Anbieter von IT-Lösungen und Managed Services vertraut auf die von ihm vertriebenen Quest-Produkte

Phoenix Software stärkt seine eigene Sicherheit und Cyber Resilience mit Lösungen von Quest

Land: **Großbritannien**

Mitarbeiter: **430**

Branche: **Anbieter von IT-Lösungen und Managed Services**

Website: **www.phoenixs.co.uk**

Der preisgekrönte Anbieter von IT-Lösungen und Managed Services prüft die von ihm angebotenen Lösungen sorgfältig

Phoenix Software bietet IT-Lösungen und Managed Services an, die es britischen Unternehmen ermöglichen, ihre Infrastrukturen zu modernisieren und zu sichern und gleichzeitig ihre Daten zu schützen, zu visualisieren und zu verwalten. Die herausragenden Leistungen des Unternehmens wurden mit einer Vielzahl von Auszeichnungen gewürdigt, darunter „Microsoft Modern Endpoint Management Partner of the Year 2023“ und „Microsoft UK Partner of the Year 2021“.

Die Verpflichtungen und Zusagen von Phoenix gegenüber seinen Kunden haben für das Unternehmen höchste Priorität. „Wir haben einen umfassenden Onboarding-Prozess für unsere strategischen Anbieter“, erklärt Laura Banks, Data Protection Specialist bei Phoenix.

Herausforderungen

Als preisgekrönter Anbieter von IT-Lösungen und Managed Services arbeitet Phoenix Software nur mit renommierten Anbietern zusammen, die höchste Qualität bieten. Wann immer es möglich ist, testen die IT-Teams des Unternehmens künftige Lösungen in ihrer eigenen Umgebung, bevor sie Kunden angeboten werden. Während dieses Prozesses erweisen sich einige wenige Tools als so wertvoll, dass sie schließlich Teil des unternehmenseigenen IT-Technologie-Stacks werden.

Lösung

Phoenix prüfte die von Quest angebotenen Sicherheits- und Cyber-Resilience-Lösungen für Active Directory sorgfältig – und die Lösungen bestanden sämtliche Tests mit Bravour. Seitdem verlassen sich auch die internen IT-Teams von Phoenix bei einer Vielzahl von Anwendungsfällen, etwa von der Erkennung von und Reaktion auf Bedrohungen bis hin zur Notfallwiederherstellung, auf Tools von Quest.

Ergebnisse oder Vorteile

- Blockierung von Bedrohungen, indem es Änderungen an wichtigen Administratorkonten, GPOs und anderen Objekten verhindert
- Verbesserung der AD-Sicherheit mit effektiver Gruppenrichtlinien-Governance
- Sicherstellung von Cyber Resilience durch Verkürzung der erforderlichen Zeit für die Notfallwiederherstellung von mehreren Tagen auf nur ein oder zwei Stunden
- Erleichterung der Einhaltung von Vorschriften und Verträgen durch automatisierte Aufgaben für die Privilegienverwaltung

„Wenn ich in unserem Portfolio eine Möglichkeit für eine neue Lösung sehe, wird diese von unserem technischen Team geprüft und getestet. Bevor wir das Produkt anbieten, muss dieses Team sagen: ‚Ja, das ist das Beste, was es auf dem Markt für diesen Bedarf gibt.' Wir nehmen nur die besten Anbieter und Lösungen auf."

Der Einsatz dieser Lösungen im eigenen Unternehmen, wann immer dies möglich ist, bietet darüber hinaus zahlreiche Vorteile. „Es ist uns sehr wichtig, die von uns verkauften Tools auch innerhalb unseres Unternehmens einzusetzen", erklärt Shaun Tosler, Infrastructure and Security Manager bei Phoenix. „Natürlich können wir das nicht mit allem machen, aber wenn eine Lösung für uns gut funktioniert, können wir darauf vertrauen, dass sie auch für unsere Kunden gut funktioniert. Außerdem können unsere Teams dadurch Erfahrung mit den von uns angebotenen Tools sammeln, sodass wir Kunden, die sie einsetzen, besser unterstützen können."

Als Quest Platinum Partner hatte Phoenix die Möglichkeit, die von Quest angebotenen Sicherheits- und Wiederherstellungslösungen für Active Directory zu testen. Diese Lösungen haben nicht nur die Kriterien für die Aufnahme in das Portfolio des Unternehmens erfüllt, sondern sich auch als so wertvoll erwiesen, dass sie nach wie vor wichtige Bestandteile des IT-Ökosystems von Phoenix sind. Gemeinsam tragen Change Auditor, GPOADmin und Recovery Manager for Active Directory Disaster Recovery Edition von Quest und One Identity Active Roles dazu bei, dass Phoenix umfassende Active Directory-Sicherheit und Cyber Resilience gewährleisten kann.

Change Auditor bietet eine fortschrittliche Bedrohungserkennung – und kann Angreifer sogar komplett stoppen

Change Auditor ermöglicht Phoenix die Bedrohungsüberwachung in Echtzeit sowie eine Sicherheitsanalyse aller wichtigen Benutzeraktivitäten und Änderungen durch Administratoren. „Für Sicherheits-Auditierung ist Microsoft Sentinel unser wichtigstes Tool", erklärt Tosler. „Aber wir halten es nicht für klug, alles auf eine Karte zu setzen, indem wir nur ein einziges Tool für wichtige Funktionen nutzen. Was ist, wenn es einen Fehler macht oder kompromittiert wird? Change Auditor ist daher eine wichtige sekundäre Informationsquelle. Außerdem liefert es aufgrund seiner Position in der technischen Struktur von AD noch mehr wertvolle Informationen, die in den nativen Protokollen nicht erfasst werden."

Noch begeisterter ist Phoenix von der Fähigkeit von Change Auditor, unerwünschte Änderungen an wichtigen Objekten zu blockieren, wie z. B. an leistungsstarken administrativen Konten und wichtigen Gruppenrichtlinienobjekten (GPOs). „Change Auditor stoppt Angreifer, die versuchen, geschützte Objekte zu verändern – ganz gleich, welche Berechtigungen sie haben", sagt Tosler. „Es ist unser Sicherheitsnetz gegen Privilegieneskalation und AD-Fehlkonfigurationen. Wir können beispielsweise festlegen, dass ein bestimmtes Konto überhaupt nicht verändert werden kann oder dass es sich nur von einem bestimmten IP-Adressbereich aus bearbeiten lässt. Wenn zum Beispiel jemand versehentlich alle Konten zu Domänenadministratoren macht, ist das egal, denn Change Auditor blockiert und verweigert kritische Änderungen."

Mit Change Auditor ist Phoenix in der Tat besser in der Lage, Bedrohungen sofort zu erkennen und darauf zu reagieren. „Wenn ein Angreifer mit Change Auditor in unser AD eindringen würde, würden zwei Dinge passieren", erklärt Tosler. „Erstens erregt er mehr Aufmerksamkeit, sodass unsere anderen Sicherheits-Tools ihn noch besser erkennen können. Und zweitens: Selbst wenn es dem Angreifer gelungen ist, unsere primäre Protokollierungsquelle abzuschalten, protokolliert Change Auditor die Informationen dennoch. Kurz gesagt verschafft uns Change Auditor mehr Zeit und sorgt für eine bessere Erkennung und mehr Schutz in der gesamten Angriffskette."

> **Recovery Manager ist genial – es ist das einzige Tool, das den Aufbau von Domänencontrollern nach einem Notfall automatisiert. Jedes andere Sicherungs-Tool stellt einfach die Active-Directory-Datenbankdatei wieder her und überlässt Ihnen die dazugehörige Arbeit. Recovery Manager stellt nicht einfach nur einzelne Dateien wieder her – es automatisiert den gesamten Wiederherstellungsprozess. In nur ein oder zwei Stunden kann ich die gesamte Umgebung wiederherstellen. Ohne diese Lösung bräuchten wir dafür mehrere Tage.**
>
> *Shaun Tosler, Infrastructure and Security Manager, Phoenix Software*

GPOADmin ermöglicht eine effektive Gruppenrichtlinien-Governance

Gruppenrichtlinien spielen eine entscheidende Rolle bei der Sicherheit von Active Directory, und Phoenix nutzt GPOADmin, um seine GPOs effizient und effektiv zu verwalten. „GPOADmin macht es uns leicht, die Einführung von GPOs zu kontrollieren“, sagt Tosler. „Wenn wir eine Änderung bis zu einem bestimmten Zeitpunkt einführen müssen, müssen unsere Techniker nicht bis 1:00 Uhr morgens warten, um sie so zu implementieren, dass die Auswirkungen auf die Benutzer so gering wie möglich sind. Stattdessen können wir die Änderung vornehmen, die GPO erstellen und die Einführung so planen, dass sie unseren Anforderungen entspricht.“

Außerdem bietet GPOADmin eine robuste GPO-Änderungsverwaltung. „Tatsache ist, dass 99 % der Sicherheitslücken auf eine unzureichende Änderungsverwaltung zurückzuführen sind – jemand führt einfach eine Aktion durch, ohne dass ein entsprechender Prozess vorhanden ist“, bemerkt Tosler. „Wir verwenden die Genehmigungsfunktion in GPOADmin, um sicherzustellen, dass jede Änderung einer Person von einer anderen Person genehmigt werden muss. So können wir sowohl übereilte Fehler als auch böswillige Aktionen verhindern. Außerdem verfolgt GPOADmin jedes Ereignis und liefert detaillierte Informationen, sodass wir immer genau sehen können, was geändert wurde.“

Natürlich können auch bei den sorgfältigsten Prozessen Probleme auftreten – daher bietet GPOADmin erweiterte Rollback-Funktionen. „Selbst bei sorgfältigsten Tests und Genehmigungen ist es möglich, dass ein GPO eingeführt und erst danach ein Problem damit festgestellt wird“, erklärt Tosler. „Mit GPOADmin können wir die GPOs schnell und einfach auf einen früheren Zustand zurücksetzen, um die Sicherheit von Active Directory umgehend wiederherzustellen. Es ist sehr selten, dass ein Tool genau das tut, was es in Bezug auf die Kontrolle und Administration von Gruppenrichtlinien verspricht, aber GPOADmin setzt genau das um, und zwar ziemlich gut.“

Recovery Manager for Active Directory ist „genial“ und verkürzt die Wiederherstellungszeit von Tagen auf Stunden

Um die Cyber Resilience zu gewährleisten, bietet Recovery Manager effiziente und zuverlässige AD-Sicherungen, die durch den Verzicht auf überflüssige und riskante Komponenten wie Boot-Dateien weniger umfangreich sind. In der Tat hält Tosler es für „eines der besten Tools für AD-Sicherungen auf dem Markt“.

Die größten Stärken der Lösung sieht er jedoch bei der Wiederherstellung. „Recovery Manager ist genial – es ist das einzige Tool, das die Erstellung von Domänencontrollern nach einem Notfall automatisiert“, erklärt Tosler. „Jedes andere Sicherungs-Tool stellt einfach die Active-Directory-Datenbankdatei wieder her und überlässt Ihnen die dazugehörige Arbeit. Recovery Manager stellt nicht einfach nur einzelne Dateien wieder her – es automatisiert den gesamten Wiederherstellungsprozess. In nur ein oder zwei Stunden kann ich die gesamte Umgebung wiederherstellen. Ohne diese Lösung bräuchten wir dafür mehrere Tage. Außerdem können Sie damit Informationen wiederherstellen, die sich nicht einfach neu erstellen lassen. Das steigert den Mehrwert dieser Lösung exponentiell.“

> **Wir haben einen umfassenden Onboarding-Prozess für unsere strategischen Anbieter. Wenn ich in unserem Portfolio eine Möglichkeit für eine neue Lösung sehe, wird diese von unserem technischen Team geprüft und getestet. Bevor wir das Produkt anbieten, muss dieses Team sagen: ‚Ja, das ist das Beste, was es auf dem Markt für diesen Bedarf gibt.‘ Wir nehmen nur die besten Anbieter und Lösungen auf.**
>
> *Laura Banks, Data Protection Specialist*
> *Phoenix*

Auch wenn Phoenix noch nie eine Notfallwiederherstellung durchführen musste, gibt die Gewissheit, dass die schnellen Wiederherstellungsmöglichkeiten zur Verfügung stehen, dem Unternehmen Sicherheit. „Im Falle einer Domänenkompromittierung müsste ich über 1.000 Dinge nachdenken, und der CEO oder CTO würde mir Druck machen, weil das Unternehmen jede Sekunde Geld verlieren würde“, sagt Tosler. „Mit Recovery Manager weiß ich, dass ich nur einen Knopf drücken muss, um die Wiederherstellung in Gang zu setzen, unsere Identitäten wiederherzustellen und Services wie E-Mail wieder zu aktivieren. Die Lösung ist wirklich von unschätzbarem Wert.“

In der Tat würde Tosler Recovery Manager jedem Unternehmen empfehlen, dessen Active Directory durch einen Notfall ausgelöscht wurde, denn die Lösung würde sich wahrscheinlich sofort voll auszahlen. „Recovery Manager schafft eine solide Grundlage für die ersten Schritte der Wiederherstellung“, sagt er. „Angenommen, Sie haben Zehntausende von Benutzern – die manuelle Erstellung all dieser Konten könnte 10, 20 oder 30 Stunden dauern. Recovery Manager nimmt Ihnen die ganze Arbeit ab und automatisiert die Kontoerstellung. Das kann kein anderes Tool leisten. Durch die Zeit, die Sie in solchen Fällen sparen, zahlt sich die Lösung wahrscheinlich mehr als aus.“

Active Roles sorgt für mehr AD-Sicherheit durch ein vereinfachtes Identity Management

Für die Identitätssicherheit verwendet Phoenix Active Roles, das die Verwaltung und fein abgestufte Delegation von Privilegien über Active-Directory-Domänen und Entra ID-Tenants (früher Azure AD) von einer einzigen Konsole aus ermöglicht. Mit der rollenbasierten Zugriffskontrolle (Role-Based Access Control, RBAC) kann Phoenix das Least-Privilege-Prinzip streng durchsetzen.

„Active Roles bietet die Abstraktion, die wir für die Identitätssicherheit benötigen“, erklärt Tosler. „Wir müssen zum Beispiel unseren Service-Desk-Technikern keine Administrationskonten mehr zur Verfügung stellen, sondern leiten sie auf eine Weboberfläche weiter. Außerdem können wir Aufgaben wie die Gruppenverwaltung an Personen mit dem nötigen Fachwissen delegieren, z. B. an die Entwickler speziell angepasster Anwendungen. Und niemand außer den berechtigten Konten kann Änderungen direkt im AD vornehmen.“

Active Roles hilft Phoenix auch bei der Datensouveränitäts-Compliance, die sich aus Unternehmensverträgen und Vorschriften wie der DSGVO ergeben. „Unsere Mitarbeiter müssen auch im Urlaub auf ihre E-Mails zugreifen können, aber einige Kunden erlauben keine Datenverarbeitung außerhalb Großbritanniens“, sagt Tosler. „Active Roles bietet die Automatisierung, die wir brauchen, um diese Verträge zu erfüllen. Wir haben es einfach so eingerichtet, dass der Benutzer automatisch aus bestimmten Gruppen entfernt wird, wenn sein Urlaub beginnt, und wieder hinzugefügt wird, wenn er zurückkehrt. Daher müssen wir uns keine Sorgen machen, dass Benutzer Zugriffsrechte behalten, die sie nicht haben sollten.“

Eine Reihe von Lösungen, die zusammenarbeiten

So wertvoll jede Lösung für sich genommen auch ist – Phoenix weiß, dass sie zusammen einen noch größeren Nutzen bieten. „Wenn Sie Active Roles für das Identity Management einsetzen, können Sie auch Change Auditor für die AD-Sperrung einsetzen“, erklärt Tosler. „In ähnlicher Weise erstellt Recovery Manager Sicherungen, und Change Auditor überwacht sie und verhindert, dass jemand sie manipuliert. Mit dieser Art von Kontrollen kann ich darauf vertrauen, dass die Daten, die für die Wiederherstellung eines bestimmten Services erforderlich sind, zur Verfügung stehen, wenn ich sie brauche.“

PRODUKTE UND SERVICES

Produkte

- Change Auditor
- GPOADmin
- Recovery Manager for Active Directory Disaster Recovery Edition
- One Identity Active Roles

Lösungen

- Verwaltung von Microsoft-Plattformen

Über Quest

Quest stellt Softwarelösungen bereit, mit denen das volle Potenzial neuer Technologien in einer zunehmend komplexen IT-Landschaft ausgeschöpft werden kann. Von der Datenbank- und Systemverwaltung über die Migration zu und Verwaltung von Active Directory und Microsoft 365 bis hin zur Cyber Resilience: Quest hilft Kunden, bereits heute ihre IT-Herausforderungen von morgen zu bewältigen. Quest Software. Where Next Meets Now.

CaseStudy-Phhoenix-KA-DE-WL-87341