DELL Technologies

Zero-day : renforcer la cybersécurité et la résilience avec Dell Technologies

La menace grandissante des attaques Zero-day

Les attaques Zero-day sont rapidement devenues l'une des plus redoutables difficultés dans l'environnement de cybersécurité actuel. Ces attaques exploitent des vulnérabilités inconnues des fournisseurs de logiciels et des experts en sécurité, laissant les entreprises mal préparées et exposées. Les entreprises de tous les secteurs, de la santé à la finance, sont vulnérables à ces violations, qui entraînent souvent de graves conséquences financières et opérationnelles.

La transformation numérique s'accélère et les attaques Zero-day sont devenues plus fréquentes et sophistiquées. Jamais le besoin de protections robustes n'a été aussi important. Dell Technologies comprend la nature critique de cette menace et fournit aux entreprises des défenses innovantes et évolutives pour lutter efficacement contre les attaques Zero-day et s'en remettre.

Que sont les attaques Zero-day ?

Une attaque Zero-day consiste à exploiter une vulnérabilité de sécurité non détectée dans un logiciel ou un matériel avant qu'un correctif ou une solution ne soit disponible. Les attaquants profitent de la fenêtre d'opportunité, provoquant souvent des perturbations généralisées avant que la vulnérabilité ne soit découverte et corrigée.

Fonctionnement des attaques Zero-day

1. **Détection des vulnérabilités :** les pirates informatiques identifient les failles de codage ou les portes dérobées cachées dans les applications logicielles ou les systèmes.
2. **Développement de code malveillant :** un logiciel malveillant est créé pour exploiter la vulnérabilité. Les attaquants peuvent utiliser des campagnes de phishing ciblées ou des sites Web chargés de logiciels malveillants pour transmettre le code malveillant.
3. **Exécution de l'attaque :** le code malveillant est déployé, compromettant le système et pouvant permettre un vol de données ou une interférence opérationnelle.

Techniques courantes

- Les téléchargements furtifs entraînent l'installation de logiciels malveillants à l'insu des utilisateurs.
- Les e-mails de phishing diffusent des charges utiles ou des liens malveillants pour exploiter les vulnérabilités.
- Les attaques sans fichier échappent à la détection en exécutant des opérations entièrement dans la mémoire d'un système.

Ces vecteurs d'attaque hautement avancés rendent les attaques Zero-day particulièrement dangereuses, car les outils de détection traditionnels basés sur les signatures ne parviennent souvent pas à les reconnaître.

Répercussions pour les entreprises

Les attaques Zero-day comportent des risques importants en raison de leur imprévisibilité et du délai de détection. Les conséquences peuvent être catastrophiques sur plusieurs fronts.

Pertes financières

La réussite d'une attaque Zero-day peut entraîner des coûts considérables, allant d'amendes réglementaires à une perte de revenus pendant les interruptions de service. Par exemple, une vulnérabilité non identifiée exploitée sur une plateforme de commerce électronique pourrait désactiver le processus de paiement, ce qui aurait un impact direct sur les ventes.

Conséquences sur la réputation

L'image publique d'une entreprise peut être irrémédiablement mise à mal. Les clients perdent confiance lorsque des informations sensibles sont exposées ou que les services sont interrompus.

Interruption opérationnelle

Les vulnérabilités non résolues paralysent souvent les systèmes, entraînant des pertes de productivité, des retards de projets et des opportunités commerciales manquées.

Un exemple concret

Un important prestataire de services de santé a été victime d'une attaque Zero-day ciblant des logiciels médicaux non corrigés. L'attaque a perturbé les opérations principales, exposé les données des patients, coûté **des millions** à l'entreprise en frais de récupération et a érodé par la même occasion la confiance des patients**.**

Statistiques alarmantes

Selon une étude Ponemon de 2023, les recherches indiquent que le pourcentage de violations impliquant des attaques Zero-day est d'environ 80 %

Les attaques Zero-day représentent constamment plus de **70 %** des vulnérabilités exploitées

Source : 2024 : IMandiant « M-Trends »

Lutte contre les attaques Zero-day avec Dell Technologies

Dell Technologies propose des solutions leaders sur le marché pour aider les entreprises à se prémunir activement contre les attaques Zero-day tout en favorisant une récupération rapide après de telles violations.

Solutions de serveurs et de stockage sécurisés

Les solutions de serveurs et de stockage sécurisés Dell offrent des couches de protection supplémentaires :

- Les serveurs sécurisés surveillent et bloquent les tentatives d'accès non autorisées**.**
- Les systèmes de sauvegarde et de récupération des données garantissent que, même dans les pires scénarios, les informations critiques restent accessibles et intactes.

Points de terminaison renforcés avec Dell Trusted Devices

Les points de terminaison sont un point d'entrée clé pour les attaquants. Dell Trusted Devices intègre des mesures de sécurité avancées, garantissant ainsi la protection des points de terminaison contre les menaces non détectées.

- **SafeBIOS** protège le firmware contre toute manipulation, garantissant ainsi l'intégrité totale du système.
- **SafeID** protège les informations d'identification des utilisateurs en sécurisant les processus d'authentification.
- **SafeData** chiffre les données sensibles au repos et en transit, les rendant inutilisables en cas d'interception ou d'exploitation.

Détection proactive des menaces avec CrowdStrike

CrowdStrike utilise des analyses avancées et l'IA pour surveiller l'activité des points de terminaison, en détectant les comportements inhabituels susceptibles d'indiquer des exploitations Zero-day. Sa détection proactive des menaces garantit une réponse rapide avant que les vulnérabilités n'entraînent des dommages étendus.

Par exemple, un fournisseur de télécommunications utilisant CrowdStrike a pu détecter de manière précoce des anomalies dans le trafic réseau, ce qui a atténué une exploitation Zero-day potentielle sur les serveurs des clients.

Les solutions Dell PowerProtect

Dell PowerProtect offre des sauvegardes robustes et immuables, ainsi que des options de récupération isolées. À la suite d'une attaque Zero-day, les entreprises peuvent restaurer rapidement et efficacement leurs opérations, tout en maintenant la continuité de l'activité et en protégeant les données vitales de leurs clients.

Par exemple, une grande chaîne de vente au détail a utilisé PowerProtect pour récupérer des fichiers chiffrés compromis par une attaque par ransomware résultant d'une vulnérabilité Zero-day, évitant ainsi des interruptions de service prolongées.

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

La véritable sécurité nécessite plusieurs solutions. Une stratégie multicouche combine la technologie, les processus et les personnes pour former un cadre de protection complet.

Actions clés pour renforcer la défense

- **Adopter les principes Zero-Trust :** vérifiez chaque individu et appareil tentant d'accéder au réseau.
- **Mettre en œuvre un chiffrement avancé :** utilisez des protocoles de chiffrement pour protéger les données en mouvement et au repos.
- **Former les employés :** organisez des sessions de formation complète pour apprendre aux employés à reconnaître les tentatives d'hameçonnage et les tactiques d'ingénierie sociale.
- **Tester régulièrement les systèmes :** effectuez des tests d'intrusion et des analyses de vulnérabilité cohérents pour vous assurer que les défenses s'adaptent aux nouvelles menaces.

Dell Technologies associe ces pratiques à ses solutions de sécurité avancées, garantissant ainsi que les entreprises sont prêtes à lutter efficacement contre les vulnérabilités Zero-day.

Cybersécurité renforcée via des partenariats

La collaboration de Dell avec les leaders du secteur **Microsoft**, **CrowdStrike** et **SecureWorks** permet aux clients d'accéder à des informations et des outils de sécurité de pointe.

- **Microsoft** s'intègre de manière transparente aux solutions Dell pour garantir la compatibilité à l'échelle du système et des mécanismes de protection proactifs
- **CrowdStrike** offre une intelligence avancée sur les menaces envers les points de terminaison pour détecter les exploitations potentielles Zero-day.
- **SecureWorks** assure une surveillance continue et des mesures correctives expertes pour répondre aux attaques en temps réel.

Tirer parti de Dell Professional Services

Dell Professional Services propose une gamme complète de conseils, de mise en œuvre et d'assistance à la récupération pour aider les entreprises à gérer et à atténuer les risques associés aux menaces Zero-day. De la réponse aux incidents à la planification de la feuille de route en matière de cybersécurité, Dell aide les entreprises à atteindre une résilience à long terme.

Construisez un avenir meilleur

Investir dans Dell Technologies signifie avoir un partenaire qui offre non seulement une technologie supérieure, mais aussi une tranquillité d'esprit. À travers des solutions de pointe, des partenariats stratégiques et une expertise inégalée, Dell permet aux entreprises d'anticiper et de détecter les attaques Zero-day les plus avancées, et de s'en remettre.

Contactez Dell Technologies dès aujourd'hui pour sécuriser votre entreprise, protéger votre réputation et prospérer dans un environnement numérique imprévisible. Faites confiance à Dell pour protéger votre avenir contre les menaces de demain.

Dell Technologies inspire confiance en permettant aux entreprises de garder une longueur d'avance sur les défis que représentent les attaques Zero-day en constante évolution grâce à ses solutions et services de sécurité conçus pour protéger ce qui compte le plus.

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

Consulter d'autres ressources

Prenez part à la discussion avec #hashtag

DELL Technologies