Bremer Bank

Die Bremer Bank hat sich für ForeScout CounterACT® und damit für Sichtbarkeit in Echtzeit, Gastzugang und automatisierte Verwaltung entschieden.

BRANCHE

Finanzen

UMGEBUNG

Ca. 1.900 Mitarbeiter in 87 Niederlassungen und Unternehmensstandorten und 4.200 Endpunkte

DIE HERAUSFORDERUNG

- Sicherstellen einer verlässlichen Methode, um Geräte zu klassifizieren und zu überwachen, die sich mit dem Unternehmensnetzwerk vom Unternehmenssitz oder von den mehr als 80 Niederlassungen der Bank aus verbinden
- Verbesserung der Abwehrmechanismen der Bank durch kontinuierliches Monitoring und Fehlerbehebung gegen die zunehmende Anzahl von Advanced Persistent Threats (APT)

DIE LÖSUNG

- Eine agentenlose Lösung, mit der die Bank nicht mehr auf ihre vorhandene komplizierte 802.1X-Infrastruktur angewiesen ist
- Installation und Betrieb ohne direkten Eingriff für eine unkomplizierte Integration in das vorhandene Cisco-Netzwerk der Bremer Bank
- Out-of-Box-Funktionalität für die automatische Erkennung von Geräten, Benutzern und Software, flexible Richtlinienmaßnahmen sowie Warnungen und Berichte

DIE ERGEBNISSE

- Umfassende Netzwerksichtbarkeit über sämtliche Endpunkte in Echtzeit
- Extrem schnelle und einfache Implementierung mit raschem Return of Investment
- Automatisierte Verwaltung und Registrierung von Gästen für eine Segmentierung des Gästedatenverkehrs vom internen Netzwerk des Unternehmens
- Verbesserte Compliance mit Sicherheitsrichtlinien ohne negative Auswirkungen für Endnutzer und Produktivität
- Automatisierte Isolierung von Geräten und gesendeten Warnungen, wenn Malware und schädliche Aktivitäten erkannt werden

Überblick

Die Bremer Financial Corporation ist ein privates Finanzinstitut, dessen Hauptanteilseigner die Otto Bremer Foundation und die Mitarbeiter der Bremer Bank sind und das über ein regionales Portfolio von 8,7 Milliarden US-Dollar verfügt. Die Bank wurde 1943 von Otto Bremer gegründet und deckt heute ein breites Spektrum von Privatkunden-, Investment-Banking-, Treuhand- und Versicherungsgeschäften und -Dienstleistungen in Minnesota, North Dakota und Wisconsin ab. Zu ihren Kunden gehören Privatpersonen und Familien, kleine und mittelständische Firmen, Agrarunternehmen, gemeinnützige Organisationen und öffentliche Einrichtungen und Regierungsinstitutionen.

Die Bank beschäftigt ca. 1.900 Mitarbeiter in ihren 87 Niederlassungen und Unternehmenssitzen und verfügt über 4.200 Endpunkte einschließlich Server. Das IT-Team der Bank ist verantwortlich für die Sicherheitsinfrastruktur sowie für das Design, die Implementierung und das Management der damit verbundenen Komponenten und Prozessen. Es arbeitet eng mit allen Geschäftsbereichen zusammen, speziell mit den Bereichen Informationssicherheit, Unternehmensarchitektur und der Geschäftsführung, um seine Maßnahmen stets mit der allgemeinen Strategie abzugleichen und gleichzeitig ein hohes Maß an Sicherheit zum Schutz von sensiblen Firmen- und Kundendaten zu wahren.

Die Herausforderung für das Unternehmen

Die Bremer Bank verfügte über eine vorhandene 802.1X-Network Access Control (NAC), um den Zufluss von verschiedenen Corporate- bzw. Endbenutzergeräten zu unterstützen, doch dafür waren große Supportanstrengungen nötig und das System war anfällig für Falschmeldungen und Unterbrechungen. Das IT-Team der Bremer Bank stieß auf erhebliche Schwierigkeiten beim Implementieren und bei der Wartung des Systems, für das zahlreiche Ausnahmen, vor allem an Außenstellen, konfiguriert werden mussten. Für die Implementierung waren Agenten erforderlich und es entstand ein hoher Verwaltungsaufwand bei 802.1X-Zugriffen. Darüber hinaus kam es zu nicht geplanten Ausfällen, die negative Auswirkungen auf die Benutzer und die Kunden der Bremer Bank hatten.

Um die Situation zu verbessern, begann das Bremer-Bank-Team nach einer neuen NAC-Lösung zu suchen, mit der sie die Netzwerksicherheit und Zugangskontrolle deutlich verbessern könnten. Die Bank zog eine agentenlose Lösung vor, um den Verwaltungsaufwand zu reduzieren, die Widerstandsfähigkeit des Systems und die Benutzererfahrung zu verbessern und gleichzeitig erhebliche Zeit- und Kosteneinsparungen für die IT zu erreichen.

Warum ForeScout?

Nach einer gründlichen Auswertung in Zusammenarbeit mit den Infrastruktursicherheitsexperten, den Netzwerktechnikern, der Unternehmensarchitekturabteilung und dem Informationssicherheitsteam, entschied sich Joseph Thornell – Netzwerkarchitekt und stellvertretender Vorsitzender der Technikabteilung bei der Bremer Bank – schließlich für ForeScout CounterACT® als NAC für die Bremer Bank aufgrund der einfachen Installation, der Managementfunktionen und dem außergewöhnlichen Angebot an Funktionen.

„Wir benötigten eine reibungslose, sichere Methode zum Identifizieren von Unternehmens-Assets und gleichzeitig eine sichere Zugriffsmethode für Mitarbeiter- und Gäste-Geräte“, so Thornell. „Zudem war es uns wichtig, unseren Benutzern eine gute Nutzererfahrung zu gewährleisten, besonders weil unsere vorherige Lösung für viel Frustration unter unseren Benutzern gesorgt hatte. Wir benötigten eine neue Lösung, um das negative Image wieder zu verbessern, das durch unsere vorherige Lösung entstanden war. ForeScout war da genau das Richtige und die Entscheidung dafür fiel schnell.“

> **„ForeScout CounterACT war sofort nach der Installation sehr wertvoll für uns. Durch die Fähigkeit, Informationen zu mehr als 4.000 Endpunkten zu sehen und zu sammeln, können wir unsere Netzwerksicherheit jetzt besser verwalten und kontrollieren. Nach der ersten Implementierung ist die Lösung mit uns gewachsen und wir haben einen deutlichen Mehrwert verspürt, als wir zusätzliche Funktionen in unsere Sicherheitsrichtlinien integrierten. – Ich bin gespannt, wohin wir uns damit in Zukunft bewegen. "**
>
> **— Joseph Thornell, Security Technical Architect, Bremer Bank**

Was hebt ForeScout von der Konkurrenz ab?

Zentrale Unterschiede, die zum allgemeinen Erfolg der Bremer Bank beitrugen:

- leichte Implementierung und einfaches Management der Lösung
- Sichtbarkeit in Echtzeit im gesamten Netzwerk
- Integration in Sicherheitsprodukte

Die Fähigkeit von ForeScout, für IT-Abteilungen einen umfassenden Überblick über die Geräte bereitzustellen, die sich mit dem Netzwerk verbinden, war ein entscheidender Punkt bei der Entscheidung der Bremer Bank, CounterACT zu implementieren. Die agentenlose Herangehensweise, die flexiblen Gäste-Managementfunktionen und die Segmentierungsoptionen waren zudem weitere wichtige Vorteile für die Bank. Darüber hinaus war die ControlFabric®-Technologie von ForeScout, die eine nahtlose Integration in andere Sicherheitslösungen ermöglicht, ein wichtiges Verkaufsargument, das ein bedeutender Faktor in der Kaufentscheidung der Bremer Bank wurde.

Die Auswirkungen für das Unternehmen

Die Bremer Bank implementierte CounterACT als Ersatz für die vorhandene 802.1X-Lösung. Dabei verlief die Umstellung zum neuen System schnell und reibungslos. Dank CounterACT unterstützt das Netzwerk der Bank aktuell alle Cluster seiner regionalen Niederlassungen und wird zentral vom Unternehmenssitz aus verwaltet. Die Bremer Bank verwendet derzeit ein CounterACT 4000 und ist gerade dabei, ein CounterACT 10000 hinzuzufügen, das voraussichtlich in Kürze in Betrieb genommen wird.

„Das neue, größere Modell wird 10.000 Geräte gleichzeitig unterstützten und wir werden die alte Hardware weiter nutzen, um eine Kontinuität in unseren Geschäftsabläufen zu gewährleisten", so Thornell. „Zudem planen wir, 1.000 zusätzliche Endpunkte zu unseren bestehenden 4.200 hinzuzufügen."

Vorteile, von denen die Bremer Bank nach der Implementierung von CounterACT profitieren konnte:

Sichtbarkeit und Transparenz in Echtzeit

Bei der Bremer Bank nutzen mehrere Geschäftseinheiten im gesamten Unternehmen die Funktion für Endpunkt-Sichtbarkeit von CounterACT. Die Bank nutzt ihre neu entdeckte Netzwerksichtbarkeit für Echtzeit-Bestandsdaten, und laut Thornell ist das Tracking durch ForeScout sehr genau, sodass sich die IT-Teams auf andere Aufgaben konzentrieren können. Zudem konnte die Bremer Bank diese Funktion nutzen, um alte Software auf den Systemen zu erkennen, was besonders hilfreich während der aktuellen Windows XP-Migration war.

„Die Netzwerksichtbarkeit in Echtzeit ist extrem hilfreich, um zu verstehen, was sich genau in unserem Netzwerk befindet", so Thornell. „Dies stellt sich als besonders effizient für unsere Niederlassungen heraus und gibt uns die Möglichkeit, festzulegen, was wir isolieren und wie wir migrieren müssen – wir können uns die durch CounterACT gesammelten Daten zunutze machen, um System-Upgrades zu rechtfertigen und zu bewerten."

Gäste-Management

CounterACT wird in den vier Hauptniederlassungen der Bremer verwendet, um Mitarbeitern und Gästen einen kabellosen Netzwerkzugriff zu bieten. Und während die anderen Niederlassungen der Bank Kiosksysteme über andere kabellose Anbieter unterstützen, wird jeder Endpunkt dennoch über die Abwehrmechanismen von CounterACT geroutet, um diese Systeme in ihrem eigenen Netzwerk zu segmentieren, Website-Zugriffsberechtigungen einzurichten sowie weitere Kontrollen bei Bedarf anzuwenden.

„Die Möglichkeit, unsere Geräte zu verwalten, während wir gleichzeitig andere Zugriffsoptionen für Gäste und Mobilgeräte von Mitarbeitern bereitstellen können, ist ein zentraler Faktor", sagt Thornell.

Erstellung und Durchsetzung von Richtlinien

Die Bremer Bank war mithilfe von CounterACT nicht nur in der Lage, individuelle Sicherheitsrichtlinien im gesamten Unternehmen zu erstellen, es konnte auch BYOD- und mobile Sicherheitsrichtlinien durchsetzen, indem nicht autorisierte Anwendungen identifiziert, eingeschränkt oder blockiert werden.

Eine weitere von der Bremer Bank verwendete individuelle Richtlinie besteht darin, Betriebssysteme sowie private und mobile Geräte zu klassifizieren.

ForeScout®

Erkennung und Isolierung von Malware und schädlichen Aktivitäten

Die Bremer Bank nutzt ForeScout CounterACT, um nicht unternehmens-eigenen und bedrohlichen Geräten den Netzwerkzugriff auf seine sensiblen IT-Ressourcen zu sperren. Die Bank nutzt zudem den Bedrohungsschutz von ForeScout, der einem IPS ähnelt, um Malware-Angriffe auf das Netzwerk abzuwehren. Darüber hinaus kann CounterACT dazu verwendet werden, um Hardware- und Softwareversionen wie Adobe Flash zu prüfen und veraltete und gefährdete Endpunkte daran zu hindern, sich mit dem Netzwerk zu verbinden.

Integration in Sicherheitsprodukte

Dank der ControlFabric-Technologie von ForeScout kann CounterACT Daten mit anderen IT-Systemen austauschen und ein breites Spektrum an Problemen beheben. Die Bremer Bank macht sich diese Möglichkeiten zunutze, indem sie CounterACT in ihre SIEM- und Antivirenlösungen von QRadar integriert.

Automatisierung, Zeit- und Kosteneinsparungen

Für die Bremer Bank führten die leichte Verwaltung und das im Vergleich zu ihrer vorherigen NAC-Lösung durch ForeScout verringerte Supportaufkommen zu weniger Anrufen und sparten dem IT-Team und dem Helpdesk erhebliche Zeit.

„Die Prozesse zur Klassifizierung von Assets sind nun wesentlich schneller“, so Thornell. „Unsere Mitarbeiter im Support sind in der Lage, umgehend unternehmenseigene von nicht unternehmenseigenen Assets zu unterscheiden und ein System erneut zu klassifizieren.“ „So wurden im Vergleich zu unserer alten 802.1X-Infrastruktur Zeit, Energie und Mühen gespart.“

Durch die Möglichkeit, den Benutzer und Switch-Port zu finden, hat die Automatisierung von CounterACT dabei geholfen, die Sicherheit deutlich zu verbessern. Vor der ForeScout-Implementierung musste in den meisten Fällen die Netzwerktechnik eine Switch-Ausnahme für den entsprechenden Benutzer und das Gerät erstellen. In diesem Fall stünde das Gerät nicht länger unter der NAC-Kontrolle, bis das System sowohl den Agenten als auch den Supplikanten wiederhergestellt hätte.

Da die Helpdesk-Mitarbeiter der Bremer Bank Zugang zu den Daten von CounterACT in Bezug auf Benutzer und Endpunkte haben, können Sie erhebliche Zeit und Mühe bei der Diagnose von Problemen einsparen. Alles in allem verzeichnete die Bank beachtliche Einsparungen aufgrund des verringerten Verwaltungsaufwands, der geringeren Anzahl von Supportfällen und dem zentralen Zugriff auf alle Funktionen, während das Unternehmen zuvor mehrere Leute und Systeme benötigt hatte, um diese Daten zu sammeln.

„Um die mithilfe von ForeScout erzielte Sicherheit und Sichtbarkeit zu erreichen, würden wir mehrere Systeme benötigen und stundenlang mit der Implementierung und Verwaltung dieser Systeme beschäftigt sein“, so Thornell.

Integration in Sicherheitsprodukte

Für die Bremer Bank ist CounterACT mehr als nur Network Access Control und die Bank gibt daher anderen Finanzinstituten, die eine NAC-Lösung implementieren möchten, folgenden Rat:

„Sichtbarkeit und Monitoring sind genauso wichtig wie die Durchsetzung von Richtlinien“, rät Thornell. „Wenn Sie im Überwachungsmodus stark auf Richtlinien setzen, können Sie eine erhebliche Anzahl von Daten vom System erhalten. Dabei entstehen so gut wie keine Auswirkungen für den Endbenutzer.“

Die Bremer Bank plant künftig ForeScout CounterACT zusätzlich zur Sicherung von Benutzer-Endpunkten auch auf andere Bereiche auszuweiten. Die Bank beabsichtigt zudem, weitere Sicherheits-lösungen über die ControlFabric-Technologie zu integrieren, einschließlich des Schwachstellenscans von Tenable, des kabellosen Zugangs für Mitarbeiter und Gäste, des Mobile Device Management (MDM), VMware und Data Loss Prevention (DLP) von RSA. Darüber hinaus will die Bank eine Endpunkt-Überwachungsrichtlinie mithilfe von Windows Server Update Services (WSUS) verwenden, um Patch-Levels für Berichte und manuelle Fehlerbehebung zu prüfen. Zudem beabsichtigen sie, die Richtlinien auszuweiten, um direkte Updates und durch WSUS aktivierte Updates zu ermöglichen.

„Die von uns über erreichte Sichtbarkeit in Bezug auf unsere Endpunkte und der von uns dauerhaft gewährleistete hohe Sicherheitsgrad waren bisher von unschätzbarem Wert“, so Thornell. „ForeScout CounterACT war sofort nach der Installation sehr wertvoll für uns. Die Möglichkeit, mehr als 4.000 Endpunkte zu sehen und zu verwalten ist sehr hilfreich. Wir sind gespannt auf die weiteren kontinuierlichen Vorteile, die wir durch unsere Implementierung erreichen.“

Weitere Informationen finden Sie unter **www.ForeScout.com**

ForeScout

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

Gebührenfrei (USA) 1.866.377.8771
Tel (intern) 1.408.213.3191
Support 1.708.237.6591
Fax 1.408.371.2284