DELL Technologies

Se défendre contre les cyberattaques de la chaîne logistique avec Dell Technologies

Synthèse

La nature de plus en plus mondiale et interconnectée des opérations commerciales expose les entreprises à des menaces croissantes de cyberattaques visant la chaîne logistique. Ces attaques sophistiquées exploitent les vulnérabilités du cycle de vie du matériel, de la fabrication au déploiement, ainsi que des logiciels tiers, permettant à des acteurs malveillants de compromettre des systèmes entiers par le biais d'applications ou de mises à jour fiables. Non seulement ces incidents sont désastreux sur le plan financier, mais ils peuvent également ternir la réputation d'une entreprise et perturber ses opérations à grande échelle.

Les implications de ces menaces sont profondes. Souvent, les attaques de la chaîne logistique passent inaperçues jusqu'à ce que des dommages importants se produisent. Des stratégies de défense proactive sont donc essentielles. En offrant une protection avancée des points de terminaison, une surveillance proactive et des solutions complètes de sécurité des serveurs et des données, Dell permet aux entreprises de sécuriser leur chaîne logistique de bout en bout. Grâce à notre technologie, nos partenariats et notre expertise, les entreprises peuvent renforcer leur résilience et se protéger contre les failles de sécurité inhérentes à leurs écosystèmes.

La menace croissante des cyberattaques de la chaîne logistique

Les attaques de la chaîne logistique se sont considérablement multipliées ces dernières années. En altérant des périphériques physiques lors de la production, de l'expédition ou du déploiement, ou en détectant les failles des fournisseurs de logiciels, les attaquants parviennent à injecter des composants ou du code malveillants, corrompre des systèmes ou exfiltrer des données sensibles. Les victimes, qui sont aussi bien des petites entreprises que des multinationales, essuient alors de lourdes conséquences comme de graves pertes financières, une détérioration de la confiance des clients, ainsi que des répercussions juridiques. Dell Technologies a parfaitement conscience de l'essor de ce danger et prône l'application de mesures préventives permettant de limiter les conséquences catastrophiques de ces attaques.

Comprendre les cyberattaques de la chaîne logistique

Fonctionnement des attaques de la chaîne logistique matérielle

1. **Phase de fabrication :** les attaquants introduisent des composants malveillants lors de l'assemblage du matériel, tirant souvent parti de fournisseurs compromis.
2. **Phase d'expédition :** les périphériques sont interceptés pendant le transport et altérés pour y inclure des modifications matérielles ou de firmware nuisibles.
3. **Déploiement et activation :** une fois que le matériel compromis pénètre dans le réseau de l'entreprise, les attaquants accèdent aux données sensibles ou activent des portes dérobées.

Fonctionnement des attaques de la chaîne logistique logicielle

1. **Violation initiale :** un fournisseur de logiciels tiers est compromis, souvent par le biais d'un hameçonnage, de failles non corrigées ou de menaces internes.
2. **Manipulation de code :** les acteurs malveillants injectent des éléments malveillants tels que des logiciels malveillants ou des portes dérobées dans des logiciels destinés à la distribution.

3. **Propagation aux utilisateurs finaux :** les entreprises qui installent ou mettent à jour des logiciels compromis téléchargent sans le savoir des composants malveillants.

Techniques courantes - Attaques matérielles

- **Manipulation de firmware :** incorporation de code malveillant qui s'active après le déploiement.
- **Implantation matérielle :** intégration de composants cachés pour surveiller ou exfiltrer les données.
- **Exploitation des fournisseurs de confiance :** mise à profit de fournisseurs tiers dont les processus sont moins sécurisés.

Techniques courantes - Attaques logicielles

- **Détournement de composants :** infection de bibliothèques ou de structures tierces par du code malveillant.
- **Injection de mises à jour :** modification des mises à jour logicielles officielles pour y inclure des failles d'exploitation.
- **Confusion liée aux dépendances :** exploitation de la dépendance des entreprises à des packages non sécurisés.

L'impact sur les entreprises

Conséquences financières

Les attaques ciblant les chaînes logistiques entraînent souvent des coûts divers : sanctions légales, frais de restauration des systèmes et indemnisation des clients. Pour illustrer les ravages financiers que peuvent causer ces violations, citons l'exemple d'un incident très médiatisé ayant coûté plus de 70 millions de dollars à une entreprise mondiale de gestion IT.

Interruption opérationnelle

Les systèmes corrompus ou neutralisés à la suite d'une infiltration malveillante conduisent souvent à des temps d'arrêt prolongés, ce qui nuit à la productivité de l'entreprise et retarde la livraison des projets.

Conséquences sur la réputation

Les entreprises modernes doivent impérativement pouvoir faire confiance à leurs partenaires logiciels. Une violation de la chaîne logistique liée aux solutions logicielles d'une entreprise peut ternir sa réputation et éroder la fidélité des clients.

Exemples concrets - Attaques matérielles/logicielles

Un fabricant mondial de produits électroniques a découvert des composants compromis dans sa chaîne logistique, entraînant des pannes généralisées du système. L'attaque lui a coûté plus de **45 millions de dollars** en frais juridiques et en dépenses de restauration, sans compter les dommages irréparables causés aux relations avec ses fournisseurs.

La violation qu'a subie SolarWinds figure parmi les attaques de chaîne logistique logicielle les plus notoires. La compromission de son produit Orion a infecté de nombreuses organisations à travers le monde, y compris des administrations et des entreprises du classement Fortune 500. Les dommages ont été estimés à plus de **90 millions de dollars**, et cette violation a mis en évidence les conséquences étendues des failles de sécurité de la chaîne logistique.

L'expertise de Dell Technologies dans la lutte contre les attaques de la chaîne logistique

La vaste gamme de solutions de sécurité de Dell Technologies donne aux entreprises les moyens de garder une longueur d'avance sur l'évolution des cyberrisques.

Dell Secure Component Verification (SCV)

L'outil Dell Secure Component Verification (SCV) fait partie intégrante de la stratégie de sécurité de la chaîne logistique de Dell Technologies. Il est conçu pour garantir l'authenticité et l'intégrité des composants matériels sur plusieurs solutions Dell. SCV assure la validation cryptographique des composants du système, de la fabrication à la livraison et au déploiement. Dell Technologies offre une sécurité robuste de la chaîne logistique, garantissant que les systèmes sont inviolables et sécurisés dès l'usine et jusqu'à leur déploiement. Les clients Dell bénéficient ainsi d'une sécurité, d'une fiabilité et de performances globales améliorées.

Sécuriser les points de terminaison avec Dell Trusted Devices

Les Dell Trusted Devices intègrent la sécurité au niveau du matériel et du firmware pour créer des systèmes inviolables.

- **SafeBIOS** garantit l'intégrité du firmware au démarrage, empêchant les modifications de configuration non autorisées. Il vérifie également l'intégrité du firmware au démarrage afin d'empêcher le lancement des systèmes qui pourraient être compromis.
- **SafeID** sécurise les identifiants d'authentification au niveau du matériel, empêchant ainsi les accès non autorisés, et protège les identifiants de connexion en sécurisant les clés d'authentification, ce qui permet de bloquer les utilisateurs non autorisés.
- **SafeData** permet un chiffrement de bout en bout des fichiers professionnels sensibles, bloquant ainsi les tentatives d'exfiltration des données à des fins d'exploitation.

Détection proactive des menaces avec CrowdStrike

CrowdStrike s'intègre aux technologies Dell pour fournir des informations en temps réel sur le comportement des logiciels malveillants.

- **Analyse comportementale pour la détection des menaces :** surveille le comportement du matériel et du firmware pour identifier toute tentative de manipulation, et détecte les activités logicielles inhabituelles afin d'empêcher le déploiement de logiciels malveillants.
- **Outils de réponse immédiate :** l'IA isole les systèmes compromis, empêchant ainsi tout mouvement latéral au sein du réseau.
- **Mesures correctives basées sur l'IA :** pour identifier et isoler activement les menaces, empêchant ainsi leur propagation latérale au sein des systèmes de l'entreprise.
- **Capacités d'intégration :** les environnements hybrides et multicloud sont protégés de manière globale avec Dell et les outils CrowdStrike.

Une sécurité renforcée grâce aux solutions de serveurs et de stockage Dell

La gamme de serveurs Dell PowerEdge intègre une protection avancée pour sécuriser les plateformes logicielles stratégiques. Les systèmes de stockage tels que Dell PowerStore offrent un chiffrement de pointe pour les applications et les données.

- **Firmware de serveur sécurisé :** surveille et bloque les modifications non autorisées au niveau du matériel.
- **Surveillance de réseau isolé :** détecte les anomalies indiquant une altération de la chaîne logistique.
- **Sauvegardes immuables :** protègent les points de récupération même lorsque le stockage principal est compromis.
- **Coffres-forts de récupération :** les environnements isolés protègent contre les défaillances en cascade déclenchées par des systèmes compromis.

Approches à plusieurs niveaux pour atténuer les risques

Dell encourage les entreprises à adopter des stratégies complètes combinant technologie, bonnes pratiques du personnel et processus actualisés.

Étapes stratégiques

- **Améliorer la visibilité de la chaîne logistique :** exigez de tous les fournisseurs qu'ils respectent des normes de sécurité strictes et qu'ils certifient le matériel à chaque étape.
- **Mettre en œuvre un chiffrement avancé :** sécurisez les données à tous les niveaux à l'aide de protocoles avancés afin de limiter l'accessibilité, même sur le matériel compromis.
- **Adopter des stratégies Zero-Trust :** aucun périphérique, aucune application, ni aucun utilisateur ne peut être automatiquement considéré comme fiable sans vérification.
- **Sécuriser les normes de codage :** collaborez avec des partenaires logiciels qui appliquent des directives strictes en matière de plug-ins, d'API et d'intégrations.
- **Surveiller l'activité et mener des audits de manière régulière :** des audits de visibilité fréquents garantissent l'intégrité des services tiers.
- **Réaliser des tests réguliers :** déployez des tests d'intrusion et des évaluations de firmware pour valider l'intégrité des périphériques de manière continue.
- **Former les employés :** formez vos équipes à reconnaître les composants ou les packages qui présentent des comportements suspects.

Comment Dell Professional Services garantir la résilience de l'entreprise

Dell Professional Services accompagne les entreprises dans la mise en place de défenses robustes de leur chaîne logistique. Nos équipes d'experts en cybersécurité fournissent des évaluations, une formation et des stratégies de réponse aux menaces adaptées aux besoins uniques de chaque entreprise.

- **Conseils de mise en œuvre :** pour aligner stratégiquement les pratiques Zero-Trust et d'audit des fournisseurs dans les environnements des fournisseurs.
- **Réponses aux incidents :** pour garantir une reprise rapide des activités à la suite d'incidents malveillants.

Préparer les systèmes d'entreprise pour l'avenir avec Dell

Les cyberattaques de la chaîne logistique illustrent la sophistication des menaces modernes. Les entreprises ont besoin d'une protection qui empêche les violations, mais qui garantit également une récupération rapide lorsqu'un incident survient. En vous associant à Dell Technologies, vous accédez à des outils de pointe, à une expertise stratégique et à un réseau de collaborateurs de confiance.

Passez à l'étape suivante

Protégez vos actifs les plus précieux et rationalisez votre fiabilité opérationnelle en mettant en œuvre les pratiques d'excellence proposées par Dell Technologies. Contactez-nous dès aujourd'hui pour bénéficier d'une consultation personnalisée en vue de sécuriser le cœur de vos systèmes d'entreprise.

Dell Technologies est gage de confiance, d'adaptabilité et d'innovation dans un contexte où la cybersécurité de la chaîne logistique ne cesse d'évoluer. Votre engagement d'aujourd'hui garantit votre réussite de demain.

Un avenir plus sûr et plus sécurisé commence avec Dell Technologies. Faites-nous confiance 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