'à l'implémentation. Faites-en bon usage et adaptez ses concepts aux risques, à l'infrastructure et aux objectifs spécifiques de votre entreprise. McAfee consacre tous ses efforts à trouver des solutions novatrices afin d'assurer à ses clients une protection irréprochable.

Téléchargez les ressources les plus récentes sur le site www.mcafee.com/fr/enterprise/reference-architecture/index.aspx.

Pour une approche proactive de la gestion des risques

Défis

Jusqu'il y a peu, la gestion de la sécurité et des risques se préoccupait essentiellement des risques financiers et de la conformité. Les audits et les processus de gouvernance étaient des événements prévisibles que les équipes informatiques tentaient de minimiser et d'automatiser. Le risque était un concept relativement figé. Aujourd'hui, par contre, les attaques se sont diversifiées, qu'elles se fassent discrètes et lentes comme les attaques ciblées, ou ultrarapides dans le cas des actions cyberactivistes ou des attaques de logiciels malveillants. Leur cadence est telle que les équipes de direction et les administrateurs informatiques doivent accorder une plus grande attention aux événements émergents et prendre rapidement des décisions basées sur l'évaluation des risques pour les neutraliser.

Bien entendu, la notion de risque financier ou de conformité est également devenue plus dynamique. Quand on sait que les organismes de réglementation peaufinent de façon indépendante plus de 200 directives dans le monde pour les adapter à l'évolution des modèles économiques et commerciaux, il est naturel que le tableau autrefois statique des risques soit désormais aussi changeant qu'un kaléidoscope.

Gérer des grands volumes de données de sécurité

A l'heure actuelle, gérer les risques revient à donner un sens à des informations toujours plus nombreuses : analyses des vulnérabilités, journaux des bases de données et des applications, flux, enregistrements des sessions et des accès, alertes et analyses des tendances. Les flux de données sont issus de multiples systèmes chargés de protéger un nombre croissant d'utilisateurs qui ont partout accès à un éventail toujours plus large de terminaux.

Les audits, qu'ils soient motivés par des directives internes ou externes, illustrent parfaitement la difficulté de gérer des données recueillies auprès d'une multitude de sources. Les administrateurs informatiques doivent identifier et collationner des flux de données dans le format demandé par les auditeurs. Les audits, par définition, analysent une situation antérieure et évaluent les risques passés. Ils drainent les ressources de l'entreprise et la détournent d'une priorité plus importante : la gestion proactive des risques, à savoir la capacité à anticiper, à comprendre et à limiter des risques en constante évolution avant qu'ils n'affectent l'entreprise.

Evaluer les risques

Le monde entier est confronté au phénomène de l'explosion des volumes de données et, dans le cas qui nous occupe, de grands volumes de données de sécurité. (L'expression anglaise utilisée pour le décrire est « *Big Data* ».) Appréhender toutes les nuances des menaces de sécurité peut prendre plusieurs jours, voire plusieurs mois. La plupart des analystes en sécurité sont confrontés à des problèmes de gestion de données similaires à ceux des administrateurs informatiques chargés des audits : face à la multitude de flux de données isolés, il devient difficile de dresser un tableau précis et cohérent des événements. Plus le volume de données collectées et analysées est important, plus il est malaisé d'y mettre de l'ordre et de reconstituer les événements. Il faut attendre de disposer d'une image précise de la situation, c.-à-d. longtemps après l'événement, pour adapter les stratégies et les systèmes de protection afin d'éviter que cet événement se reproduise.

Et que faire en cas d'attaque brutale et rapide, par exemple une attaque par déni de service ou un ver à propagation rapide ? S'il faut plusieurs jours ou mois pour diagnostiquer le problème, celui-ci peut avoir sur l'entreprise des répercussions majeures voire fatales, du point de vue de sa santé financière ou de sa conformité. Quelles ressources sont réellement vulnérables à cette menace et combien disposent de contrôles ou de contre-mesures pour la neutraliser ? Pour répondre à cette question, les administrateurs ont besoin d'une visibilité sur le niveau de sécurité de l'ensemble des systèmes, y compris le parc toujours plus important de terminaux personnels et mobiles qui accèdent à leurs réseaux.

Réagir face aux événements

Après avoir correctement appréhendé la menace, il faut ensuite établir des priorités et appliquer des mesures correctives. Parmi les ressources, lesquelles sont les plus critiques ? Lesquelles peuvent attendre ? Les administrateurs jonglent souvent entre différentes consoles de gestion pour lancer des analyses, exécuter des scripts, rectifier des stratégies, installer des mises à jour ou placer des systèmes en quarantaine. Tous les produits qui inondent le marché de la sécurité ne font qu'accroître les coûts et la complexité à cause de la diversité des interfaces utilisateur, des formats de données, des modèles de stratégies ou des types de rapports. Cela se traduit inévitablement par des erreurs et des lacunes dans la couverture, qui exposent l'entreprise et ses ressources à des risques inutiles, par ailleurs souvent mal identifiés.

Vous ne pouvez plus vous contenter d'être réactif en matière de gestion des risques. Vous devez anticiper, grâce à une vue complète de la situation, afin d'identifier et de gérer les risques à mesure qu'ils évoluent. La collecte d'informations sur la situation de risque fournit un contexte dynamique sur l'environnement de menaces mondial, mais aussi sur les ressources et le niveau de sécurité de votre entreprise. Les technologies de gestion des risques automatisées utilisent ce contexte pour vous aider à percevoir les relations entre les différents éléments afin que vous puissiez optimiser vos stratégies et vos systèmes de protection.

Solutions

Les grands volumes de données de sécurité et les problèmes qu'ils suscitent au niveau des processus opérationnels compliquent la gestion de la sécurité et des risques, mais une stratégie complète alliée aux technologies dernier cri peut aider à remettre de l'ordre. Dans le cadre de la gestion des risques financiers et de la conformité, vous devez prendre en compte, en temps réel, les risques potentiels introduits par les événements internes et externes. Une approche unifiée permet de rationaliser les processus et de mettre en place des réponses automatisées qui diminuent les coûts et les temps de réponse. L'équipe de direction bénéficie d'une visibilité de l'impact potentiel des événements de sécurité sur le niveau de risque, tandis que les administrateurs disposent des informations pertinentes et du contrôle nécessaires pour limiter les risques de façon proactive.

Les systèmes de gestion des événements et des informations de sécurité (SIEM) récents sont étroitement intégrés avec la gestion de la sécurité et de la conformité pour les équipements, les serveurs, les applications et les bases de données. Cette plate-forme de gestion de la sécurité peut fournir une console de contrôle qui facilite la visibilité et l'agilité opérationnelle. Plus l'intégration sera forte entre ces systèmes de gestion, les informations sur les risques et les systèmes de sécurité, mieux vous pourrez comprendre et gérer les risques. Une approche basée sur une plate-forme permet d'harmoniser et d'unifier les processus, les stratégies, les workflows ou encore les rapports fragmentés et spécifiques. L'incorporation de connaissances à jour permet d'analyser les données en fonction de l'évolution des risques et contribue à améliorer la précision, la pertinence et les temps de réponse pour limiter le risque.

Evaluer les vulnérabilités

La plupart des entités soumises à des réglementations analysent les vulnérabilités afin de respecter leurs impératifs de conformité. Cela dit, il arrive souvent que les analyses planifiées « oublient » les systèmes distants ou inactifs et qu'elles ignorent des actifs stratégiques comme les applications ou les bases de données. Des systèmes non fiables peuvent ainsi passer entre les mailles du filet alors qu'ils hébergent des vulnérabilités exploitables. Une approche rigoureuse en matière de gestion des vulnérabilités des ressources du réseau peut prendre en compte ces différents systèmes et éliminer les failles de conformité. Vous pouvez utiliser des informations dynamiques sur les risques, la valeur des actifs et des contre-mesures pertinentes pour mieux cibler les analyses ou l'implémentation de contre-mesures.

Améliorer la connaissance du contexte situationnel

Face aux cyberattaques et à la perméabilité des périmètres, la plupart des entreprises souhaitent mieux cerner les risques en constante évolution et y réagir de façon plus adaptée. La clé du problème consiste à identifier les informations réellement pertinentes, au moment opportun. S'ils possèdent la vitesse et la capacité requises pour traiter de grands volumes de données, les outils SIEM peuvent surveiller les applications et les bases de données, gérer les journaux et normaliser les événements dans des tableaux de bord de données corrélées. Certains intègrent également des connaissances en temps réel sur le paysage des menaces ainsi que les utilisateurs, les systèmes, les données, les risques et les contre-mesures. Avec un tableau aussi complet du contexte situationnel, vous pouvez comprendre rapidement les activités liées à la sécurité, y compris les activités passées. Des outils d'analyse robustes vous aident à prévoir et à repérer les attaques, puis à les neutraliser en quelques minutes au lieu de plusieurs jours.

Inspecter le trafic réseau

Les réseaux représentent à la fois des infrastructures critiques et des vecteurs de fuites de données sensibles et réglementées. En surveillant et en gérant le trafic réseau, y compris le trafic chiffré, les administrateurs peuvent limiter les aspects dangereux ou indésirables de la navigation Internet ou de l'utilisation des applications et faire en sorte que les stratégies relatives au contenu soient mises en œuvre. L'intégration de solutions de sécurisation des réseaux de dernière génération avec des produits SIEM ou de sécurisation des systèmes peuvent aider les gestionnaires des risques à mettre en œuvre des stratégies, à se protéger contre les menaces de type « jour zéro » ainsi qu'à surveiller, à analyser et à générer des rapports sur la conformité.

Optimiser la gestion des journaux

Les journaux fournissent une mine d'informations utilisées dans le cadre de l'administration des preuves électroniques, des audits et d'autres exigences de conformité. Pour autant bien sûr que vous puissiez faire le tri dans la masse d'informations collectées pour en extraire les données significatives. Avec une solution de gestion des journaux performante, sécurisée et intégrée, vous pouvez recueillir des données en temps réel auprès de toutes les sources pertinentes et conserver les journaux conformément à une procédure normalisée et sécurisée de chaîne de traçabilité.
Le contrôle des applications permet d'éviter que des cybercriminels ne viennent pirater les journaux pour dissimuler leurs actions. L'association de fonctions de contrôle des journaux et d'autres outils d'analyse des risques et de la sécurité permet de transmettre les informations des journaux aux utilisateurs les plus aptes à les exploiter pour gérer les risques.

Meilleures pratiques

- Aligner et unifier les processus et contrôles fragmentés
- Automatiser la collecte, la corrélation, l'évaluation, la réponse et la surveillance
- Exploiter des informations dynamiques sur les risques, des analyses d'hypothèses et des réponses basées sur des stratégies pour assurer une identification et un blocage proactifs des menaces
- Veiller à ce que les programmes de gestion des risques et de la sécurité couvrent tous les équipements, toutes les données et l'intégralité de l'infrastructure informatique
- Rassembler toutes les informations sur les risques et la sécurité à l'échelle de l'entreprise sur une même plate-forme pour optimiser la gestion
- Surveiller la situation de façon continue et proactive pour détecter et réagir à une évolution du risque, préserver la conformité et prévenir des événements de sécurité futurs

Les processus manuels de sécurisation et de gestion des risques sont associés à une probabilité d'échec plus forte et constituent l'un des principaux facteurs de l'augmentation des coûts de conformité et de sécurisation.

Génération de valeur

Une stratégie de gestion de la sécurité et des risques complète qui s'appuie sur une plate-forme automatisée avec gestion des risques pourra apportera de multiples avantages à votre entreprise :

- Connaissance de la situation grâce à des données de contexte et des analyses riches en informations pertinentes
- Diagnostic des incidents et réaction en quelques secondes au lieu de plusieurs heures pour limiter les dommages, prévenir les compromissions de données et diminuer les coûts de l'application de mesures correctives
- Diminution du nombre d'incidents de sécurité, de violations de conformité et des coûts par incident
- Simplification des processus de configuration des stratégies de conformité et de la génération de rapports pour améliorer l'efficacité opérationnelle
- Diminution du nombre de plates-formes, de composants matériels et de logiciels de différents fournisseurs utilisés pour la gestion de la sécurité
- Réduction des coûts opérationnels et du temps consacré à la formation

Architecture de référence McAfee Security Connected — Documentation associée

Niveau II

- Contrôle et surveillance des modifications
- Protection des centres de données
- Gestion efficace de la conformité PCI, au bénéfice de l'entreprise tout entière

Niveau III

- Evaluation des vulnérabilités
- Amélioration de la connaissance du contexte situationnel
- Inspection du trafic réseau
- Optimisation de la gestion des journaux
- Investigation des fuites de données
- Intégration sécurisée des médias sociaux à notre quotidien
- Protection de la propriété intellectuelle

Pour plus d'informations sur l'architecture de référence McAfee Security Connected, consultez notre site à l'adresse : www.mcafee.com/fr/enterprise/reference-architecture/index.aspx.

L'auteur

Barbara G. Kay est analyste en chef de l'agence Secure By Design Group. Dotée d'une certification CISSP, elle est experte dans le domaine de la protection des informations dans les entreprises mobiles et distribuées ainsi que dans la sensibilisation des internautes à une utilisation d'Internet sans risques. Avant de créer Secure By Design en 2006, Barbara G. Kay était Directrice du Marketing du projet SPI (Security and Privacy Initiative) de Sun. Elle est diplômée du Dartmouth College.

McAfee S.A.S.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr