

Die Axpo Group nutzt SecureTrack™ für das Firewall-Management



Das Unternehmen

Die Axpo Gruppe ist ein führendes Schweizer Energieunternehmen. Mit den Elektrizitätswerken der Nordost- und Zentralschweiz sowie ihren Partnern versorgt Axpo drei Millionen Menschen mit Strom.

Seit Herbst 2001 erbringt die Axpo Informatik AG Dienstleistungen in der technischen und kommerziellen Informatik für die Axpo Gruppe und die angeschlossenen Kantonswerke. Die Axpo Informatik AG mit Sitz in Baden ist mit regionalen Niederlassungen in Aarau, Beznau, Dietikon, Schaffhausen, Zürich und Genua vertreten. Als technisch hoch kompetente Serviceorganisation betreut die Axpo Informatik aktuell 3.500 Anwender sowie über 500 Applikationen in der Schweiz und in verschiedenen Orten innerhalb Europas.

Zusätzlich zu einem umfangreichen Spektrum betriebswirtschaftlicher, logistischer und technischer Systeme ist die Axpo Informatik auch für die Handelssysteme in der Schweiz, Frankreich, Italien und Österreich zuständig. Die oberste Anforderung hier lautet, eine höchstmögliche Sicherheit und Erreichbarkeit zu gewährleisten.

Das Umfeld

Auf das schnelle Wachstum der Axpo Gruppe müssen sich auch die IT-Security-Maßnahmen sehr flexibel und rasch einstellen. Um zügig neue Services – unter Einhaltung hoher Sicherheitsstandards – einrichten und bereitstellen zu können, hat die Axpo Informatik Teile der Firewall- und Server-Infrastruktur virtualisiert. Dadurch ist Axpo in der Lage, deutlich schneller als zuvor die Firewall für einen neuen Kunden zu konfigurieren. Axpo benötigte dazu eine Managementlösung, mit der sich sowohl virtuelle als auch physikalische Firewall-Architekturen administrieren lassen.

Die Firewall-Infrastruktur von Axpo Informatik basiert auf einem redundanten Crossbeam X40 Cluster; darauf läuft Check Point VPN-1 Power VSX. Dessen Firewall-Management besteht aus einem zentralen Check Point Provider-1 Server mit einem dedizierten Log-Server, der mit 29 virtuellen und physikalischen Firewall-Systemen zehn Kunden absichert. Unternehmenskritische Systeme sind als Hot-Standby-Cluster konfiguriert. Die Netzwerkverbindungen mit dem Crossbeam-System basieren auf VLAN- und Multi-Trunk-Technologie.

Die Herausforderung

Die Instandhaltung und der Betrieb von 29 Firewalls mit einer Vielzahl zu administrierender Objekte und den zugehörigen Sicherheitseinstellungen erforderten umfangreiche manuelle Eingriffe. Bei jeder Änderung mussten die Administratoren ermitteln, welche Kunden und welche Einstellungen betroffen sind, um dann jedes Objekt in jeder kundenspezifischen Konfiguration manuell zu ändern. Da viele Kunden die gleiche Infrastruktur nutzen, nahmen Komplexität und Risiken zu. Die drei Administratoren konnten zudem sehr schwer nachvollziehen, wer welche Änderung vorgenommen hatte und welche Auswirkungen sich daraus für den Sicherheitsstatus ergaben. Im Alltag war es daher nahezu unmöglich, die Sicherheitseinstellungen und die Datenbank mit den Objekten zu jedem Zeitpunkt konsistent und sicher zu halten.

Auch wenn die interne Managementplattform Informationen zentral speicherte, benötigte Axpo Informatik dennoch eine einheitliche Top-Down-Sicht auf die Security Policy. Konkret bestand der Bedarf nach einer Lösung, mit der Administratoren Kunden individuell betreuen können, während gleichzeitig jede Änderung an den Einstellungen koordiniert und freigegeben wird.

Die Lösung

Axpo entschied sich für die Firewall-Management-Lösung Tufin SecureTrack™ und hat heute einen umfassenden Überblick über die Firewall Policies aller Kunden und Objekte. Eine einheitliche grafische Benutzeroberfläche ermöglicht den Administratoren die Firewall Policy zu visualisieren, Änderungen einzusehen und entsprechende Maßnahmen zu ergreifen.

Das Firewall Change Management von SecureTrack erfüllt den Bedarf von Axpo Informatik an Verantwortlichkeiten und Konsistenz – und das Ganze verknüpft mit einer vollständigen zeitnahen

Nachvollziehbarkeit und Dokumentation der Änderungen. SecureTrack ermöglicht Axpo Informatik durch einen Abgleich aller Eingriffe mit einmal definierten Vorschriften Abweichungen und mögliche Sicherheitsrisiken rechtzeitig festzustellen, bevor ein Schaden eintritt.

Angesichts der vielen, komplizierten Sicherheitsregeln hatte sich im Laufe der Zeit ein solcher Wildwuchs ausgebreitet, dass die Einzelheiten kaum noch überschaubar waren. Axpo Informatik begann mit Hilfe der Cleanup- und Optimierungsfunktionen von SecureTrack alle nicht genutzten Regeln und Objekte aufzuspüren. Das Firewall-Administrations-Team konnte damit potenzielle Sicherheitslücken schließen und gleichzeitig die Performance und Ressourcenausnutzung steigern. Unter Anwendung der innovativen Policy-Analysis-Funktionen war Axpo Informatik in der Lage, die Wirkung der Sicherheitseinstellungen nachzuvollziehen und letztlich die zuvor äußerst komplexen Firewall Security Policies zu vereinfachen.

Da die Axpo Gruppe eine Aktiengesellschaft ist, erweisen sich die Auditing- und Compliance-Funktionen von SecureTrack als besonders nützlich. Sie vereinfachen die Dokumentation und Einhaltung wichtiger internationaler Richtlinien und Vorschriften der Unternehmensführung.

Für die Installation und die technische Betreuung zeichnet Clounet, ein führender Schweizer Systemintegrator, verantwortlich: „Die Einrichtung von SecureTrack erwies sich als problemlos. Innerhalb weniger Stunden war die Lösung betriebsbereit. In der Zwischenzeit hat Axpo Informatik selbst ein Upgrade installiert und sowohl Clounet als auch Axpo sind mit dem Support von Tufin sehr zufrieden“, sagt Martin Christen, Partner bei Clounet. „Axpo hat auch andere Lösungen evaluiert und sich für SecureTrack wegen dessen Kombination aus Real-time-Funktionen und einfacher Nutzung entschieden.“

Der Nutzen

„Nach wenigen Monaten bereits hat sich SecureTrack sehr positiv auf das Firewall-Management bei Axpo ausgewirkt und dazu beigetragen, die Störungen und Netzwerkausfälle deutlich zu reduzieren. Heute wissen wir ganz genau, welche Änderungen von wem durchgeführt wurden und SecureTrack ermöglicht uns, zu jedem Zeitpunkt die Sicherheitseinstellungen unterschiedlicher Firewalls zu analysieren.“

David Spale
Security Officer, Axpo Informatik

„Wir verbringen jetzt deutlich weniger Zeit mit manuellen Updates der Firewalls und können uns stattdessen mehr um unsere Kunden kümmern. Durch die Automatismen von SecureTrack arbeitet unser Team weit effizienter.“

Werner Bühler
Team Manager, Network & Security Services, Axpo Informatik

Die Stärken von SecureTrack:

- Verbesserte Netzwerksicherheit
- Höhere Verfügbarkeit des Netzwerks
- Niedrigere Betriebskosten
- Einhaltung unternehmensweiter Sicherheitsrichtlinien
- Risikomanagement
- Business Continuity
- IT Governance und regulatorische Compliance
- Verbesserte Performance der Sicherheitsinfrastruktur
- Proaktive Umsetzung von Sicherheitsmaßnahmen