DELL Technologies

Utilisateur interne malveillant : renforcer la cybersécurité et la résilience avec Dell Technologies

La menace grandissante des attaques internes malveillantes

Les attaques internes malveillantes sont devenues l'une des menaces les plus préoccupantes en matière de cybersécurité dans le monde de l'entreprise actuel. Contrairement aux menaces externes, les utilisateurs internes malveillants disposent déjà d'un certain niveau de confiance et d'accès au sein d'une organisation, ce qui rend leurs actions particulièrement dommageables et plus difficiles à détecter. Qu'il s'agisse d'un accès à des données sensibles ou de sabotages de systèmes, les attaques internes peuvent paralyser les opérations stratégiques et avoir de graves répercussions sur les finances et la réputation d'une société.

Conscient du danger croissant que représentent ces attaques, Dell Technologies développe des solutions innovantes et évolutives pour permettre aux entreprises d'identifier, de prévenir et d'atténuer les risques occasionnés par des utilisateurs internes malveillants. En associant une technologie de pointe à des services assurés par des experts, Dell aide les organisations à garder une longueur d'avance sur ces menaces internes.

En quoi consistent les attaques internes malveillantes ?

Une attaque interne malveillante se produit lorsqu'un individu au sein d'une organisation utilise ses droits d'accès de manière frauduleuse afin de compromettre des données, de perturber des opérations ou d'obtenir des informations sensibles à des fins personnelles, financières ou concurrentielles. Il peut s'agir d'un employé, d'un prestataire, d'un partenaire ou de toute personne disposant d'un accès autorisé aux systèmes et réseaux de la société.

Fonctionnement des attaques internes malveillantes

Des utilisateurs internes malveillants profitent de leur position de confiance pour contourner les mécanismes de défense traditionnels en matière de sécurité. Voici quelques-unes des techniques qu'ils utilisent couramment :

1. **Vol de données :** exfiltration de données confidentielles sur les clients, d'informations de propriété intellectuelle ou de documents financiers.
2. **Sabotage :** dommages causés de manière intentionnelle aux systèmes IT dans le but de perturber les opérations commerciales ou de ternir la réputation.
3. **Utilisation frauduleuse d'informations d'identification :** recours à des informations d'identification volées ou utilisées à mauvais escient pour augmenter les privilèges d'accès ou créer des comptes factices.
4. **Collaboration avec des cyberattaquants externes :** partage d'accès ou d'informations sensibles avec des cybercriminels externes en échange d'un gain financier.

Ce double avantage (confiance et connaissances internes) rend les utilisateurs internes malveillants particulièrement dangereux comparés aux cyberattaquants externes.

Les répercussions sur les entreprises

Les attaques internes malveillantes ont des répercussions majeures et occasionnent des dommages qui vont bien au-delà des pertes financières. Les entreprises peuvent se trouver confrontées aux conséquences suivantes :

Perte financière

Le vol d'informations sensibles, la fraude ou le sabotage entraînent des pertes de revenus et des frais de récupération pouvant se chiffrer à plusieurs millions de dollars.

Interruption des opérations

Le sabotage des systèmes ou la destruction des données peut interrompre les opérations, avec pour résultat des retards, des opportunités manquées et une baisse de productivité.

Atteinte à la réputation

Une violation ou une attaque par des utilisateurs internes érode la confiance des clients et des parties prenantes, avec des répercussions sur la fidélité des clients et la perception du marché.

Non-respect des obligations réglementaires

En fonction du secteur, les attaques internes peuvent donner lieu à de lourdes amendes et pénalités si elles concernent des informations sensibles telles que les données médicales ou financières.

Exemple concret

En 2020, un prestataire IT travaillant pour une grande institution financière a supprimé intentionnellement des configurations système importantes, provoquant des pannes réseau de plus de **10 heures**. Cet acte de sabotage a entraîné des pertes financières à hauteur de **plusieurs millions** de dollars, des coûts de récupération considérables et une atteinte à la réputation. De tels incidents illustrent la capacité de nuisance des menaces internes et soulignent l'urgence de mettre en place de solides mesures de détection et de prévention.

Coût estimé

D'après une étude réalisée en 2024 par le Ponemon Institute, le coût moyen d'un incident impliquant un utilisateur interne est estimé à **4,99 millions de dollars**, et ce type d'incident représente près de **55 %** des violations de sécurité. Ce chiffre tient compte des dépenses liées à la détection, à la récupération et à l'atténuation des risques. Cela illustre la nécessité pour les organisations d'investir dans des stratégies de défense préventive contre les risques venant de l'intérieur.

83 %

des organisations ont signalé au moins une attaque interne au cours de l'année écoulée

Source : rapport 2024 de Cybersecurity Insiders

Lutter contre les attaques internes malveillantes avec Dell Technologies

Dell Technologies propose un écosystème complet d'outils et de services pour lutter contre les menaces internes malveillantes, permettant à votre entreprise de se prémunir contre l'imprévu.

Sécuriser les points de terminaison avec Dell Trusted Devices

Les points de terminaison servent souvent de points d'entrée aux menaces internes. Dell Trusted Devices intègre des fonctions de sécurité de pointe au matériel pour renforcer les points de terminaison et protéger les données sensibles.

- **Dell SafeBIOS** garantit l'intégrité du firmware et évite les tentatives de manipulation des opérations système au niveau du matériel.
- **SafeID** protège les données d'identification, empêchant tout accès non autorisé et toute utilisation frauduleuse des informations d'identification.
- **SafeData** chiffre les données sensibles de bout en bout, garantissant que les informations interceptées ou extraites restent illisibles pour les utilisateurs internes malveillants.

En déployant ces solutions, les organisations peuvent s'assurer que leurs points de terminaison sont protégés, que la menace vienne de l'intérieur ou de l'extérieur.

Détection proactive des menaces avec CrowdStrike

L'identification des menaces internes requiert de la visibilité et une surveillance du comportement des utilisateurs. CrowdStrike, intégré aux solutions Dell, utilise l'intelligence artificielle et l'analytique comportementale pour détecter les anomalies pouvant être le signe de menaces internes.

Par exemple, les transferts de données anormaux en dehors des heures de bureau ou l'accès non autorisé à des zones stratégiques du réseau sont signalés immédiatement, ce qui permet d'apporter une réponse rapide. Un organisme de santé américain a récemment utilisé la détection proactive des menaces pour identifier et mettre un terme à la tentative d'exfiltration des données patients par un employé, empêchant ainsi une violation aux lourdes conséquences financières.

Protection des données améliorée avec Dell PowerProtect

Dell PowerProtect fournit une ligne de défense solide grâce à des sauvegardes sécurisées, à un stockage air-gapped et à des copies immuables des données stratégiques. En protégeant les informations sensibles contre toute altération ou suppression, les entreprises peuvent rendre inefficaces les attaques internes ciblant l'intégrité des données.

Une entreprise de fabrication a par exemple été confrontée à la situation suivante : un employé mécontent a essayé de saboter des fichiers de conception. Le coffre-fort de récupération de Dell PowerProtect a permis à la société de restaurer ses opérations en quelques heures, évitant ainsi les interruptions et assurant la continuité des activités.

Reprise rapide après incident avec Dell Professional Services

Lorsqu'une menace interne se transforme en incident, il est essentiel de pouvoir effectuer une récupération rapide. Grâce à Dell Professional Services, dont font partie les services de récupération des données à distance et de réponse aux incidents, les entreprises peuvent récupérer leurs données et rétablir leurs systèmes rapidement. Les experts Dell pilotent le processus afin de réduire au minimum les interruptions de service et de limiter les répercussions.

Ce ne sont là que quelques exemples de solutions Dell qui peuvent vous aider à contrer les menaces internes malveillantes.

Sécurité réseau avancée et microsegmentation avec Dell PowerSwitch Networking et SmartFabric OS

Protège contre les attaques « Zero-Day » en fournissant une segmentation avancée du réseau, des contrôles d'accès stricts et une analyse du trafic en temps réel sur l'ensemble de votre infrastructure.

L'importance d'une approche de sécurité multicouche

Une défense efficace contre les risques venant de l'intérieur nécessite plusieurs couches de protection. La mise en œuvre d'une stratégie de sécurité multicouche garantit qu'aucune vulnérabilité ne se transforme en point faible. Voici les étapes clés :

Étapes clés pour améliorer la défense

- **Principes Zero-Trust :** vérifiez en permanence toutes les demandes d'accès et partez du principe qu'aucune entité n'est intrinsèquement fiable, même à l'intérieur du périmètre.
- **Contrôles d'accès basés sur les rôles (RBAC) :** limitez l'accès des employés aux seuls systèmes et données requis en fonction de leur rôle.
- **Solutions de chiffrement avancées :** chiffrez les données au repos et en transit pour empêcher efficacement les vols de données.
- **Formation et sensibilisation des employés :** intégrez des programmes réguliers de sensibilisation à la sécurité pour prévenir toute implication accidentelle dans des activités malveillantes.
- **Tests réguliers des systèmes :** effectuez des tests d'intrusion et des analyses des failles de sécurité pour vous assurer que les moyens de défense restent fiables.

Ces pratiques, soutenues par les solutions Dell, créent un remarquable cadre de protection global contre les utilisateurs internes malveillants.

Renforcer la défense par le biais de partenariats stratégiques

Afin de renforcer ses produits, Dell collabore avec des fournisseurs de solutions de cybersécurité leaders sur le marché, tels que **CrowdStrike** et **Secureworks**. CrowdStrike améliore la sécurité des points de terminaison et fournit une précieuse cyber-intelligence concernant les indicateurs de compromission, tandis que Secureworks offre des services de détection et de réponse aux menaces avancées. Ces partenariats permettent aux clients de Dell de bénéficier d'un écosystème de technologies intégrées de pointe.

Pourquoi choisir Dell Technologies pour la cybersécurité

Dell Technologies reste la référence incontournable en matière de solutions de cybersécurité multicouche. Les entreprises clientes profitent de l'expertise de pointe de Dell, de solides partenariats et d'une suite de produits innovants qui s'adaptent à l'évolution du paysage actuel des menaces. De la sécurisation des points de terminaison à la détection des utilisateurs internes malveillants en passant par la reprise après incident, Dell fournit un cadre de résilience complet qui inspire confiance et favorise la croissance.

Bâtir un avenir reposant sur la résilience avec Dell Technologies

Protégez votre entreprise contre les menaces internes malveillantes avec les solutions complètes et évolutives de Dell Technologies. En faisant appel à Dell, non seulement vous sécurisez vos opérations, mais vous garantissez également la continuité de vos activités, vous renforcez la confiance des clients et vous assurez la pérennité de votre entreprise. Contactez-nous pour savoir comment mettre en œuvre dès aujourd'hui des mesures de défense proactive.

Dell Technologies est votre allié de confiance pour lutter contre les menaces internes, protéger vos ressources stratégiques et permettre à votre entreprise de prospérer dans un environnement numérique dynamique. L'avenir de la sécurité est un avenir placé sous le signe de la réussite, et cela commence avec Dell.

Découvrez comment relever certains des défis actuels majeurs en matière de cybersécurité sur **Dell.com/SecuritySolutions**

En savoir plus sur les solutions Dell

Contacter un expert Dell Technologies

Afficher plus de ressources

Prenez part à la discussion avec #hashtag

DELL Technologies