Microsoft

Six étapes vers une stratégie de sécurité holistique

Ces informations vous concernent si :

vous êtes un responsable de la sécurité des systèmes informatiques qui

- recherche un guide rapide et concis sur la stratégie de sécurité globale
- souhaite se tenir au courant des dernières pratiques en matière de sécurité

Temps de lecture estimé : 9 minutes

Table des matières

Répondre au défi

La sécurisation des données et des systèmes est une priorité absolue pour les organisations. Mais relever ce défi devient de plus en plus difficile au fur et à mesure que les attaques deviennent plus sophistiquées, que les employés utilisent un plus grand nombre d'appareils et d'applications, et que les flux de données entrent et sortent de votre entreprise de plus de façons. Avec la généralisation du travail à distance, les risques pour la sécurité sont encore plus grands.

Les dirigeants doivent trouver un équilibre entre ces difficultés et les besoins de collaboration, d'innovation et de croissance d'une entreprise. Il vous faut une approche multiforme en matière de sécurité qui protège constamment tous les points de terminaison, détecte les signes précoces d'une atteinte à la sécurité et y répond avant que des dommages ne surviennent. Indépendamment de la solidité de vos défenses, les mesures préventives ne suffisent plus. Il vous faut également adopter une posture de « violation présumée » qui comprend des mesures de détection et de réponse.

Les responsables de la sécurité des systèmes informatiques (RSSI) d'aujourd'hui ont besoin de cadres de sécurité agiles qui permettent la transformation numérique, soutenus par des stratégies globales intégrées dans les technologies, les processus et les programmes de formation. Bien que les solutions sur place disposent de telles fonctionnalités, une migration vers le nuage améliore immédiatement les capacités de sécurité de votre organisation.

> **Ce livre électronique dévoile les six pratiques exemplaires des RSSI qui font de la sécurité la pierre angulaire du succès des entreprises. Ces pratiques exemplaires sont applicables à une infrastructure sur place, mais sont infiniment plus faciles à appliquer dans un système infonuagique**

1. Utiliser des produits de sécurité intégrés pour garantir une réaction rapide

75

Le nombre de produits de sécurité utilisés par une grande organisation typique[1].

Les menaces ont évolué des attaques qui visent à briser les systèmes pour les piller à celles qui les compromettent dans le but de maintenir une présence persistante à long terme. Les pirates exploitent désormais différents vecteurs d'attaque ainsi qu'un éventail de techniques et d'outils de plus en plus sophistiqués : vol des informations d'identification, installation de logiciels malveillants qui s'autodétruisent pour éviter d'être détectés, modification des processus internes, redirection des données du réseau, fraude au piratage psychologique et même ciblage du téléphone mobile ou des appareils personnels des employés.

La difficulté de l'intégration rend difficile d'avoir une vue globale et de prioriser les menaces rapidement. Bien qu'elles soient destinées à résoudre des problèmes précis, ces solutions œuvrent rarement de concert. Bon nombre d'entre elles utilisent des tableaux de bord, des consoles et des journaux propriétaires. Les difficultés liées à leur intégration compliquent la définition d'une vision globale et la hiérarchisation rapide des différentes menaces. Le défi est encore plus grand lorsqu'il s'agit de gérer à la fois des ressources dans le nuage et des ressources sur place. Par conséquent, les attaques peuvent passer inaperçues pendant plus de 140 jours[2].

[1] « Symantec Introduces New Era of Advanced Threat Protection », Businesswire, October 2015.

[2] « Threat Landscape: By the Numbers », Mandiant, une société de FireEye Company, 2016.

Essayez cela

Alors que la détection et la réponse rapides deviennent plus importantes, ces pratiques exemplaires ont été déterminées :

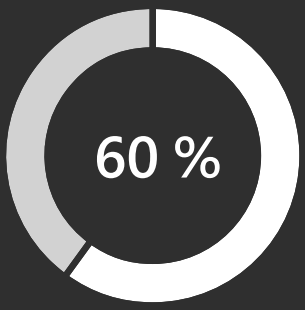
- Bénéficiez d'une vue globale sur l'ensemble de votre système de sécurité pour votre réseau, y compris le nuage et les environnements hybrides.
- Créez un écosystème de produits et de plateformes de sécurité qui s'intègrent les uns aux autres tout en fournissant des informations.
- Travaillez avec des fournisseurs de technologies qui collaborent et partagent leurs informations avec tous les professionnels de la sécurité.

Points-clés

Le manque d'intégration entre les produits de sécurité complique pour les équipes de sécurité la détection et la résolution rapides des menaces de manière holistique.

Recherchez des produits conçus pour s'intégrer avec d'autres.

2. Gérer l'accès en fonction de l'identité, indépendamment du point de terminaison



des violations résultent d'un point de terminaison compromis[3].

Une violation de données peut entraîner des coûts considérables. La mise en place de contrôles de sécurité adéquats pour gagner en visibilité sur les menaces et les attaques peut permettre de remédier à ces coûts élevés. Mais les équipes de sécurité doivent également prendre en charge la « consumérisation » des TI, où les employés ne travaillent plus exclusivement sur des appareils strictement contrôlés produits par l'entreprise, et doivent s'attendre à travailler n'importe où, indépendamment de l'appareil ou de la plateforme, qu'ils aient été approuvés ou non par le service informatique de l'entreprise.

Dans le monde actuel, les stratégies de sécurité axées sur l'identité lient l'accès à l'identité, et non aux appareils eux-mêmes. Appliquez des mécanismes de contrôle adaptés au rôle et aux besoins de l'utilisateur, quels que soient la façon et l'endroit où il se connecte. Se concentrer sur l'authentification et la gestion des utilisateurs au moment où ils accèdent aux ressources de l'organisation permet également à cette dernière de protéger ses données indépendamment du lieu de stockage, du mode d'accès et des personnes qui les partagent.

[3] « Top Five Security Threats Facing Your Business and How To Respond », blogue Microsoft Secure, octobre 2016.

Essayez cela

L'abandon d'une stratégie de sécurité uniquement axée sur les points de terminaison vous permet d'adopter une approche plus robuste. Ces outils peuvent vous aider :

- **Les solutions de gestion des identités et des accès (GIA)** et la gestion des applications mobiles **avec les solutions de prévention des pertes de** données (PPD). Elles contribuent toutes deux à réduire les risques en protégeant l'accès aux applications et aux données dans les ressources de l'entreprise et le nuage. La GIA évite la multiplication des informations d'identification en attribuant à chaque employé une identité unique pour accéder aux ressources dans le nuage et sur place. Les systèmes de GIA infonuagiques peuvent aussi bénéficier des renseignements sur les menaces et des analyses du fournisseur de technologies pour mieux détecter les tentatives d'accès anormales et intervenir de manière automatique et appropriée.
- **L'authentification multifacteur (MFA)** ajoute une couche de protection supplémentaire en demandant à l'utilisateur à la fois un élément qu'il connaît (son mot de passe) et un autre qu'il possède (authentification secondaire via l'appareil, l'empreinte digitale ou la reconnaissance faciale). D'autres tactiques rigoureuses comprennent la base de l'accès en fonction des risques pour les utilisateurs, pour l'appareil, pour l'application et même pour l'emplacement. Ces fonctionnalités peuvent automatiquement autoriser, bloquer ou exiger la MFA d'un utilisateur en temps réel selon les politiques que vous définissez, ce qui permet essentiellement aux organisations d'augmenter leur protection à leur propre porte principale.

Points-clés

Une stratégie de sécurité basée sur les identités permet de se concentrer sur le suivi des utilisateurs qui accèdent aux données de l'entreprise plutôt que sur le suivi des points de terminaisons (appareils) eux-mêmes.

Une protection plus robuste des points de terminaison fournit des informations post-violation sur les techniques adverses.

3. Contrer les menaces grâce à un modèle de confiance zéro

17 000

détection de logiciels malveillants

C'est le chiffre qu'une grande organisation doit passer au crible chaque semaine[4].

Les pirates informatiques sont conscients que toute organisation comporte plusieurs points d'entrée. Ils utilisent l'hameçonnage par courriel, les attaques de logiciels malveillants et espions, les vulnérabilités des navigateurs et des logiciels, l'accès par des appareils perdus et volés, le piratage psychologique et d'autres tactiques pour percer votre sécurité. Une vigilance de tous les instants s'impose pour conserver un bon niveau de visibilité sur les menaces que vous connaissez déjà et pour rester au fait des nouvelles vulnérabilités.

Certains outils peuvent aider à maintenir une approche de sécurité permanente, mais une approche plus large est plus logique. Les outils classiques se concentrent sur la prévention, mais cela n'est plus suffisant. Les organisations doivent supposer qu'une violation a déjà eu lieu ou qu'elle aura bientôt lieu. Ce concept s'appelle la « confiance zéro ». Elles doivent donc trouver des moyens de réduire de manière significative le temps nécessaire à la détection de la violation et à la récupération après celle-ci.

[4] « The Cost of Malware Containment ». Ponemon Institute, janvier 2015.

Essayez cela

Devenez un expert de la sécurité avancée. Pour garder une longueur d'avance sur les menaces, il faut parfois regarder en arrière pour tirer les leçons des incidents, des activités et des mesures prises par les pirates.

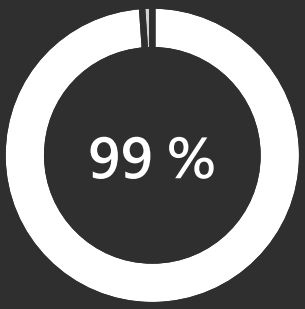
- De nombreuses applications de sécurité utilisent des capacités d'analyse et d'apprentissage automatique intégrées pour analyser la manière dont un pirate informatique a pu accéder à un système. Des solutions de sécurité et d'analyse plus avancées utiliseront ces informations pour agir automatiquement afin de prévenir et de répondre à des violations similaires, ce qui permet de réduire considérablement le délai d'atténuation.
- Elles sont bâties sur des capacités de signalement et de veille d'une étendue et d'une profondeur immenses. Combinées avec l'expérience et le savoir des experts humains, elles peuvent s'avérer redoutables dans la lutte contre des pirates toujours plus mobiles.

Points-clés

Les applications natives du nuage soutiennent un modèle de confiance zéro bien plus facilement que les applications héritées.

Ces applications doivent être modernisées pour prendre en charge l'accès conditionnel basé sur l'identité.

4. Migrer vers le nuage en toute sécurité



des défaillances de sécurité dans un environnement infonuagique seront la faute du client jusqu'en 2025[5].

Les organisations ne sont pas toutes au même stade dans leur périple vers le nuage. À cause des exigences de conformité, de la réglementation locale et d'autres difficultés de migration, toutes les organisations ne sont pas prêtes à transférer des charges de travail critiques vers le nuage. Les stratégies basées sur le nuage hybride permettent aux entreprises de transférer facilement certaines charges de travail vers le nuage, tout en en conservant d'autres sur place.

Les modèles de services infonuagiques influent sur la façon dont les fournisseurs de services et les clients partagent leurs responsabilités. Quand ils doivent renoncer à une part de leur contrôle sur les solutions sur place au bénéfice de la plus grande sécurité offerte par les fournisseurs de nuage, les responsables de la sécurité des systèmes d'information sont confrontés à de nouveaux défis.

Le principe de base de la sécurité du nuage, c'est qu'elle relève d'une responsabilité partagée. Les fournisseurs de nuage doivent disposer de conditions de chiffrement et de protection dernier cri, mais les clients doivent s'assurer que les services achetés sont effectivement sécurisés et que leurs politiques de sécurité couvrent également leurs nouvelles ressources migrées vers le nuage.

[5] « Is the Cloud Secure », Gartner, octobre 2019.

Essayez cela

Posez-vous les bonnes questions. Au moment d'évaluer les fournisseurs de nuage, vous ne choisissez pas seulement un service, mais à qui confier vos données. Les questions essentielles en matière de sécurité et du contrôle des accès que vous devriez vous poser comprennent :

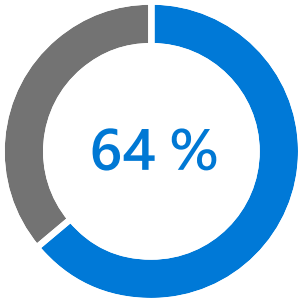
- Vos données sont-elles protégées par une sécurité renforcée et une technologie de pointe?
- Intégrez-vous le principe de la protection de la vie privée dès la phase de conception et permettez-vous le contrôle de nos données dans notre nuage d'entreprise?
- Dans quels processus de conformité robustes et innovants avez-vous investi pour vous aider à répondre à vos besoins en matière de conformité?
- Où vos données seront-elles stockées, qui pourra y accéder et pourquoi?
- Faites-vous effectuer des examens annuels par des tiers pour vous assurer que les normes de sécurité et de conformité sont respectées?
- Rejetterez-vous des demandes de divulgation des données personnelles des clients, si elles ne s'inscrivent pas dans le cadre d'une procédure juridique?
- Respectez-vous les normes réglementaires et de conformité des pays et sites dans lesquels vous opérez? Si oui, lesquelles?

Points-clés

Lors de l'évaluation des fournisseurs de services infonuagiques, assurez-vous qu'ils respectent les normes internationales.

Optez pour des fournisseurs qui publient des informations détaillées sur leurs méthodes d'exploitation des services et d'administration des données.

5. Faire la lumière sur l'informatique de l'ombre



des employés ont créé au moins un compte (en s'inscrivant sur un site Web ou une application liée au travail) sans consulter au préalable le service informatique[6].

Lorsqu'un employé crée un compte infonuagique sans l'autorisation ou la connaissance d'une entreprise, on parle alors d'informatique de l'ombre. Ces comptes peuvent paraître tout à fait inoffensifs, par exemple un outil de correction de la grammaire. Mais ces comptes créent des vulnérabilités, même dans les configurations de sécurité les plus strictes.

Les utilisateurs acceptent souvent les conditions générales des applications sans les lire, et sans bien comprendre à quoi elles autorisent l'accès. Les solutions de sécurité réseau classiques ne sont pas conçues pour protéger les données des applications SaaS et ne permettent pas au service informatique de connaître les modalités d'utilisation du nuage par les employés.

Nous ne voulons pas pour autant supprimer les motivations derrière l'informatique de l'ombre. En autorisant les utilisateurs à utiliser les applications infonuagiques les mieux adaptées à leur travail, vous stimulez l'innovation et la productivité. Pour gérer le risque et favoriser la transformation numérique qui a déjà pris pied dans votre entreprise, les premières étapes consistent à assurer la visibilité, le contrôle et la protection contre les menaces des applications SaaS de l'ombre.

[6] « New research reveals risks of shadow IT », 1password, février 2020.

Essayez cela

Obtenez les informations dont vous avez besoin. Les courtiers de sécurité de l'accès au nuage (CASB) permettent aux organisations d'obtenir une vue détaillée de l'utilisation des services infonuagiques par leurs employés :

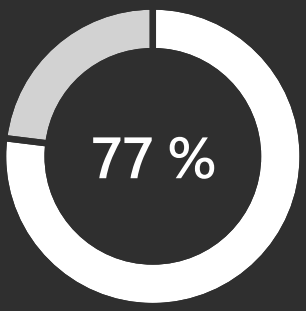
- Quelles sont les applications infonuagiques utilisées?
- Quels sont les risques que ces applications posent pour l'organisation?
- Comment accède-t-on à ces applications?
- Quelles données ces applications reçoivent-elles et permettent-elles de partager?
- Quel est le trafic de téléversement/téléchargement?
- Le comportement des utilisateurs laisse-t-il transparaître des anomalies comme l'impossibilité d'utiliser l'application ou d'ouvrir une session ou la présence d'IP suspectes?

Points-clés

Les courtiers en sécurité de l'accès au nuage (CASB) peuvent vous donner un aperçu détaillé de la façon dont les employés utilisent le nuage.

Grâce à une visibilité accrue, vous pouvez définir des politiques permettant de suivre et de contrôler l'utilisation des applications par les employés.

6. Fusionner la protection et la productivité



des RSSI disent se sentir partagés entre laisser les gens travailler librement et préserver la sécurité de l'entreprise[7].

Aujourd'hui plus que jamais, les données échappent à votre contrôle alors que vos employés, vos partenaires et vos clients les partagent. Cela stimule la productivité et l'innovation, mais peut avoir de graves conséquences si des informations très sensibles tombent entre de mauvaises mains. Les responsables de la sécurité doivent gérer et sécuriser les données stockées dans plusieurs emplacements et partagées au-delà de frontières internationales, conformément à la réglementation.

Les employés ne sauront tolérer qu'un certain niveau de désagrément avant de trouver des moyens de contourner les exigences de sécurité. La classification et le chiffrement des données sont les meilleures façons de les protéger tout en permettant l'utilisation productive et le partage de l'information. Vous pouvez éviter les erreurs humaines en automatisant la classification des données. Les outils peuvent comprendre le contexte des données, par exemple les numéros de carte de crédit dans un fichier, ou leur sensibilité en fonction de leur origine. Une fois l'étiquetage réalisé, des actions telles que le marquage visuel (en-têtes, pieds de page et filigranes) et des mesures de protection (chiffrement, authentification et droits d'utilisation) peuvent être appliquées automatiquement aux données sensibles.

[7] « IT security hindering productivity and innovation, survey shows », ComputerWeekly.com, octobre 2017.

Essayez cela

Maîtrisez les moindres détails. Les équipes de sécurité doivent avoir la possibilité de suivre l'activité des fichiers partagés hautement confidentiels ou à fort impact commercial et de révoquer les accès si nécessaire.

- Cette protection permanente voyage avec les données et les protègent en tout temps, peu importe où elles sont stockées ou avec qui elles sont partagées.
- Un système de gestion de l'accès basé sur l'identité facilite le suivi des dossiers hautement confidentiels.

Points-clés

La sécurité au niveau des données est la responsabilité de chacun.

Les données doivent être classifiées et étiquetées au moment de leur création, et les équipes de sécurité doivent pouvoir surveiller l'activité des fichiers et intervenir rapidement.

Microsoft

Conclusion

En raison de la nature multiforme des cybermenaces, se contenter de relever uniquement certains de vos défis en matière de sécurité ne suffit plus. Les besoins de sécurité de chaque entreprise sont uniques, mais les entreprises font face aux mêmes défis et partagent la même responsabilité en matière de protection de leurs données, de leurs employés et de leurs systèmes, tout en encourageant l'innovation et la croissance. Vous avez besoin de cadres de sécurité agiles qui favorisent la transformation numérique, soutenus par des stratégies de sécurité globales intégrées dans les technologies, les processus et les programmes de formation.

Si vous n'avez pas envisagé de passer au nuage, c'est le moment idéal pour explorer les capacités de sécurité accrues que vous y trouverez. Microsoft 365 offre aux entreprises de toutes tailles une solution complète et intelligente qui prend en charge votre transformation numérique grâce à des fonctionnalités de sécurité et de conformité intégrées à tous les niveaux.

Pour en savoir plus, consultez cette série de webinaires complets et gratuits.

Regarder la série >