regio iT erhöht Performance und Schutz mit Firewalls von Palo Alto Networks™

BACKGROUND

Der IT-Dienstleister regio iT ist ein Partner für Städte und Kommunen. Mit Standorten in Aachen und Gütersloh unterstützt regio iT rund 320 Kunden und betreut 20.500 Clients aus dem kommunalen Umfeld bei Herausforderungen mit der rasanten IT-Entwicklung und zunehmendem Kostendruck. Mit derzeit 340 Mitarbeitern übernimmt regio iT den Betrieb und die Betreuung von Datenbank- und Server-Systemen sowie der gesamten IT-Infrastruktur bei Energie- und Entsorgungsunternehmen, Schulen und Non-Profit-Organisationen und verwaltet die Daten von Bürgerinnen und Bürgern in der Region.

DIE HERAUSFORDERUNG EINER NEUEN FIREWALL

Der IT-Dienstleister regio iT ist ein Partner für Städte und Kommunen. Mit Standorten in Aachen und Gütersloh unterstützt regio iT rund 320 Kunden und betreut 20.500 Clients aus dem kommunalen Umfeld bei Herausforderungen mit der rasanten IT-Entwicklung bei zunehmendem Kostendruck. Mit derzeit 340 Mitarbeitern übernimmt regio iT den Betrieb und die Betreuung von Datenbank- und Server-Systemen sowie der gesamten IT-Infrastruktur bei Energie- und Entsorgungsunternehmen, Schulen und Non-Profit-Organisationen und verwaltet die Daten von Bürgerinnen und Bürgern in der Region. Die daraus resultierende Verantwortung nimmt regio iT sehr ernst – als erstes kommunales Rechenzentrum ist das Unternehmen daher nach den wichtigen international gültigen Standards ISO 9001 (Qualitätsmanagement), ISO 20000 (IT Service-Management) und ISO 27001 (Informationssicherheitsmanagement) zertifiziert.

Um den eigenen Qualitätsanforderungen gerecht werden zu können, überprüft regio iT den Status dieser Standards regelmäßig in internen und externen Audits. Ounsal Ouzeir, Leiter Team IT-Infrastruktur bei regio iT: „Mit dem neuen Konzept sollte ein serviceorientierter Ansatz verfolgt werden, damit das Bedürfnis der Kunden nach mehr Sicherheit ihrer Daten noch besser abgedeckt werden kann. Also haben wir als Grundvoraussetzung definiert, dass das neue Konzept in jedem Fall unterschiedlichen Sicherheitsanforderungen gerecht werden soll. Neben Firewalls, einer zentralen Protokollierung, Überwachung und Verwaltung mussten identifizierbare Zugriffe über Zertifikate von Endgeräten und Nutzern durch das Netz unterstützt und verwaltet werden können."

regio iT hatte sich im Vorfeld über verschiedene Firewall-Hersteller nach einer für sie geeigneten Lösung erkundigt, jedoch keine entsprechende Ausführung gefunden. Im Zuge eines erfolgreich durchgeführten Storage-Projekts wandte sich regio iT an die DTS Systeme GmbH, die seit dem Jahr 2000 eine auf Security spezialisierte Abteilung führt und zudem über mehr als 29 Jahre Erfahrung in der IT-Branche verfügt. Die DTS Systeme GmbH ist ein auf Systemintegration und Cloud Services spezialisierter Anbieter mit bundesweit sechs Standorten und zwei eigenen leistungsstarken Rechenzentren in Herford und Münster. Im April 2011 präsentierte DTS Systeme GmbH den Projektverantwortlichen von regio iT verschiedene Lösungsszenarien von Palo Alto Networks und einem weiteren Hersteller.

regio iT

ORGANISATION:
regio iT

BRANCHE:
Government / Non-Profit

HERAUSFORDERUNG:
Mit einem neuen Sicherheitskonzept sollte ein serviceorientierter Ansatz verfolgt werden, damit das Bedürfnis der Kunden von regio iT nach mehr Sicherheit ihrer Daten noch besser abgedeckt werden kann. Neben Firewalls, einer zentralen Protokollierung, Überwachung und Verwaltung sollten identifizierbare Zugriffe über Zertifikate von Endgeräten und Nutzern durch das Netz unterstützt und verwaltet werden können.

LÖSUNG:
Die Implementierung von je zwei PA-5020 sowie zwei PA-5050 Appliances, um die installierte Perimeter Firewall zu ersetzen und eine separate Firewall für die interne Segmentierung der Kundennetze aufzubauen.

ERGEBNIS:
regio iT ist in der Lage, potenzielle Threats zu erkennen, die das bereits implementierte Konkurrenzprodukt nicht hinreichend aufgezeigt hatte. Mithilfe der Identifizierung des Inhalts konnte in den beiden Bereichen Perimeter und Data Center ein erheblich höherer Schutz erzielt werden, als mit klassischen Firewall-Technologien. Gleichzeitig erhält die IT-Abteilung anhand des zusammengeführten Loggings der Firewall von Palo Alto Networks und IPS-Logs deutlich mehr Transparenz. Darüber hinaus lässt sich die Firewall auch virtualisieren, so dass auf Wunsch einzelner Kunden ein eigenes virtuelles System zur Verfügung steht.

paloalto NETWORKS
the network security company™

„Wir sind sehr zufrieden mit der Lösung. Damit waren wir von Anfang an in der Lage, potentielle Threats zu erkennen, die das bereits implementierte Konkurrenzprodukt nicht hinreichend aufgezeigt hatte. Mithilfe der Identifizierung des Inhalts konnte in den beiden Bereichen Perimeter und Data Center ein erheblich höherer Schutz erzielt werden, als mit klassischen Firewall-Technologien."

Andreas Pelzner
technischer Leiter und CIO
regio iT

Markus Kohlmeier, Leiter IT-Infrastructure & Security bei DTS Systeme GmbH: „Mit der Technologie von Palo Alto Networks entsteht ein Rechenzentrum, das die Standorte effektiv voneinander trennt. Palo Alto Networks favorisiert das Konzept des logischen Perimeters, welcher den notwendigen Rahmen zur Verfügung stellt, um einen standardisierten und konsistenten Sicherheitsanspruch unabhängig von der Netzwerkanbindung und vom Standort zu gewährleisten. Regeln und Policies bleiben konsistent und werden, bei bestmöglicher Intelligenz und Netzwerksicherheit, netzwerkübergreifend angewendet."

Bei einem Folgetermin wurden auf Wunsch von regio iT die Lösungen der beiden Firewall-Hersteller vor Ort demonstriert. Palo Alto Networks hatte die Nase vorn, dank der überzeugenden Technologie und einem plausiblen Kostenrahmen.

Wie üblich implementierte DTS Systeme eine Palo Alto Networks-Teststellung bei regio iT. „Die Ergebnisse waren beeindruckend", erinnert sich Ounsal Ouzeir. „Bereits zwei Stunden nach Beginn der Test-Installation hat das Palo Alto Networks-System schon die ersten Threats erkannt, die das bestehende Intrusion Prevention System (IPS-System) nicht hinreichend identifiziert hatte. Das IPS-Modul von Palo Alto Networks schützt vor Schwachstellen beziehungsweise Exploits und erkennt sowohl bekannte als auch unbekannte Sicherheitslücken in der Netzwerk- und Anwendungsschicht. Es verhindert Pufferüberläufe sowie Denial-of-Service-Attacken und blockiert Port Scans." Zu weiteren Testzwecken erhielt regio iT die Lösung für zusätzliche vier Wochen.

Im August 2011 wurden schließlich mehrere Palo Alto Networks-Firewalls innerhalb der Netzwerkinfrastruktur von regio iT implementiert. Dabei übernehmen die Firewalls hauptsächlich das Steuern der Kommunikationswege sowie die Prüfung auf Threats. DTS Systeme verantwortete dabei die gesamte Implementierung - von der Einbindung des Setups der Systeme mit einer Schulung über die Beratung und Unterstützung bei der Migration der Regelwerke bis hin zum Remote Support.

INTELLIGENTE SEGMENTIERUNG DER NETZE UND APPLIKATIONSKONTROLLE

Achim Kraus, Senior Systems Engineer bei Palo Alto Networks: „Die Architektur moderner Rechenzentren muss eine strikte Trennung zwischen öffentlichen, nicht öffentlichen und sogar geheimen Bereichen ermöglichen. Web-Server, die einen Zugriff von außen erlauben, müssen beispielsweise durch Firewalls von allen Firmendaten abgeschottet werden. Mail-Server gehören ebenfalls in das öffentliche Segment und sollten gesondert geschützt werden. Durch die Sende- und Empfangsfunktion verbinden sie vertrauenswürdige und nicht-vertrauenswürdige Bereiche. Die Segmentierung kann natürlich auch nach funktionalen Kriterien erfolgen."

Diese intelligente Segmentierung gelingt durch umfassende Applikationskontrollen, mit deren Hilfe sehr einfach ein optimales Regelwerk aufgesetzt werden kann. Die Funktion vereinfacht die Administration des Regelwerks der Firewall. Die Applikationskontrolle ist auch in der Lage, unerwünschte Kommunikation zu unterbinden. Klassische Firewalls können dies nicht gewährleisten. Mithilfe von bis zu vier verschiedenen Mechanismen zur Klassifizierung des Datenverkehrs identifiziert die Funktion App-ID, welche Anwendungen im Netzwerk ausgeführt werden – unabhängig von Port, Protokoll, SSL-Verschlüsselung oder möglichen Umgehungsmethoden. Die eindeutige Identifizierung der Anwendung ist die erste Aktion der

Firewall und wird anschließend als Basis für weitere Entscheidungen innerhalb des Regelwerks herangezogen. Neben der Identifizierungstechnik App-ID verwendet die Firewall von Palo Alto Networks auch „Content-ID“. Ein stream-basiertes Überprüfungsmodul erkennt und blockiert Bedrohungen und begrenzt nicht autorisierte Übertragungen von Dateien und vertraulichen Daten. Gleichzeitig kontrolliert eine URL-Datenbank die Internetnutzung.

Die Wiederherstellung von Transparenz und Kontrolle über die Nutzung von Anwendungen ist jedoch nur ein Teil der heutigen Herausforderung an IT-Abteilungen. Die Prüfung des zulässigen Datenverkehrs wird zur nächsten wichtigen Aufgabe. Hierzu ist ein Modul zur Erkennung von Sicherheitsrisiken nahtlos in die Firewall integriert. Die Erkennung beruht auf Signaturen und kombiniert diese mit einem stream-basierten Scan, um Sicherheitslücken, Viren und Spyware in einem einzigen Durchlauf zu blockieren.

„Wir konnten mit der Konsolidierung der Firewalls Kosten senken, den Zeitaufwand der Administration deutlich reduzieren und die Flexibilität auf Kundenanforderungen erhöhen. Gleichzeitig wurde die Sicherheit für unsere Kunden verbessert.“

Andreas Pelzner
technischer Leiter und CIO
regio iT

FAZIT

Andreas Pelzner, technischer Leiter und CIO der regio iT zieht eine positive Bilanz: „Wir sind sehr zufrieden mit der Lösung. Damit waren wir von Anfang an in der Lage, potenzielle Threats zu erkennen, die das bereits implementierte Konkurrenzprodukt nicht hinreichend aufgezeigt hatte. Mithilfe der Identifizierung des Inhalts konnte in den beiden Bereichen Perimeter und Data Center ein erheblich höherer Schutz erzielt werden, als mit klassischen Firewall-Technologien. Gleichzeitig erhält man anhand des zusammengeführten Loggings der Firewall von Palo Alto Networks und IPS-Logs deutlich mehr Transparenz. Unsere Marktanalyse ergab, dass Palo Alto Networks der einzige Anbieter ist, der die geforderten Leistungsdaten mit Applikationskontrolle und Threat Prevention zur Verfügung stellen kann. Dies hat besonders im Datacenter-Umfeld eine große Relevanz. Unseren Kunden können wir durch die strikte Trennung von öffentlichen und nicht öffentlichen Bereichen eine größtmögliche Sicherheit bieten.“ Darüber hinaus lässt sich die Firewall auch virtualisieren, sodass auf Wunsch einzelner Kunden ein eigenes virtuelles System zur Verfügung steht. Das ist beispielsweise notwendig, wenn der Kunde seine Logfiles und Regelwerke auditieren lassen muss oder sein Regelwerk einsehen und eigenständig verwalten möchte. All diese Funktionalitäten haben einen positiven Nebeneffekt: „Wir konnten mit der Konsolidierung der Firewalls Kosten senken, den Zeitaufwand der Administration deutlich reduzieren und die Flexibilität auf Kundenanforderungen erhöhen. Gleichzeitig wurde die Sicherheit für unsere Kunden verbessert“, so Andreas Pelzner.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com