

BeteiligungsHolding Hanau konsolidiert kommunale Security-Infrastruktur mit Fortinet-Lösungen

Auf den Säulen von mehr als 20 städtischen Unternehmen und Eigenbetrieben ruht das Dach der BeteiligungsHolding Hanau GmbH. Die Handlungsfähigkeit der Politik in wirtschaftlich schwierigen Zeiten zu sichern, war 2003 Anlass, die Holding als neue städtische Muttergesellschaft zu gründen. Damit sollte das wirtschaftliche Betätigungsfeld der Kommune strukturiert und die Verwaltung der städtischen Gesellschaften und Betriebe gesichert werden. Die BeteiligungsHolding Hanau vereint deshalb alle klassischen Funktionen einer Konzernmutter: IT-Dienstleistungen, modernes Berichtswesen und Controlling, Revision und Finanzmanagement, Steuern und Recht, Presse- und Öffentlichkeitsarbeit. Auch die Bereitstellung und das Management des kommunalen Rechenzentrums, einschließlich Wartung und Helpdesk für die IT-Systeme, fällt in die Zuständigkeit der Holding.

Die Herausforderung:

Reduzierung der Betriebskosten, Transparenz und einheitliche Infrastruktur

Als zentraler Knotenpunkt für die verschiedenen Gesellschaften und Betriebe der Holding wie die Baugesellschaft Hanau, das städtische Klinikum, die Hanauer Straßenbahn und die Stadtwerke muss die BeteiligungsHolding Hanau den unterschiedlichen Anforderungsprofilen der einzelnen Unternehmen gerecht werden. Als IT-Dienstleisterin setzt die Holding deshalb auf Homogenität bei den Strukturen, um mit einem einheitlichen und effizienten IT-Konzept ohne großen Managementaufwand die individuellen Bedürfnisse der Betriebe zu erfüllen.

Bei der Security stieß die Holding jedoch mit der Zeit an ihre Grenzen. „Es waren zu viele verschiedene Security-Komponenten im Einsatz, um wirklich effizient in allen Bereichen agieren zu können“, erklärt Janko Schiebeck, Leiter des IT-Service-Centers bei der BeteiligungsHolding Hanau GmbH. „Wir hatten etwa Mailfilter von GWAVIX und Firewall-Lösungen von Checkpoint, Astaro und Securepoint aus den verschiedenen Betrieben der Holding im Einsatz. Diese Heterogenität war nicht nur verwaltungstechnisch ineffizient. Wir waren auch mit der Performance einzelner Systeme nicht mehr zufrieden, so dass wir nach einer konsolidierten Lösung gesucht haben.“ Zudem erwiesen sich die Betriebs- und Lizenzkosten sowie Schulungs- und Managementaufwendungen für die verschiedenen Systeme als zu hoch und daher unrentabel für die Holding im Vergleich zu einer einheitlichen Lösung.

Gesucht wurde nach einer neuen, transparenten Lösung, die die Betriebskosten reduziert, die Bedienbarkeit und das Management der Security-Systeme vereinfacht, eine einheitliche Infrastruktur liefert und direkten Herstellersupport sowie Vor-Ort-Service gewährleistet.

Die Lösung:

Konsolidierung der IT-Infrastruktur auf FortiGate- und FortiMail-Cluster

Nach Evaluierung verschiedener Lösungen – unter anderem von Checkpoint, Astaro und ECOS – fiel die Wahl letztlich auf FortiGate- und FortiMail-Appliances von Fortinet. „Die Systeme haben nicht nur ein sehr gutes Preis-Leistungs-Verhältnis, auch liefert uns die FortiGate die beste konsolidierte Lösung mit allen für uns relevanten Services, einschließlich Firewall, VPN, Antispam, Webfilter, IDS und Gateway-Antivirus-Funktion“, erklärt Schiebeck.

Bevor die Fortinet Appliances installiert wurden, hatte die Holding eine einstufige Paketfilter-Firewall, Spamfilter, Web- bzw. Contentfilter und Gateway Antivirus von verschiedenen Herstellern im Einsatz. Das erhöhte den Administrationsaufwand und das Management erheblich und führte schließlich dazu, dass kein durchgängiges und einheitliches Security-Konzept mehr gegeben war. In einem Workshop wurde daher gemeinsam mit dem Fortinet Vertriebspartner, der das Projekt betreute, die passende Lösung ermittelt – zwei FortiGate-1000A Appliances, zwei FortiMail-400 Appliances und ein FortiAnalyzer-800B. Die FortiGate- und FortiMail-Systeme wurden als Cluster aufgesetzt, um die Ausfallsicherheit zu maximieren und die Einhaltung der vereinbarten Service Level Agreements (SLAs) mit den einzelnen Betrieben der Holding zu garantieren.

Aktuell managen die FortiGate- und FortiMail-Systeme etwa 1.600 User. FortiAnalyzer ist für die Aufzeichnung, Auswertung und Berichterstattung des Datentransfers der FortiGate- und FortiMail-Systeme zuständig. Durch die umfangreichen und individuell anpassbaren Reporting-Möglichkeiten von FortiAnalyzer können die Administratoren einfach und unkompliziert Aufzeichnungen filtern und überprüfen, einschließlich Datenverkehr, Viren, Bedrohungen, Internetinhalte und E-Mail-Daten.

Zwei Mitarbeiter sind bei der BeteiligungsHolding Hanau für Betrieb, Pflege und Wartung der Systeme zuständig. Durch die Installation der Fortinet Systeme konnte auch hier erheblich an Zeitaufwand gespart werden. Mittlerweile werden nur noch zwei bis drei Stunden pro Woche für die Administration benötigt. „Vorher waren das noch deutlich mehr“, weiß Janko Schiebeck. „Mit der Fortinet Lösung haben wir wirklich ein verlässliches Produkt von einem leistungsstarken Partner erhalten. Fortinet war zwar beim Kaufpreis nicht der günstigste Anbieter, hat uns aber durch das Gesamtangebot vollkommen überzeugt. Wir sind mit der neuen Lösung rundum zufrieden.“

Vorteile:

Vereinheitlichung sorgt für minimierte Ausfallzeiten und verbesserte Service Level

Mit der Konsolidierung der bestehenden Lösungen auf nur eine Plattform konnte die BeteiligungsHolding Hanau die Performance bei der Security deutlich steigern und so für mehr Sicherheit in den Einzelbetrieben sorgen. Mit der Einführung eines Intrusion Detection Systems (IDS) wird die Antivirus-Funktion der Fortinet Systeme zudem unterstützt, und die Spamfilter-Rate konnte damit beträchtlich erhöht werden.

„Auch Ausfallzeiten sind für uns kein Thema mehr“, so der Leiter des IT-Service-Centers Janko Schiebeck. „Da wir sowohl die FortiGate- als auch die FortiMail-Appliances als Cluster implementiert haben, sind unsere Ausfallzeiten gleich null. Mit unserer vorherigen Stand-alone-Lösung mussten wir bei einem Ausfall etwa mit vier Stunden rechnen, bis alles wieder lief. Jetzt springt einfach das andere System im Cluster ein und der Betrieb läuft weiter. Das ist natürlich eine enorme Verbesserung, und das merken auch unsere Kunden.“ Durch die Minimierung der Ausfallzeiten konnte die Holding ihre Service-Levels für die Einzelunternehmen wie Schulen, Klinikum und Stadtwerke steigern und kann nun zum Beispiel eine erhöhte Security für den Emailverkehr anbieten.

„In einem nächsten Schritt haben wir vor, mit FortiManager die IT-Security-Struktur nochmals zu optimieren und das Management weiter zu vereinfachen“, so Schiebeck. „Darüber hinaus sollen auch die Schulen und Kindertagesstätten, die **zum Wirkungsbereich der Holding zählen**, an unser zentrales Netz angebunden und mit kleineren FortiGate-Appliances abgesichert werden. Wir nähern uns also Schritt für Schritt einer einheitlichen Security-Infrastruktur. Für ein mittelständisches Unternehmen, wie wir es sind, kann das nur von Vorteil sein.“