Microsoft

6 étapes pour une stratégie holistique en matière de sécurité

Ces informations sont pour vous

si vous êtes responsable de la sécurité des informations ou responsable de la sécurité informatique, vous avez besoin de ce qui suit :

- Obtenir un guide rapide et explicatif sur la stratégie de sécurité globale.
- Rester informé sur les dernières pratiques en matière de sécurité.

Temps de lecture estimé : < 9 minutes

Table des matières

Relever le défi 4

1. Utiliser des produits de sécurité intégrés pour accélérer les réponses 5
2. Gérer l'accès via l'identité, et non les points de terminaison 7
3. Adopter un modèle de confiance zéro pour vaincre les menaces 9
4. Migrer vers le Cloud en toute sécurité 11
5. Examiner de près les pratiques informatiques non conventionnelles 13
6. Assurer la protection et la productivité en toute simplicité 15

Conclusion 17

Relever le défi

La sécurisation des données et des systèmes est une priorité absolue pour les organisations. Mais relever ce défi devient plus difficile chaque jour, à mesure que les attaques gagnent en sophistication, que les employés utilisent un éventail toujours plus vaste d'appareils et d'applications, et que les voies d'entrée et de sortie des flux de données se diversifient au sein de votre organisation. Avec le recours massif au télétravail, la sécurité devient encore plus compromise.

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 directeurs de la sécurité (DSI) d'aujourd'hui ont besoin de cadres de sécurité agiles pour mettre en place la transformation numérique, soutenus par des stratégies globales intégrées dans les technologies, les processus et les programmes de formation. Bien que tout cela soit disponible pour les solutions sur site, en réalité une migration vers le Cloud améliore immédiatement les fonctionnalités de sécurité au sein de votre organisation.

Cet Ebook présente les 6 meilleures pratiques des RSSI qui ont fait de la sécurité la base fondamentale du succès des entreprises. Ces bonnes pratiques s'appliquent à un scénario sur site, mais sont infiniment plus faciles à réaliser dans un scénario Cloud.

1. Utiliser des produits de sécurité intégrés pour accélérer les réponses

75

Nombre de produits de sécurité utilisés en moyenne par de grandes entreprises.[1]

Le mode opératoire des cyberattaquants a changé. Ils ne se contentent plus d'entrer dans les systèmes, mais les compromettent dans l'espoir de maintenir une présence persistante et à long terme. Les cyberattaquants utilisent désormais de nouveaux vecteurs d'attaque et un large éventail de techniques et d'outils avancés : vol d'identifiants, installation de logiciels malveillants qui s'effacent d'eux-mêmes pour éviter d'être repérés, modification de processus internes et réacheminement des données réseau, piratage psychologique et ciblage des téléphones mobiles et des appareils domestiques des collaborateurs.

Les organisations déploient de plus en plus d'outils de sécurité contre ces menaces. 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. En raison de la difficulté de l'intégration, il est ardu d'avoir une vue globale et d'établir un ordre de priorité des menaces rapidement. Le défi est encore plus important si des ressources sont conservées à la fois dans le Cloud et 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, octobre 2015.

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

Essayez ce qui suit

Alors que la détection et l'intervention rapides deviennent plus importantes, ces pratiques exemplaires ont été identifiées :

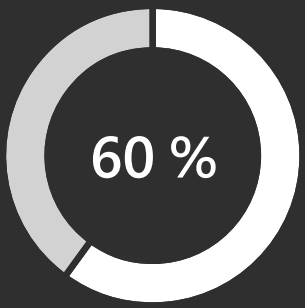
- Bénéficiez d'une vue globale de la sécurité sur l'ensemble de votre réseau, y compris le Cloud et les environnements hybrides.
- Créez un écosystème de plateformes et de produits de sécurité conçus pour s'intégrer les uns avec les autres et fournir des informations.
- Travaillez en partenariat avec des fournisseurs de technologies qui collaborent et partagent des informations dans tout le secteur de la sécurité.

Points importants

En raison du manque d'intégration parmi les produits de sécurité, il est compliqué pour les équipes de sécurité de détecter et de résoudre rapidement des menaces de manière holistique.

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

2. Gérer l'accès via l'identité, et non les points de terminaison



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

Une violation de données peut occasionner des coûts considérables. La mise en place de contrôles de sécurité suffisants pour attirer la visibilité sur les menaces et les attaques est l'un des moyens de lutter contre le coût élevé. Mais les équipes de sécurité doivent également prendre en charge la « consumérisation » de l'IT, 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.

Actuellement, les stratégies de sécurité axées sur les identités lient l'accès à l'identité, pas aux appareils. Il faut appliquer des contrôles en fonction du rôle et des besoins, quelle que soit la façon dont l'utilisateur se connecte. En se concentrant sur l'authentification et la gestion appropriées des utilisateurs qui tentent d'accéder aux ressources de l'entreprise, les entreprises peuvent protéger leurs données, indépendamment de l'endroit où elles sont stockées, de la manière dont on y accède ou avec qui elles sont partagées.

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

Essayez ce qui suit

Le fait de délaisser une stratégie de sécurité uniquement axée sur les points de terminaison vous donne une approche plus robuste. Ces outils peuvent aider à constituer ce qui suit :

- **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 Cloud. Une solution IAM permet d'éviter la multiplication d'informations d'identification en donnant aux collaborateurs une identité unique pour accéder aux ressources Cloud et sur site. Les systèmes IAM basés sur le Cloud peuvent également profiter des renseignements sur les menaces et de l'analyse du fournisseur de technologies afin de mieux détecter les tentatives d'accès anormales et réagir automatiquement de façon appropriée.
- **Une authentification multifacteur (MFA)** propose une autre couche de protection, qui nécessite que l'utilisateur utilise un élément qu'il connaît (son mot de passe) et un élément qu'il possède (une authentification secondaire via son appareil, son empreinte digitale ou la reconnaissance faciale). D'autres tactiques rigoureuses comprennent le fait de baser l'accès sur les 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 d'entrée.

Points importants

Une stratégie de sécurité basée sur les identités ne s'occupe plus uniquement de suivre un nombre croissant de points de terminaison (appareils), mais aussi de gérer les utilisateurs ayant accès aux données d'entreprise.

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

3. Adopter un modèle de confiance zéro pour vaincre les menaces

17 000

alertes de logiciels malveillants

En moyenne, une grande entreprise doit passer cela au crible chaque semaine.[4]

Les pirates savent que chaque organisation possède 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 déjouer votre sécurité. Une vigilance de tous les instants s'impose pour conserver un bon niveau de visibilité sur les menaces que vous connaissez, 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 partir du principe qu'une violation s'est déjà produite ou se produira bientôt. C'est ce que l'on appelle la confiance zéro. Ils doivent ensuite trouver des moyens de réduire considérablement le temps nécessaire pour la détecter et récupérer à la suite de celle-ci.

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

Essayez ce qui suit

Devenez un expert de la sécurité avancée. Rester en avance sur les menaces peut signifier regarder en arrière : tirer des leçons des incidents, des activités et des étapes empruntées par les pirates.

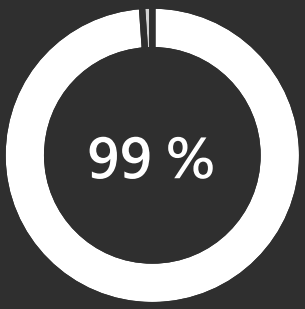
- De nombreuses applications de sécurité ont des fonctionnalités d'analyse et d'apprentissage automatique intégrées pour analyser la façon dont un pirate s'est infiltré. Davantage de solutions de sécurité et d'analyse avancées vont utiliser les connaissances sur ces menaces et agir automatiquement afin de prévenir les violations similaires et d'intervenir au besoin, ce qui réduit fortement le délai d'atténuation.
- Une prodigieuse variété de signaux et de renseignements sont à l'origine de ces solutions, et lorsqu'elles sont combinées avec l'expérience et le savoir des spécialistes, elles peuvent constituer des outils puissants contre les cyberattaquants qui prolifèrent rapidement.

Points importants

Les applications natives du Cloud prennent en charge un modèle de confiance zéro plus facilement que les applications héritées.

Les applications héritées nécessitent une modernisation pour prendre en charge l'accès conditionnel basé sur les identités.

4. Migrer vers le Cloud en toute sécurité



des défaillances de sécurité dans le Cloud seront de la faute du client d'ici 2025. [5]

Chaque organisation se trouve à une étape différente de son parcours vers le Cloud. Face aux exigences de conformité, aux réglementations locales et à d'autres questions liées à la migration, toutes les entreprises ne sont pas prêtes à déplacer leur activité vers le Cloud. Les stratégies de Cloud hybride constituent pour les organisations une manière de s'intégrer facilement dans le Cloud, en gardant des charges de travail sur site et en déplaçant d'autres.

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

Le principe de base de la sécurité dans le Cloud, c'est qu'elle relève d'une responsabilité partagée. Les fournisseurs de Cloud 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 Cloud.

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

Essayez ce qui suit

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

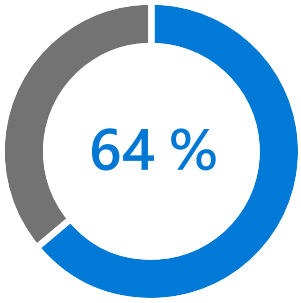
- Vos données sont-elles protégées par un dispositif de sécurité renforcé et une technologie de pointe ?
- Intégrez-vous la confidentialité au niveau de la conception et autorisez-vous le contrôle de nos données dans votre Cloud d'entreprise ?
- Quels sont les investissements importants que vous avez apportés dans des processus de conformité robustes et innovants afin de répondre aux besoins en matière de conformité ?
- Où seront stockées vos données, qui pourra y accéder et pourquoi ?
- Effectuez-vous des évaluations annuelles tierces pour vous assurer que les normes de sécurité et de conformité sont respectées ?
- Allez-vous rejeter toute demande de divulgation des données personnelles des clients qui ne sont pas juridiquement contraignantes ?
- Respectez-vous les normes de sécurité et de conformité des différents pays et localités et, si c'est le cas, lesquelles ?

Points importants

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

Recherchez des fournisseurs qui publient des informations détaillées sur la façon dont ils gèrent leurs services et les données.

5. Examiner de près les pratiques informatiques non conventionnelles



des collaborateurs ont créé au moins un compte (en s'inscrivant sur un site Web ou une application en relation avec le travail) sans impliquer le service IT.[6]

Lorsqu'un collaborateur crée un compte basé sur le Cloud sans que l'entreprise soit au courant ou l'y autorise, on appelle cela une pratique informatique non conventionnelle. Les comptes semblent tout à fait inoffensifs : un outil pour corriger la grammaire, par exemple. 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 comprendre complètement à qui ils donnent accès. Les solutions de sécurité réseau classiques ne sont pas conçues pour protéger les données dans les applications SaaS. Elles ne permettent pas non plus au département informatique de déterminer comment vos collaborateurs se servent du Cloud.

Au final, nous ne voulons pas supprimer les motivations qui sous tendent la pratique informatique non conventionnelle. Cette pratique favorise l'innovation et la productivité, car elle permet aux utilisateurs et aux équipes d'utiliser les applications Cloud les plus adaptées à leur activité. Voici les principes à suivre pour gérer les risques et faciliter la transformation numérique que votre société a déjà amorcée : gagner en visibilité, améliorer le contrôle et assurer la protection contre les menaces associées aux applications SaaS.

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

Essayez ce qui suit

Obtenez les informations dont vous avez besoin. Les Cloud Access Security Brokers (CASB) permettent aux entreprises d'avoir une vision détaillée sur la façon dont leurs collaborateurs utilisent le cloud :

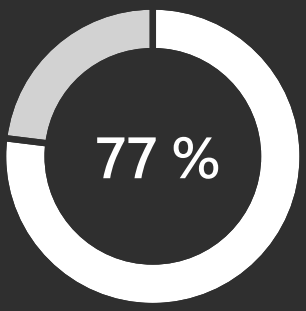
- Quelles sont les applications Cloud utilisées par les collaborateurs ?
- Quels sont les risques de ces applications pour l'organisation ?
- Comment accéder à ces applications ?
- Quels types de données sont envoyés et partagés à partir de ces applications ?
- Comment se présente le trafic de chargement/téléchargement ?
- Le comportement de l'utilisateur révèle-t-il des anomalies, par exemple un déplacement impossible, des échecs de connexion ou des adresses IP suspectes ?

Points importants

Les Cloud Access Security Brokers (CASB) peut vous donner une vision détaillée sur la façon dont leurs collaborateurs utilisent le Cloud.

Grâce à une meilleure visibilité, vous pouvez ensuite définir des stratégies qui suivent et contrôlent la façon dont les collaborateurs utilisent ces applications.

6. Assurer la protection et la productivité en toute simplicité



des RSSI disent qu'ils sont partagés entre laisser les gens travailler librement et assurer 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 aux réglementations.

Les employés ne toléreront 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 des informations. Vous pouvez éviter les erreurs humaines en automatisant la classification des données. Les outils peuvent interpréter le contexte des données, par exemple en identifiant des numéros de carte bancaire dans un fichier, ou le caractère sensible des données en fonction de leur provenance. Une fois étiquetées, les actions comme les en-têtes, pieds de page et filigranes, et la protection comme le chiffrement, l'authentification et les droits d'utilisation, peuvent être appliquées automatiquement aux données sensibles.

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

Essayez ce qui suit

Familiarisez-vous les détails. Les équipes de sécurité devraient être en mesure de suivre l'activité sur des fichiers partagés, hautement confidentiels ou des fichiers de données ayant un fort impact commercial, et de révoquer l'accès, le cas échéant.

- Cette protection en continu se déplace avec les données et les protège à tout moment, quel que soit l'endroit où elles sont stockées ou avec qui elles sont partagées.
- Un système de gestion des accès et des identités facilite la tâche de suivi des fichiers hautement confidentiels.

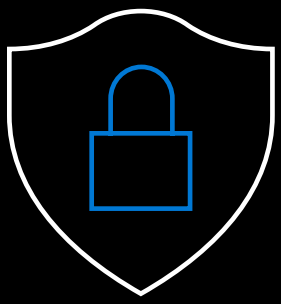
Points importants

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

La classification et l'étiquetage des données doivent avoir lieu au moment de la création. Les équipes de sécurité doivent être en mesure de surveiller les activités sur les fichiers et de réagir rapidement.

Microsoft

Conclusion



En raison de la nature multiforme des cybermenaces, vous ne pouvez plus vous contenter de relever uniquement certains de vos défis en matière de sécurité. 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 prennent en charge 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 migrer vers le Cloud, c'est le moment idéal pour explorer les fonctionnalités de sécurité accrues qui s'y trouvent. Microsoft 365 offre aux entreprises de toutes tailles une solution complète et intelligente qui prend en charge la transformation numérique grâce à des fonctionnalités de sécurité et de conformité intégrées à tous les niveaux.

En savoir plus sur cette série de webcasts complète et gratuite.

Regarder la série >