STORMSHIELD

BUSINESS CASE

Erhöhung der Sicherheit von internen Netzwerken: eine Priorität für Kommunen

ÖFFENTLICHE INFRASTRUKTUR

Gemeindeverbände und Kommunen modernisieren sich um in einer zunehmend digitalen Welt neue vernetzte Dienstleistungen anbieten zu können. Was zwei Risiken birgt: die Gefahr, dass vertrauliche Informationen, die Kommunen verarbeiten, noch weiter offengelegt werden, und dass diese Dienstleistungen durch böswillige Personen kompromittiert oder unterbrochen werden.

Daher stellt sich die Frage, wie sie das Sicherheitsniveau ihrer Netzwerke steigern können, um die Kontinuität der Dienstleistungen zu gewährleisten und die Bürgerschaft vor Cyberangriffen zu schützen. Vor dieser Herausforderung stand auch ein Gemeindeverband in Deutschland mit 200.000 Einwohnerinnen und Einwohnern.

Kritische Infrastrukturen und schutzbedürftige vertrauliche Informationen

Um alle Versorgungsdienstleistungen (Elektrizität, Gas, Trinkwasser, Fernwärme…) und die öffentliche Infrastruktur (öffentliche Beleuchtung, Parkplätze, Schwimmbäder, Transportwesen…) zu verwalten und zu leiten, gründete dieser Gemeindeverband eine eigene Gesellschaft, die sich zu 100 % in seinem Besitz befindet.

Zusätzlich zur Umsetzung und zum laufenden Betrieb der angebotenen Infrastrukturen und Dienstleistungen wurde ein Webportal zur Verfügung gestellt, über das die Bürgerinnen und Bürger alle nützlichen Informationen erhalten und bestimmte Anträge mittels Webformularen stellen können.

Angesichts der Bedeutung seiner Aktivitäten und der Daten, die in seinem IT-System transportiert und gespeichert werden, war es unerlässlich für den Gemeindeverband, das Sicherheitsniveau zu steigern.

Ein höheres Sicherheitsniveau

Der Kunde entschied sich deshalb dazu, zusätzlich zu seinem vorhandenen Equipment eine zweite Firewall hinzuzufügen, um sein internes Computernetzwerk auf zweifache Weise zu schützen.

Da der Gemeindeverband gemäß der KRITIS-Verordnung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) als Betreiber einer „kritischen Dienstleistung“ eingestuft wird, ist er gesetzlich verpflichtet, sein Informationssystem, das für das Funktionieren der öffentlichen Dienstleistung unerlässlich ist, angemessen zu schützen. Dieser doppelte Schutz ist einer der verstärkten Sicherheitsbausteine, die eingeführt wurden, um die Betriebskontinuität zu gewährleisten.

In Bezug auf die neue Hardware wollte der Kunde nicht denselben Hersteller wählen, um mögliche Eindringungsversuche zu erschweren, da die Umgehung zweier unterschiedlicher Technologien schwieriger zu bewerkstelligen ist.

Auf Anraten ihres Integrators Phalanx IT fiel die Wahl auf die Lösung Stormshield Network Security, genauer gesagt auf einen Cluster aus SN6100-Firewalls, sowie auf die zentrale Verwaltungskonsole Stormshield Management Center.

Neben der Qualität und Performance der beiden Lösungen spielte auch die Tatsache eine Rolle, dass wir ein europäischer Anbieter sind und unsere Lösungen auf höchstem Niveau anerkannt und zertifiziert sind.

DIE MOBILE LÖSUNG

→ SN6100

→ Stormshield Management Center

(The Stormshield Management Center platform)

Performance und Funktionen, die den Kundenbedürfnissen entsprechen

Nachdem die zertifizierten Teams von Phalanx IT die Implementierung zur vollsten Zufriedenheit des Kunden durchgeführt haben, verfügt dieser nun über einen Firewall-Cluster der nächsten Generation, der alle Anforderungen des Gemeindeverbands an die Performance und Funktionalität erfüllt.

Die Hardware wurde für umfangreiche, kritische Infrastrukturen entwickelt und bietet einen Durchsatz von 170 GBit/s sowie die höchste Portdichte auf dem Markt. Dies ist unerlässlich, um zukünftigen Veränderungen der Sicherheitsanforderungen an die Netzwerkinfrastruktur einen Schritt voraus zu bleiben.

Der Kunde profitiert außerdem von hoher Verfügbarkeit und verbesserter Sicherheit durch eine Segmentierung seines Netzwerks und die Einführung strenger Regeln, die es ihm ermöglichen, den Traffic zu besonders kritischen Bereichen besser zu steuern. SN6100-Firewalls verfügen außerdem über redundante Komponenten (Netzteil und Lüfter) und garantieren somit einen unterbrechungsfreien Betrieb Ihrer Sicherheitslösung.

Ergänzend dazu kommt die zentrale Verwaltungslösung Stormshield Management Center zum Einsatz: Mithilfe dieses Tools kann der Gemeindeverband seine Aufgaben hinsichtlich der Überwachung, Konfiguration und Wartung der Firewalls optimieren.

Dieses Tool, das speziell auf die Bedürfnisse von Netzwerken mit mehreren Standorten zugeschnitten ist, spart nicht nur Zeit für Administratoren und minimiert die Fehlerwahrscheinlichkeit – es ist auch Teil derselben Logik, mit der sich der zukünftige Bedarf an Skalierbarkeit des Netzwerks antizipieren lässt.