ForeScout

KKB

KKB (Credit Bureau of Turkey) bewertet ForeScout CounterACT® als führend im Bereich der Informationssicherheit

BRANCHE

Finanzen

UMGEBUNG

300 Mitarbeiter und 400 Geräte in einer streng regulierten Umgebung

DIE HERAUSFORDERUNG

- Sicherstellen, dass alle Notebooks und Workstations, die mit dem Netzwerk verbunden sind, von rechtmäßigen Usern benutzt werden, die wirklich zum Unternehmen gehören.
- Automatisierung der Sicherheitskontrollen, um Risiken zu verringern und Reaktionen auf Sicherheitsvorfälle zu beschleunigen
- Vermeidung von Produktivitätsunterbrechungen

DIE LÖSUNG

- Eine leicht zu bedienende agentenlose Lösung, die geringstmöglichen manuellen Aufwand erfordert
- Schnelle Installation ohne direkten Eingriff, einfache Integration in das kombinierte Netzwerk von KKB aus kabellosen Zugangspunkten von Aruba und Cisco®-Switches
- Integration der FireEye®- und ArcSight™-Plug-ins in die ForeScout CounterACT-Plattform, um das Teilen von Sicherheitsinformationen zu ermöglichen und Endpunkt-Fehlerbehebungsmaßnahmen zu automatisieren
- Eine hochgradig verlässliche Netzwerksicherheitslösung, wobei der gespiegelte Datenverkehr an CounterACT weitergeleitet wird

DIE ERGEBNISSE

- Sichtbarkeit in Echtzeit and kontinuierliches Monitoring von Endpunkten im Netzwerk, wodurch das Potenzial von Cyber-Angriffen über bekannte Schwachstellen verringert wurde
- Automatisierung des lokalen Administratorpasswort-Managements für Geräte von Mitarbeiterinnen und Mitarbeiter außerhalb der Büroumgebung – so können einige Wochen Arbeitsaufwand pro Jahr eingespart werden
- Präventive Kontrolle von „Pass-to-Hash"-Angriffen
- Verbesserte Compliance im Rahmen von Bankgesetzen zur Informationssicherheit

Überblick

Kredi Kayit Burosu (KKB), das erste und bisher einzige Kreditinstitut in der Türkei, wurde 1995 von neun großen türkischen Banken gegründet. KKB verringert die finanziellen Risiken zahlreicher Branchen – einschließlich Banken, Autovermietungen, Haus- und Wohnungsvermietungen und Haushalte – und verfügt über eine Million Mitglieder, die regelmäßig das Internetportal nutzen. 2014 hatte das Unternehmen 500 Millionen Anfragen.

Die Herausforderung für das Unternehmen

Compliance und Cyber-Sicherheit sowie der Schutz sensibler finanzieller und persönlicher Daten sind für das Ansehen von KKB als vertrauenswürdiger Dienstleister von großer Bedeutung. In Übereinstimmung mit der Unternehmensethik von KKB benötigte das Unternehmen eine Lösung für umfassende Netzwerksichtbarkeit und -kontrolle für seine 300 Mitarbeiter und 400 Endpunkte.

Warum ForeScout?

Als KKB sich auf die Suche nach einer Lösung begab, die seine Netzwerksichtbarkeit und Sicherheitskontrolle verbessern sollte, ging KKB auf Symturk zu, den Partner des Unternehmens in Sachen Informationssicherheit. Symturk empfahl ForeScout CounterACT® und bot einen Proof of Concept (PoC) vor Ort für den Chef im Bereich Informationssicherheit/Risikomanagement bei KKB, Ali Kutluhan Aktaş, an. Cisco ISE wurde ebenfalls in Betracht gezogen.

Zu den Kriterien für die Auswahl zählten: schnelle Installation, Fähigkeit, eine gemischte Infrastruktur zu unterstützen (kabellose Zugangspunkte von Aruba und Cisco-Switches), eine ausfallfreie Lösung für die Kontinuität der Geschäftsabläufe sowie die Bereitstellung von weiteren automatisierten Aktionen und Compliance-Kontrollen. KKB traf seine Entscheidung, nachdem das Unternehmen die Produktdatenblätter und Referenzen beider Produkte verglichen.

Aktaş erklärt: „Wir entschieden uns für ForeScout anstelle der NAC von Cisco, da wir über eine gemischte Infrastruktur verfügen (nicht nur Cisco) und dennoch eine schnelle und einfach zu installierende Lösung benötigten. ForeScout bot uns genau das. Darüber ist CounterACT eine einzigartige Plattform mit herausragenden Integrationsmöglichkeiten. Die Tatsache, dass wir problemlos andere Sicherheitsprodukte, wie FireEye, ArcSight und CyberArk® integrieren konnten, gab uns eine erhöhte Sichtbarkeit und Cyber-Sicherheit innerhalb des gesamten Unternehmens. Zudem konnten wir auf die verknüpften Sicherheitsdaten der Produkte zugreifen und davon profitieren."

Die Auswirkungen für das Unternehmen

Sichtbarkeit in Echtzeit der Geräte und Schwachstellen

Seit der Implementierung von ForeScout CounterACT erreichte KKB eine deutlich höhere Sichtbarkeit der Endpunkte in seinem Netzwerk und ist zudem in der Lage, den Sicherheitsstatus jedes Geräts kontinuierlich zu überprüfen. „Wenn zuvor ein Portscan im Netzwerk durchgeführt wurde und dabei die Möglichkeit bestand, dass schädliche Aktivitäten auftreten würden, konnten wir dies nur dann registrieren, wenn es schon geschehen war", so Aktaş. „Mit ForeScout sind wir in der Lage, derartiges Verhalten zu erkennen, zu sehen und zu blockieren – und das gleichzeitig. Zudem warnt uns CounterACT vor Sicherheitsschwachstellen, sobald diese auftreten, während es uns gleichzeitig in die Lage versetzt, unsere Endpunkt-Fehlerbehebung zu automatisieren. So können wir mögliche menschliche Fehlerquellen reduzieren."

Wir benötigten eine NAC-Lösung, die wir schnell implementieren können ohne dabei Geschäftsausfälle zu riskieren. Zudem musste diese unsere gemischte Aruba- und Cisco-IT-Infrastruktur unterstützen. ForeScout CounterACT bot und all das und noch vieles mehr – einschließlich atemberaubender Integrationsfunktionen mit unseren bestehenden Sicherheitstools von FireEye und ArcSight. Aus diesem Grund nennen wir CounterACT das ‚Schweizer Taschenmesser' unserer Informationssicherheitsabteilung, da es mehrere automatisierte Sicherheitsüberprüfungen und Compliance-Kontrollen äußerst effizient ermöglicht."

– Ali Kutluhan Aktaş, Head of Information Security/Risk Management bei KKB

Erstellung und Durchsetzung von Richtlinien

Aktaş erläutert einige der benutzerdefinierten Sicherheitsrichtlinien, die sein Unternehmen mithilfe von CounterACT erstellt hat:

- „Wir integrierten ForeScout-ArcSight-CyberArk, sodass ForeScout jedes Mal, wenn sich ein Computer oder Laptop mit unserem Netzwerk verbindet, dessen lokales Administrationsalter prüft. Und wenn es höher als 45 Tage ist, sendet ForeScout eine CEF-Nachricht mit dem Namen des Geräts an ArcSight. ArcSight wiederum korreliert diese Nachricht innerhalb unserer benutzerdefinierten Regel und startet ein Skript auf einem Agent, der auf dem CyberArk-Server installiert ist. Mit diesem Skript startet CyberArk den Passwort-Änderungsvorgang und das Passwort wird erfolgreich geändert. Dies ist eine essentielle Sicherheitsmaßname, speziell für diejenigen Mitarbeiter, die regelmäßig außerhalb des Bürogeländes arbeiten."
- „Mithilfe von ForeScout CounterACT überprüfen wir die Domain-Administrator-Anmeldehashcodes auf Client-Maschinen und wenn wir eine Domain-Administratoranmeldeinformation/oder einen Hashcode auf einer Workstation finden, isolieren wir die Maschine vom Netzwerk. So garantieren wir eine präventive Kontrolle von „Pass-to-Hash"-Angriffen. Darüber hinaus überprüfen wir lokale Administratoreinstellungen auf Workstations: Wenn der Helpdesk eine nicht genehmigte lokale Administratoreinstellung an einen Mitarbeiter vergibt, erkennen wir diesen Endpunkt und isolieren ihn."
- „Über CounterACT überprüfen wir Data-Loss-Prevention-Dienste und wenn diese nicht funktionieren senden wir einen Befehl, um sie dreimal auszuführen. Wenn diese dann noch immer nicht funktionieren oder überhaupt nicht installiert sind, isolieren wir das Gerät. Zudem prüfen wir auch Elemente wie Festplattenverschlüsselung, P2P-Programme, verdächtiges Verhalten und Antiviren-Scanfrequenzen."

Verringerung des manuellen Aufwands

Eines der Auswahlkriterien von KKB war die Optimierung von automatisierten Sicherheitskontrollen, um den manuellen Aufwand und die damit verbundenen Risiken zu minimieren. „Vor dem Einsatz von ForeScout mussten wir Passwörter auf unseren Notebooks und Workstations manuell ändern. Wenn beispielsweise ein Mitarbeiter das Unternehmen verließ, nahm dies viel Zeit in Anspruch", so Aktaş. „Über CounterACT haben wir eine benutzerdefinierte Richtlinie erstellt, die ForeScout mit ArcSight und CyberArk verbindet, sodass der Prozess jetzt automatisiert ist. So sind wir in der Lage, Geld zu sparen und gleichzeitig eine verbesserte Informationssicherheit zu gewährleisten. Angesichts der proaktiven Herangehensweise und der Automatisierung des Vorgangs gehe ich davon aus, dass wir mehrere Arbeitswochen pro Jahr sparen."

Integration von Sicherheitsprodukten

Dank der ControlFabric-Technologie von ForeScout kann CounterACT Daten mit anderen IT-Systemen austauschen und ein breites Spektrum an Problemen beheben. KKB nutzt diese Fähigkeiten, indem es seine Lösungen von FireEye und ArcSight in CounterACT integriert.

Die ForeScout-FireEye-Integration ermöglicht ein Monitoring in Echtzeit und verringert Unternehmensrisiken in Bezug auf nicht regelkonforme oder gefährdete Endpunkte. Advanced Persistent Threats, Botnetze und sich verbreitende Malware in dezentralen und BYOD-Umgebungen können schnell identifiziert, verifiziert und unter Quarantäne gestellt werden.

Dank der Interoperabilität von ForeScout mit dem ArcSight-SIEM (Security Information and Event Management) bietet es detailliert Informationen über den Sicherheitsstatus von Endpunkten, wodurch bessere, schnellere und gründlicher durchdachte Entscheidungen in Bezug auf Sicherheitsrisiken und Compliance-Verletzungen rund um Endpunkte getroffen werden können.

Was hebt ForeScout von der Konkurrenz ab?

Zentrale Unterschiede, die zum allgemeinen Erfolg von KKB beitrugen:

- Integration von Sicherheitsprodukten über die ControlFabric-Architektur
- mühelose Implementierung/ Interoperabilität in Umgebungen mit einer Vielzahl von Anbietern
- kontinuierliches Monitoring und Schadensminderung von Sicherheitsschwachstellen und Cyber-Angriffen
- Sichtbarkeit in Echtzeit der Geräte im Netzwerk
- automatisierte Sicherheits- und Compliance-Kontrollen; verringerter manueller Aufwand

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

ForeScout®

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