

Attaques contre la supply chain

Décomposition des séquences.

1. Tentative de vol de données d'identification :

Initier un effort pour acquérir des identifiants de connexion internes auprès du personnel de logiciels tiers.

1. Accès non autorisé au réseau :

Utiliser les informations d'identification obtenues pour se connecter au réseau interne et identifier les comptes disposant d'un accès privilégié.

1. Renforcement des privilèges :

Mettre en œuvre des techniques de renforcement des privilèges afin d'accéder aux données sensibles par le biais des comptes privilégiés identifiés.

Approche par contre-mesures :

Pour contrecarrer cette séquence d'attaque, il faut la perturber stratégiquement. L'application d'outils et de tactiques de sécurité peut y parvenir, mais l'efficacité des mécanismes de défense repose sur une base solide en matière de gestion des accès sécurisés.



Exemples d'attaques contre la supply chain.

[Brand Name] - Birefing sur la cyberattaque :

La cyberattaque de [Brand Name] se distingue par une violation sophistiquée de la supply chain qui a visé un important fournisseur de logiciels offrant des outils de gestion de systèmes cruciaux pour la surveillance des réseaux et des infrastructures.

1. Exploitation ciblée :

Les attaquants ont stratégiquement exploité [Brand Name] en injectant un code malveillant dans son logiciel de surveillance et de gestion informatique Orion, très répandu.

1. Importance de [Brand Name] :

En tant que fournisseur de logiciels mondialement reconnu, [Brand Name] a joué un rôle essentiel dans l'infrastructure informatique de nombreuses organisations dans le monde entier..

1. Exploitation des accès privilégiés :

[Brand Name] Orion tenait une position privilégiée avec un accès de haut niveau aux systèmes informatiques cruciaux. Les pirates ont profité de cet accès privilégié pour naviguer dans les réseaux, exfiltrer des données sensibles et établir une présence persistante dans les environnements compromis.

L'attaque de [Brand Name] a mis en évidence les risques inhérents à la compromission des fournisseurs de logiciels de confiance, en particulier ceux qui disposent d'un accès privilégié à des systèmes essentiels. L'incident a incité à réévaluer les pratiques de sécurité de la supply chain et a souligné le besoin critique de défenses robustes pour contrecarrer l'abus potentiel de positions privilégiées au sein de solutions logicielles largement déployées.



Exemples d'attaques contre la supply chain.

Briefing sur la cyberattaque d'Uber :

1. Exploitation ciblée :

L'attaque de la supply chain contre Uber s'est déroulée avec la compromission de Teqtivity, un fournisseur tiers spécialisé dans la gestion des équipements informatiques.

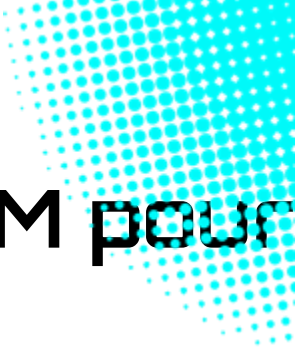
1. L'importance d'Uber :

La notoriété d'Uber en tant qu'entreprise mondiale de covoiturage et de technologie a renforcé l'importance de l'attaque. La compromission de Teqtivity a constitué une menace directe pour les vastes opérations d'Uber et la confidentialité des données appartenant à plus de 77 000 employés.

1. Exploitation des accès privilégiés :

En tant que partenaire de gestion des équipements informatiques, Teqtivity tenait une position privilégiée avec un accès aux systèmes cruciaux d'Uber. Le pirate a tiré parti de cette position pour s'introduire dans le serveur de sauvegarde AWS de Teqtivity, soulignant ainsi les risques inhérents associés à la compromission de fournisseurs de confiance disposant d'un accès privilégié.

La violation a eu un impact important sur Uber, car elle a entraîné l'exposition d'informations confidentielles sur les employés et de codes sources exclusifs. L'attaque de la supply chain d'Uber sert de leçon précieuse pour les organisations concernant l'importance de la vigilance dans la sécurisation des fournisseurs tiers. Elle souligne la nécessité de procéder à des évaluations complètes des pratiques de sécurité des fournisseurs, en particulier ceux qui disposent d'un accès sécurisé.



Principes de base de la PAM pour protéger l'infrastructure informatique contre les menaces pesant sur la supply chain :

Recherche et surveillance des comptes privilégiés :

Menace : Les comptes privilégiés oubliés sont l'un des points d'entrée des cybercriminels.

L'utilité de PAM :

- Outils de recherche automatisés pour localiser les comptes privilégiés sur l'ensemble du réseau.
- Mettre à jour et conserver régulièrement un inventaire des comptes privilégiés, notamment les attributs et les niveaux d'accès qui leur sont associés.
- Mécanismes de surveillance continue permettant de détecter rapidement les comptes privilégiés nouveaux ou dormants.

Sécuriser les comptes privilégiés :

Menace : Une authentification faible facilite la violation des comptes privilégiés.

L'utilité de PAM :

- Utiliser l'authentification multifactorielle (MFA) pour l'accès aux comptes privilégiés.⁷
- Mise à jour et rotation régulières des mots de passe pour les comptes privilégiés afin de limiter le risque d'attaques basées sur les informations d'identification.
- Principe du moindre privilège, garantissant que les individus n'ont accès qu'aux privilèges nécessaires à leur fonction.
- Chiffrement pour protéger les informations d'identification des comptes privilégiés lors de la transmission et du stockage.



Suivi des activités d'accès privilégié :

Menace : La détection et la réaction tardives augmentent les pertes après les incidents de sécurité.

L'utilité de PAM :

- Mécanismes de consignment permettant de recueillir des informations détaillées sur les événements liés aux accès privilégiés.
- Examiner et analyser les journaux afin d'identifier les activités suspectes ou anormales.
- Alertes en temps réel en cas de schémas d'accès spécifiques ou d'actions non autorisées.
- Audits périodiques des journaux d'accès privilégiés afin de garantir la conformité avec les politiques de sécurité.

Automatiser la gestion des privilèges :

Menace : La gestion manuelle des accès privilégiés augmente le risque d'erreur humaine.

Ce que fait PAM automatiquement :

- Recherche de comptes privilégiés et gestion de l'inventaire.
- Approvisionnement et désapprovisionnement des accès privilégiés sur la base de politiques prédéfinies.
- Rotation des mots de passe et processus de mise à jour pour minimiser la fenêtre de vulnérabilité.
- Intégration avec le système de gestion des informations et des événements de sécurité (SIEM) pour des réponses automatisées aux incidents de sécurité.

La protection contre les attaques de la supply chain est partielle sans PAM. En intégrant ces activités dans le dispositif de sécurité, les entreprises peuvent renforcer leur résilience et atténuer les risques liés aux vulnérabilités des accès privilégiés