ARMIS®

Kalahari RESORTS & CONVENTIONS

FALLSTUDIE

Einzigartiges Us-Resort Erhöht Sichtbarkeit Über Alle Netzwerke Hinweg

Armis ermöglicht es CISO und IT, eine zentralisierte Ansicht der Netzwerkressourcen zu erhalten und sich auf die wichtigsten Prioritäten zu konzentrieren

Branche

Resort und Kongresszentrum

IT-Umgebung

Mehrere Umgebungen (PCI-Infrastruktur, Gastnetzwerk, Audio-/Videoeinrichtungen) mit etwa 5.000 vernetzten Geräten

Einführung

Kalahari Resorts & Conventions bietet seinen Gästen in seinen vier Einrichtungen in den USA einzigartige Urlaubs- und Tagungserlebnisse. Mit drei hochaktiven Netzwerken zur Verwaltung – Unternehmen, PCI und Gast – implementierte der CISO Armis, um einen tieferen und breiteren Einblick in Netzwerkgeräte, Benutzer und Netzwerkverkehr zu erreichen. Die erfolgreiche Bereitstellung führte zu zusätzlichen Anwendungsfällen, die den Betrieb erheblich verbessert und Zeitersparnisse erzielt haben, indem ein Fokus auf Schlüsselbereiche gelegt wurde.

Kalahari Resorts & Conventions sind im afrikanischen Design gestaltete Urlaubs- und Konferenzziele in den USA, die umfassenden Service mit erstklassigen Unterkünften, hochmodernen Tagungs- und Kongresseinrichtungen und Amerikas größten Indoor-Wasserparks bieten. Derzeit gibt es Kalahari Resorts an vier Standorten in den USA: Wisconsin Dells, Wisconsin; Sandusky, Ohio; Pocono Mountains, Pennsylvania; und Round Rock, Texas. Darüber hinaus gehören zu den Anlagen von Kalahari Resorts ein Golfplatz und eine Firmenzentrale.

Tim Everson ist seit drei Jahren als CISO von Kalahari Resorts als Teil des Führungsteams tätig, das für rund 30 IT-Experten verantwortlich ist. Er ist auf praktischer Ebene in alle Sicherheitsbereiche involviert – Design, Architektur, Implementierung, Strategie, Compliance und Gästeprobleme.

Bei Kalahari Resorts beaufsichtigen Everson und sein Team mehrere Umgebungen: die Unternehmensinfrastruktur, die Infrastruktur der Zahlungskartenbranche (Payment Card Industry; PCI), ein großes Gastnetzwerk und Audio-/Videoeinrichtungen. Everson wurde aufgefordert, Armis zu evaluieren, weil er sich zunehmend Sorgen über mangelnde Transparenz in all diesen Bereichen machte. Nachdem er in der Einrichtung in Wisconsin Dells einen nahtlosen „Proof-of-Value“ (PoV) durchgeführt hatte, war Everson überzeugt, dass Armis genau das war, wonach er suchte.

„Armis hob sich von anderen Anbietern ab, vor allem wegen seiner Benutzerfreundlichkeit, Einfachheit, unkomplizierten Schnittstellen, Plug-and-Play-Bereitstellung und seiner Fähigkeit zum Segmentieren, Anzeigen, Sortieren und Warnen. Der Nutzen war sofort da, ohne Zweifel. Wir konnten am ersten Tag anfangen und Dinge erledigen“, sagt er. „Armis ist großartig darin, alles in meiner Umgebung zu finden. Ich sehe, was ich sehen muss, und schätze die Funktionen, die ich vorher nicht hatte.“

Darüber hinaus nutzen Everson und sein Team die umfangreichen Integrationsmöglichkeiten von Armis voll aus, wodurch sie mehr Wert aus bestehenden Tools ziehen können. Sie haben bereits Integrationen mit Microsoft Active Directory, vCenter Server, dem zentralen Verwaltungsprogramm für VMware, Simple Network Management Protocol (SNMP), einem Protokoll zum Sammeln und Organisieren von Daten über verwaltete Geräte in Netzwerken, und einer der vielen Integrationen mit Wireless-Herstellern, die Armis anbietet, abgeschlossen. In naher Zukunft planen Everson und sein Team auch, andere Anbieter von kabelgebundener und drahtloser Endgeräteausrüstung und Endgerätesicherheitsintegrationen zu nutzen.

Die PCI-Umgebung steht im Mittelpunkt

Zu den unternehmenskritischsten Anwendungsfällen für Armis bei Kalahari Resorts gehört es, einen besseren Einblick in die PCIInfrastruktur zu erhalten, in der Kreditkarteninhaberinformationen abgerufen und übertragen werden. Um die Sicherheit und Vertraulichkeit von Karteninhaberdaten zu gewährleisten und Kreditkartenbetrug zu verhindern, muss Kalahari Resorts die Payment Card Industry Data Security Standards (PCI-DSS) einhalten.

Vor diesem Hintergrund hat Armis maßgeblich dazu beigetragen, dass Everson sicherstellen konnte, dass die Netzwerksegmentierung ordnungsgemäß funktioniert. Armis überwacht auch die Kommunikation zwischen den Segmenten. Schließlich bietet es einen umfassenden und genauen Einblick in die Aktivität der Geräte und der Personen, die sie verwenden, sowie die Gewissheit, dass die Karteninhaberdaten dort sind, wo sie sein sollten.

„Dank Armis sind wir jetzt in der Lage, Einblicke in die PCI-Umgebung zu haben und Warnungen zu erhalten, wenn neue Geräte versuchen, in sie einzudringen. Die Fähigkeit, anormalen Datenverkehr, der durch PCI-Firewalls und Subnetze geht, klar zu erkennen, war für uns ein großer Vorteil“, bemerkt Everson. „Wenn wir eine Benachrichtigung von Armis erhalten, dass ein Gerät versucht, in das PCI-Netzwerk einzudringen, können wir zurück zur Firewall gehen und sicherstellen, dass die Ports geschlossen sind, damit die Daten keine Endpunkte erreichen. Allein dieser Anwendungsfall ist eine Rechtfertigung und Bestätigung für eine Investition in Armis.“

Herausforderungen

- Bereitstellung einer klareren Transparenz auf Managementebene in Unternehmens-, PCI- und Gastnetzwerken
- Gewinnen tieferer Einblicke und Umgang mit problematischem Traffic
- Verbesserung der Fähigkeiten im Bereich des Schwachstellenmanagements für das IT-Personal der Resorts
- Entlastung überlasteter Sicherheitsressourcen

Gerätebestand über alle Netzwerke hinweg

Kalahari Resorts verfügt über einen großen Bestand an verwalteten Netzwerkanlagen, der aus fast 2.200 PCs im gesamten Unternehmen sowie hunderten von Switches, Videokameras und anderen Geräten besteht. Armis verfolgt und kategorisiert diese Geräte und sammelt wertvolle Daten wie Sicherheitsstatus, Schwachstellen, Anomalien und wo und von wem Geräte verwendet werden.

Darüber hinaus und ebenso wichtig ist die Fähigkeit von Armis, Gastgeräte zu erkennen. Everson erklärt, dass Armis in jeder Woche gezeigt hat, dass fast 140.000 Geräte – von Mobiltelefonen und Laptops bis hin zu mit Drahtlostechnologie ausgestatteten Fahrzeugen auf den Parkplätzen der Resorts – versuchen können, auf das Kalahari Resorts-Netzwerk zuzugreifen.

Er weist auch darauf hin, dass es nicht ungewöhnlich ist, dass es im Gastnetzwerk enorme Traffic-Spitzen gibt. Wenn dies auftritt, hilft Armis Everson und seinem Team dabei, sofort zu erkennen, welche Gäste im Netzwerk dies verursachen. Dazu gehört die Erkennung von Aktivitäten, die von BitTorrent verursacht werden, einem Protokoll, das es jedem ermöglicht, Multimediadateien wie Videos, Musik, Apps, Bilder und Dokumente herunterzuladen und zu teilen. Das Problem bei der Verwendung von BitTorrent besteht darin, dass die Software nicht nur die Internetverbindung verlangsamt, sondern möglicherweise auch bösartige Dateien oder Malware in das Netzwerk einschleusen kann.

„Es ist erstaunlich, wie schnell wir Dinge wie BitTorrent in unserem Netzwerk sehen können. Wir sind ein Resort, aber wir müssen trotzdem sicherstellen, dass Gäste in unserem Netzwerk keine Dinge wie das Herunterladen von Torrents tun“, erklärt Everson. „Mit Armis können wir diese Art von Aktivität bei den Gästen sofort sehen. Dann können wir sie vom Netzwerk trennen und den Zugangspunkt sperren, ohne uns darum kümmern zu müssen.“

Ergebnisse der Einführung von Armis

- Genaue und umfassende Bestandsaufnahme von Geräten in allen drei Netzwerken
- Strengere Kontrolle über abnormales Verhalten im Gastnetzwerk
- Bessere Übersicht über Bandbreite und Netzwerkperformance
- Verbesserte PCI-Sicherheit und -Compliance
- Zentralisierte, leicht zugängliche Dashboards mit granularen Daten für eine effizientere Problemlösung
- Erhebliche Zeitersparnis durch Reduzierung des Sicherheitsaufwands

Unerwartete Anwendungsfälle für Armis

Neben der Nutzung von Armis, um vollständige Transparenz und Einblicke in Geräte zu erhalten, hat Kalahari Resorts auch andere Anwendungen für die Lösung gefunden.

Das Schwachstellenmanagement beispielsweise wurde mit Armis vereinfacht, da es Geräte ausfindig macht, die ungepatchte Apps oder ältere Betriebssysteme verwenden, was das Gesamtrisiko erhöhen kann. Die Lösung überwacht auch auf verdächtiges oder abmomales Verhalten. Mit Armis sehen wir Dinge, die andere Scanner im Bereich des Schwachstellenmanagements möglicherweise nicht sehen“, bemerkt Everson. „Wir konnten Anwendungsdatenverkehr sehen, der versuchte unsere Firewalls zu unterlaufen, und konnten dies unterbinden.“

Ein weiterer Anwendungsfall ist die Überwachung von Zertifikaten für Netzwerksicherheitsprotokolle. Armis sieht die Zertifikate, die die Netzwerke durchlaufen, und zeigt die abgelaufenen an. Dies ermöglicht Everson und seinem Team Zertifikate schnell auf den neuesten Stand zu bringen, um sichere Anwendungsworkflows und Transaktionen für Benutzer zu gewährleisten.

Darüber hinaus hat Armis Netzwerkauthentifizierungsfehler aufgedeckt. Dies tritt auf, wenn Benutzerkonten mit kürzlich geänderten Passwörtern wiederholt erfolglos versuchen, sich bei einer Website anzumelden. Das kann die Bandbreite beeinträchtigen. Durch die Identifizierung dieser Ereignisse kann Everson eine Person in seinem Team damit beauftragen, das Problem zu beheben und Korrekturmaßnahmen zu ergreifen.

„Armis hob sich von anderen Anbietern ab, vor allem wegen seiner Benutzerfreundlichkeit, Einfachheit, unkomplizierten Schnittstellen, Plug-and-Play-Bereitstellung und seiner Fähigkeit zum Segmentieren, Anzeigen, Sortieren und Warnen. Der Nutzen war sofort da, ohne Zweifel.”

Tim Everson
Chief Information Security Officer
Kalahari Resorts and Conventions

Ein großer Zeitvorteil

All diese Anwendungsfälle haben es Everson und seinem Team ermöglicht, eine größere betriebliche Effizienz zu genießen und ihr Zeitmanagement zu verbessern.

„Eine der Herausforderungen, vor denen wir standen war, dass Kalahari Resorts, obwohl wir heute etwa 30 IT-Mitarbeiter haben, nur ein kleines Sicherheitsteam hat. Armis hat uns unsere Zeit zurückgegeben. Jetzt können wir das Dashboard teilen und dem IT-Team die Informationen geben, die es zum Handeln benötigt“, erzählt er. „Dies war für uns von entscheidender Bedeutung, da es so viel Zeit freigesetzt und es uns ermöglicht hat, andere wichtige Arbeiten zu erledigen.“

Armis sammelt eine Fülle von Daten, die Everson und sein Team filtern, in einem Dashboard anzeigen und teilen können. Es erspart ihnen, auf 15 verschiedenen Tools zuzugreifen, um Informationen zu sammeln und zu verstehen. Armis bietet dem Sicherheitsteam die Möglichkeit, das Netzwerk zu sortieren und zu segmentieren, damit es in Echtzeit einen Drilldown durchführen kann, um alle Arten von Geräten zu sehen und zu lokalisieren und Warnungen zu erhalten, wenn es rote Flaggen gibt.

Everson empfiehlt Armis ohne zu zögern anderen Organisationen: „Armis hat für uns alles verändert. Es hat uns so viel Mühe erspart, und ich freue mich, das anderen mitteilen zu können.“