Comment Varonis a aidé un hôtel-casino américain à vaincre une cyberattaque en 30 minutes

ÉTUDE DE CAS

« Sans Varonis, je n'aurais probablement jamais su qu'un compte avait été piraté. Avec Varonis, j'étais au téléphone avec l'équipe de réponse aux incidents pendant une demi-heure et le problème était résolu. »

À PROPOS DE CETTE ÉTUDE DE CAS :

À propos de cette étude de cas : notre client est un hôtel et casino américain. À sa demande, nous ne mentionnons aucun nom ni aucun lieu dans cette étude.

EN BREF

LES PROBLÈMES

- Les hackers ont ciblé un RDP ouvert et obtenu des noms de comptes
- Ils ont lancé une attaque par force brute et tenté de pirater des comptes dotés de privilèges
- Des données sensibles, dont des données à caractère personnel et PCI étaient en danger

LA SOLUTION

La plateforme de sécurité des données la plus solide :

- **DatAdvantage** surveille l'accès aux données et les activités Active Directory et sur site
- **Data Classification Engine** identifie les données sensibles à risque, dont les données à caractère personnel et PCI
- **DatAlert Suite** permet de surveiller en continu les systèmes et de générer des alertes

RÉSULTATS

- Varonis a détecté la menace et l'équipe de réponse aux incidents a réussi à la vaincre en 30 minutes
- L'admin réseau a gagné entre 2 et 3 heures par jour grâce aux alertes et aux rapports automatisés
- Pouvoir joindre une équipe d'experts rapidement par téléphone garantit la tranquillité d'esprit

Les problèmes

Vaincre une attaque malveillante avant qu'elle ne se répande

Tout a commencé par un serveur exposé.

Un hôtel-casino américain (qui a demandé à rester anonyme) avait une connexion ouverte RDP (remote desktop port) à Internet.

Les attaquants ont obtenu accès au serveur et ont également récupéré des noms de comptes. Ils ont essayé tous les mots de passe imaginables, tentant une attaque par force brute pour s'infiltrer sur des comptes utilisateur.

Ce fut un moment éprouvant pour le responsable de l'administration réseau.

> « Ils avaient réussi à obtenir les noms de comptes. Ils auraient pu employer la force brute pendant longtemps pour tenter de s'infiltrer sur un compte privilégié. Et après, qui sait ? Ils auraient pu avoir accès à nos serveurs de fichiers… ou n'importe lequel de nos systèmes. »

Une fuite de données aurait été catastrophique. Les données à caractère personnel et PCI de centaines d'employés et de milliers de clients auraient pu être dérobées. Et comme l'incident a eu lieu le week-end, personne n'aurait probablement détecté quoi que ce soit pendant au moins 2 jours.

Pire encore, avec leur précédente solution de sécurité, il est possible que l'entreprise n'ait jamais rien su de la menace. À cause d'un manque d'assistance et de formation, l'entreprise n'était pas préparée à enquêter ni à faire face à une attaque de cette ampleur.

> « Une seule personne était formée pour utiliser notre ancien produit. Nous savions vaguement comment nous y prendre, mais nous ne le maîtrisions pas. **Nous sommes passés à Varonis, en partie pour bénéficier de leurs supports de formation très bien conçus et de leur excellent service client.** »

Varonis assure la surveillance continue et génère des alertes sur tous les systèmes essentiels du casino et de l'hôtel. L'admin réseau a donc été prévenu de l'attaque en quelques secondes.

Grâce à l'aide de l'équipe de réponse aux incidents de Varonis, ce qui aurait pu être une faille de sécurité a rapidement été corrigé.

> « Ils avaient réussi à obtenir les noms de comptes. Ils auraient pu employer la force brute pendant longtemps pour tenter de s'infiltrer sur un compte privilégié. »

La solution

Un moyen fiable de détecter et vaincre les menaces de façon proactive

Trois produits de Varonis ont permis à l'admin réseau de détecter et vaincre l'attaque sur le serveur exposé de l'hôtel-casino :

1. **DatAdvantage pour Windows et les directory services**, qui prend en charge les serveurs sur site et Active Directory en indiquant clairement qui peut accéder aux données et qui le fait.
2. **Data Classification Engine pour Windows et SharePoint**, qui identifie automatiquement les données sensibles à risque, dont les données à caractère personnel et les données PCI.
3. **DatAlert Suite**, qui surveille les actifs essentiels et détecte toute activité suspecte et comportement inhabituel.

> « Varonis génère une alerte à chaque fois que quelqu'un essaie d'accéder au serveur. La solution enregistre qui a accédé à quels fichiers. Elle fait également attention aux tentatives de connexion des personnes étrangères à votre réseau. Nous pouvons localiser les problèmes et les régler. »

Le premier signe de l'attaque est survenu quand Varonis a détecté des anomalies dans Active Directory et envoyé deux alertes à l'admin réseau :

- Attaque d'énumération de compte à partir d'une seule source (à l'aide de NT LAN Manager ou NTLM).
- Verrouillage : nombreux événements de verrouillage d'un compte

L'admin réseau a immédiatement appelé leur responsable de compte Varonis, qui a mobilisé sans attendre l'équipe de réponse aux incidents Varonis.

> « Ce fut incroyable. J'ai appelé mon responsable de compte un dimanche à 8 heures du matin. L'équipe s'est arrangée pour me mettre immédiatement en contact avec un interlocuteur. Ils nous ont aidés à résoudre le problème rapidement et facilement et nous n'avons pas rencontré d'autres difficultés depuis. »

À l'aide de l'interface Web, l'équipe de réponse aux incidents a enquêté sur les événements d'échec d'authentification et déterminé que les noms d'utilisateur et les noms des appareils avaient été falsifiés. Puis ils ont inspecté le contrôleur de domaine qui avait enregistré les échecs d'authentification et ont consulté les logs du NTLM.

L'analyse post-mortem a révélé qu'un serveur Exchange et le système CVC étaient à l'origine de ces échecs d'authentification. Un serveur avait été laissé ouvert pour que l'entreprise de maintenance CVC puisse y avoir accès. Une vulnérabilité qui aurait pu compromettre tout le réseau.

> « Varonis m'aide à localiser précisément les serveurs et les ports ciblés par les pirates. La solution me permet de facilement verrouiller des serveurs un par un et de mettre en priorité les zones les plus à risque. »

Pour identifier l'adresse IP source et le port utilisé dans l'attaque par force brute, l'équipe de réponse aux incidents a lancé une commande NETSTAT (statistiques du réseau) sur les postes affectés. Cette commande a révélé que les échecs d'authentification provenaient d'une adresse IP basée en Russie sur un protocole RDP.

L'équipe de réponse aux incidents a aidé l'admin réseau à désactiver le serveur CVC pendant leur appel téléphonique et à mettre fin à l'attaque par force brute. Ils ont également recommandé à l'hôtel-casino de désactiver l'accès externe à distance et d'activer le pare-feu Windows sur le serveur Exchange pour se protéger des attaques à l'avenir.

« J'étais au téléphone avec l'équipe de réponse aux incidents de Varonis pendant une demi-heure et le problème était résolu. »

Résultats

Tranquillité d'esprit et gain de temps

Avec Varonis, l'admin réseau a obtenu une visibilité sur les serveurs sur site et sur Active Directory. Il n'aurait jamais cru que la solution pouvait leur être aussi vitale.

« C'est génial d'avoir la possibilité de surveiller et de voir tout ce qui se passe sur mes serveurs. Les alertes automatiques, c'est le petit plus. Tous ces avantages ont rapidement porté leurs fruits. »

Lorsque l'on a une équipe de réponse aux incidents dans son camp et un partenaire prêt à réagir au quart de tour pour enquêter sur les menaces et les vaincre à la source, on a une confiance inébranlable.

L'admin réseau explique comment une cyberattaque potentiellement catastrophique pour leurs systèmes a été résolue en un rien de temps, grâce à Varonis :

> « Sans Varonis, je n'aurais probablement jamais su qu'un compte avait été piraté. Avec Varonis, j'étais au téléphone avec l'équipe de réponse aux incidents pendant une demi-heure et le problème était résolu. »

À présent, Varonis continue d'assurer la surveillance et les alertes sur tous les systèmes essentiels de l'hôtel-casino. La visibilité renforcée permet à l'admin réseau d'identifier et de corriger les vulnérabilités en toute confiance et beaucoup plus rapidement.

> « Entre les alertes en continu et les rapports automatiques, Varonis me fait gagner entre 2 et 3 heures par jour. La surveillance des systèmes essentiels est bien plus facile. La fonction de reporting à elle seule en justifie le coût. »

« Entre les alertes en continu et les rapports automatiques, Varonis me fait gagner entre 2 et 3 heures par jour. »

Vous aussi ayez l’esprit tranquille et faites-vous accompagner par une équipe d’experts.

Varonis vous permet d’enquêter sur les menaces, de résoudre des incidents de sécurité et de protéger vos systèmes essentiels.

DEMANDER UNE DÉMO