DELL Technologies

Infiltration des sauvegardes : renforcer la cybersécurité et la résilience avec Dell Technologies

Synthèse

L'infiltration des sauvegardes constitue une menace croissante pour les entreprises de tous les secteurs, car elle exploite les vulnérabilités des systèmes qui servent précisément à protéger les informations critiques. Ces attaques compromettent les systèmes de récupération des données, ébranlent la confiance et mettent en péril les opérations. Importantes pertes financières, temps d'arrêt prolongés et réputation ternie sont autant de conséquences qui ne pardonnent pas.

Dell Technologies fournit une suite de défenses complète qui protège les données sensibles et prévient ces attaques, notamment via Dell Trusted Device, Dell Trusted Infrastructure et des fonctions de sécurité étendues intégrées à toutes nos solutions. En les complétant avec des partenariats stratégiques et des services professionnels, Dell aide les entreprises à mettre en place des cadres de sécurité résilients à plusieurs niveaux capables de détecter et déjouer efficacement les incidents d'infiltration des sauvegardes, mais aussi de s'en remettre.

En mettant en œuvre les solutions innovantes de Dell et son support assuré par des experts, les entreprises seront mieux préparées à sécuriser leur infrastructure et à maintenir leurs opérations.

L'infiltration des sauvegardes : un risque de plus en plus menaçant

Les systèmes de sauvegarde jouent un rôle déterminant dans la continuité des activités et dans la récupération après un cyberévénement, comme un ransomware ou une panne matérielle. Malheureusement, ces bouées de sauvetage sont de plus en plus souvent la cible des cybercriminels. L'infiltration des sauvegardes corrompt ou supprime les données de sauvegarde, les rendant inaccessibles au moment où elles sont les plus nécessaires.

Ces menaces en constante évolution appellent des mesures proactives. Toute incapacité à protéger les systèmes de sauvegarde compromet les opérations et expose les données sensibles. Les entreprises de toutes tailles, des petites entreprises aux multinationales, ont une cible dans le dos, notamment dans les secteurs de la santé, de la finance et de la fabrication industrielle.

Dell Technologies reconnaît la nécessité absolue de renforcer les environnements de sauvegarde en proposant des outils et des conseils avancés pour contrer ces attaques sophistiquées.

Attaques d'infiltration des sauvegardes

L'infiltration des sauvegardes se produit lorsque les cybercriminels exploitent les vulnérabilités des systèmes de sauvegarde afin de compromettre, détruire ou chiffrer des données de récupération critiques. Ces attaques complexes peuvent coïncider avec d'autres incidents ou en être la conséquence, par exemple le déploiement d'un ransomware ou d'un malware, amplifiant les retombées opérationnelles et financières.

Fonctionnement des attaques ciblant les sauvegardes

1. **Violation initiale :** les pirates parviennent à accéder au réseau sans autorisation, souvent grâce au hameçonnage, à des identifiants peu sécurisés ou à des vulnérabilités non corrigées.
2. **Mouvement latéral :** une fois à l'intérieur du réseau, les pirates utilisent des outils pour s'y déplacer sans être détectés, en ciblant les référentiels de sauvegarde et les jeux de données critiques.
3. **Compromission des sauvegardes :** le chiffrement des fichiers de sauvegarde, la suppression des points de récupération et la corruption des données sont autant de tactiques clés utilisées par les pirates.

Techniques courantes

- **Le vol d'informations d'identification** leur donne accès aux comptes administratifs et, à terme, aux systèmes de sauvegarde.
- **Le déploiement de ransomwares** chiffre à la fois les données en direct et les sauvegardes, qui ne sont déchiffrées qu'après paiement d'une rançon.
- **La corruption planifiée** compromet progressivement les sauvegardes pour rester discret et expose les entreprises lorsqu'une récupération est nécessaire.

Ces techniques mettent en évidence la sophistication et la gravité de ces menaces et exigent des mesures préventives.

Impact sur les entreprises

Pertes financières

L'infiltration des sauvegardes augmente les coûts de récupération et les interruptions de service, doublant ou triplant souvent les frais d'intervention. Pour remettre la main sur des sauvegardes chiffrées ou compromises, l'entreprise doit parfois payer une rançon à des pirates, investir dans une nouvelle infrastructure ou faire appel à des consultants coûteux.

Interruption opérationnelle

En l'absence de sauvegardes viables, les entreprises sont confrontées à de longs délais de reprise qui perturbent les services, retardent les projets et interrompent les fonctions critiques.

Conséquences sur la réputation

La perte permanente de données et les interruptions de service prolongées érodent la confiance des parties prenantes, ce qui peut nuire à la viabilité à long terme d'une entreprise.

Exemple concret

Un prestataire de santé mondial a découvert que ses sauvegardes avaient été corrompues lors d'une attaque par ransomware. Bien qu'il ait payé la rançon, les données des patients sur trois semaines ont été définitivement perdues, retardant les interventions chirurgicales et entraînant des poursuites judiciaires. Le coût total de la récupération s'est élevé à plus de **50 millions de dollars.**

Des statistiques alarmantes

Des études récentes estiment que le coût moyen d'un système de sauvegarde compromis dépasse les **4,45 millions de dollars**[1], en incluant les amendes, les interruptions de service et les frais de récupération. L'augmentation du nombre de ces incidents est particulièrement alarmante. En effet, les rapports mondiaux signalent une augmentation de **39 %** des menaces liées aux sauvegardes par rapport à l'année précédente.

57 %
des attaques ciblant les sauvegardes parviennent à infiltrer les référentiels de secours

Source : 2024 : Index Engines

Lutter contre les infiltrations de sauvegardes avec Dell Technologies

Dell Technologies fournit une suite robuste d'outils et de services qui répondent aux défis uniques posés par les attaques d'infiltration des sauvegardes, permettant aux entreprises de prévenir, de détecter et de reprendre leur activité efficacement.

Solutions de serveurs et de stockage sécurisées

Les solutions de serveurs et de stockage Dell offrent une résilience inégalée face aux attaques ciblant les sauvegardes. Leurs fonctions intégrées assurent la sécurité des sauvegardes et des snapshots.

- **Les sauvegardes/snapshots immuables** créent des points de restauration inviolables.
- **La récupération isolée** met les données des réseaux actifs en quarantaine pour éviter leur corruption.

[1] Ponemon, Cost of a Data Breach Report 2024

Renforcez les appliances de protection des données Dell

Les appliances de protection des données Dell intègrent des fonctions telles que Dell SafeBIOS pour l'intégrité du firmware et SafeData pour un chiffrement sécurisé afin de vous protéger contre les attaques ciblant les sauvegardes. De plus, ces solutions offrent des fonctionnalités telles que l'authentification multifacteur (MFA), les contrôles d'accès basés sur les rôles et la double authentification pour empêcher les pirates d'accéder au réseau.

Détection avancée des menaces avec CrowdStrike

L'intégration entre CrowdStrike et la protection des données Dell se concentre sur l'amélioration de la sécurité et de la surveillance des environnements de protection des données grâce à un ensemble de capacités avancées.

1. **Points de terminaison et protection des données :** Dell intègre la sécurité des points de terminaison et la détection et la réponse étendues (EDR/XDR) de CrowdStrike à ses solutions de protection des données. Cela inclut la collecte des données de télémétrie à partir de PowerProtect Data Manager et PowerProtect Data Domain de Dell, ainsi que des informations de sécurité provenant de la console CrowdStrike Falcon et du logiciel SIEM de nouvelle génération
2. **Surveillance et réponse :** le service Managed Detection and Response (MDR) de Dell gère le logiciel CrowdStrike pour le compte des clients, collecte les journaux et enquête sur tout indicateur de compromission (IoC) ou toute anomalie détectée. Cette intégration permet à Dell d'assurer une surveillance continue et de collaborer avec le SOC du client afin de garantir une correction rapide et efficace des menaces
3. **Visibilité en temps réel et contrôle des mouvements de données :** la plateforme de protection des données CrowdStrike Falcon offre une visibilité en temps réel sur les mouvements de données entre différentes sources et différents canaux, en classant les données par contenu et par contexte. Cela permet de prévenir le vol de données et de garantir l'application efficace des politiques de protection des données en combinant le contenu et l'analyse contextuelle
4. **Gestion unifiée et déploiement simplifié :** l'intégration permet à une seule plateforme et à un seul agent de gérer la protection des données et des points de terminaison, réduisant ainsi la complexité et les coûts opérationnels. L'approche Cloud et légère de la plateforme CrowdStrike Falcon facilite ce processus, pour un déploiement rapide et une interruption minimale

L'intégration entre CrowdStrike et la protection des données Dell tire parti des fonctionnalités EDR/XDR avancées, de la surveillance en temps réel et de la gestion complète des données pour améliorer la sécurité et la résilience globales des environnements de protection des données.

Une institution financière de premier plan a récemment déployé PowerProtect Cyber Recovery, empêchant les pirates d'accéder à 90 % des sauvegardes critiques lors d'une violation de sécurité, ce qui lui a permis de se remettre tranquillement sans rançon à payer.

Solutions Dell PowerProtect pour l'intégrité des sauvegardes

Dell PowerProtect offre une protection de sauvegarde complète, en tirant parti de l'immuabilité, de la mise en quarantaine et de la compression pour éviter toute compromission du système de sauvegarde. En s'intégrant aux outils de détection des ransomwares, PowerProtect fait en sorte que les modifications suspectes déclenchent des alertes qui entraînent une action immédiate.

L'approche de la sécurité sur plusieurs niveaux

Pour protéger les données, il faut adopter des stratégies de sécurité coordonnées et aux multiples facettes. Dell aide les entreprises à mettre en œuvre les meilleures pratiques du secteur pour créer un environnement de sauvegarde résilient.

Étapes clés pour améliorer ses défenses

- **Adoptez des principes Zero-Trust :** validez en permanence tous les utilisateurs, appareils et processus pour réduire le risque d'accès non autorisé.
- **Chiffrez toutes les sauvegardes :** assurez-vous que les données restent illisibles si elles sont compromises, en transit comme au repos.
- **Formez les collaborateurs :** apprenez aux employés à reconnaître les tentatives d'hameçonnage et les autres tactiques d'ingénierie sociale qui conduisent à des violations.
- **Effectuez des tests de vulnérabilité réguliers :** des tests fréquents aident les entreprises à identifier et corriger les points faibles avant que les pirates ne les exploitent.

Dell associe ces pratiques à des solutions de pointe, créant ainsi une infrastructure robuste et réactive prête à relever de nouveaux défis.

Des partenariats stratégiques qui renforcent la sécurité

Dell collabore avec des leaders de la cybersécurité tels que Microsoft, CrowdStrike et Secureworks. Chaque partenariat enrichit les solutions Dell, offrant aux clients des capacités de protection inégalées : renseignements avancés sur les menaces, surveillance des points de terminaison et stratégies d'intervention complètes.

Tirer parti de Dell Professional Services

Les services professionnels de Dell Technologies proposent une expertise et des conseils qui aident les entreprises à relever efficacement les défis complexes de cybersécurité qu'elles rencontrent. De la création de plans de réponse aux incidents à la mise en œuvre d'architectures Zero-Trust, les spécialistes Dell veillent à ce que les environnements clients restent résilients face aux menaces modernes telles que l'infiltration des sauvegardes.

Renforcer la résilience métier avec Dell

En se tournant vers Dell Technologies, les entreprises sont en mesure de déjouer les pirates sophistiqués tout en maintenant la continuité opérationnelle. Grâce à l'innovation, aux partenariats et à son expertise, Dell s'assure que les entreprises peuvent prévenir, détecter et se remettre des attaques d'infiltration de sauvegardes les plus graves.

Passez à l'étape suivante

Contactez Dell Technologies dès aujourd'hui pour sécuriser votre entreprise. Ensemble, nous protégerons vos ressources stratégiques, votre réputation et votre avenir.

Dell s'engage à renforcer la confiance à l'ère numérique, en mettant entre les mains des entreprises les outils, les connaissances et l'assistance dont elles ont besoin pour fonctionner et prospérer en toute sécurité.

La résilience des sauvegardes commence avec Dell Technologies. Agissez dès maintenant pour pérenniser vos opérations et gagner en confiance dans votre posture de cybersécurité.

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

En savoir plus sur Solutions Dell

Contacter un expert Dell Technologies

Consulter d'autres ressources

Prenez part à la discussion avec #hashtag

DELL Technologies