Forcepoint

Customer Story

Das GNZ sorgt für sichere Forschung an Instituten der Max-Planck-Gesellschaft

Die Next-Generation Firewall hilft dem GNZ, sein Hochleistungsnetzwerk und damit die Arbeit der Wissenschaftler zu schützen.

Das Gemeinsame Netzwerkzentrum (GNZ) der Max-Planck-Gesellschaft evaluierte Firewall-Anbieter auf dem Markt, da ein echtes zentralisiertes Management für dessen Next-Generation Firewall (NGFW) fehlte. Die NGFW von Forcepoint stellte sich bei der gemeinsamen Betrachtung mit IT-Administratoren aller teilnehmenden Institute als die beste Lösung heraus. Grund dafür ist die hohe Benutzerfreundlichkeit und die umfassende Funktionalität. Damit ist das GNZ nun in der Lage, den Datenverkehr von vier Instituten zu sichern und damit deren bahnbrechende Forschung zu unterstützen.

KUNDENPROFIL:
Das Gemeinsame Netzwerkzentrum (GNZ) des Fritz-Haber-Instituts der Berlin-Brandenburgischen Max-Planck-Einrichtungen ist ein regionales IT-Kompetenzzentrum, das sich mit Netzwerktechnik, Data Storage und IT-Security-Services beschäftigt. Das GNZ unterstützt sämtliche Institute und Bereiche der Max-Planck-Gesellschaft (MPG) in Berlin und Brandenburg.

BRANCHE:
Bildungswesen

LAND:
Deutschland

PRODUKTE:
› Next-Generation Firewall

Zentralisierter Schutz für die MPG-Institute

Seit der Gründung der wissenschaftlichen Stiftung im Jahr 1948 ist die Max-Planck-Gesellschaft (MPG) in Deutschland auf rund 25.000 Wissenschaftlerinnen und Wissenschaftler angewachsen, die in über 80 Einrichtungen forschen. Das Gemeinsame Netzwerkzentrum (GNZ) der Institute der Max-Planck-Gesellschaft in Berlin-Brandenburg ist für acht dieser Institute sowie für einige kleinere Einrichtungen zuständig.

„Wir unterstützen mit unserer Arbeit in den Bereichen Networking, Datenmanagement und IT-Security rund zehn Prozent der Wissenschaftler, die der MPG angehören"

GERD SCHNAPKA, LEITER DES GNZ

"Jedes Institut hat seine eigene IT-Gruppe—manche größer, manche kleiner—die alle eng zusammenarbeiten."

Das GNZ unterhält eine Hochgeschwindigkeitsleitung für seine Wissenschaftler, um deren Forschung, Experimente und andere webbasierte Projekte zu ermöglichen. Darüber hinaus muss das Gemeinsame Netzwerkzentrum individuelle Richtlinien für das Gäste-Netzwerk verwalten, das einen offenen Zugang zum Internet auf dem Campus bietet. Der Grundsatz einer offen zugänglichen Forschungsumgebung macht das MPG-Netzwerk zu einem besonderen Angriffsziel für Hacker, da die Forschenden ihre eigenen Geräte verwenden können.

Als schließlich die Aktualisierung der bestehenden Firewall anstand, stellte der Firewall-Administrator Robert Gruppe fest, dass auch die Kosten für das GNZ und dessen Hardware steigen würden. Da die Plattform kein echtes zentralisiertes Management über alle Institute hinweg bot, beriet sich Robert Gruppe, der beim GNZ für die IT-Sicherheit zuständig ist, mit verschiedenen Anbietern, um eine neue Lösung mit passender Funktionalität und höherer Kosteneffizienz zu finden.

Nahtlose und einfache Migration

Forcepoint ist schon lange ein Teil der deutschen Bildungsgemeinschaft und unterhält Verbindungen zu vielen Universitäten des Landes. Kein Wunder also, dass sich auf einem Thementag zur Sicherheit für universitäre IT-Abteilungen ein Vertreter der RWTH Aachen während einer Präsentation sehr lobend über die Next-Generation Firewall von Forcepoint äußerte. Diese Aussage in Verbindung mit einer Demonstration, die Robert Gruppe einige Jahre zuvor gesehen hatte, überzeugte das GNZ, die Plattform von Forcepoint genauer zu betrachten.

Nach einer gründlichen Evaluierung entschied sich das Gemeinsame Netzwerkzentrum schließlich für die Forcepoints NGFW. Das Security Management Center (SMC), mit dem Robert Gruppe und seine Kollegen alle Einrichtungen zentral verwalten können, sowie die intuitive Funktionalität erleichterten diese Wahl.

„Wir haben uns mit der Benutzeroberfläche und dem System für die Definition von Regeln gleich wohl gefühlt, obwohl wir es zuvor noch nicht benutzt hatten. Das kommt daher, dass die Richtlinienkonfiguration und -erstellung bei unserer bisherigen Lösung ähnlich aufgebaut war", berichtet Robert Gruppe. Ursprünglich rechnete das GNZ mit einem beträchtlichen Zeit- und Ressourcenaufwand für die Migration auf die NGFW, aber die sehr ähnliche Funktionalität sorgte für eine überraschend leichte praktische Umsetzung.

Herausforderungen

- Aufrechterhaltung des konsistenten Netzwerkbetriebs an vier Standorten
- Ermittlung von Kosteneinsparungen gegenüber dem vorherigen Anbieter
- Zentralisierung der Verwaltung
- Schutz des Hochleistungsnetzwerks vor Gefahren und Infiltration

„Die Migration war unglaublich einfach, Wir haben unserem Partner magellan die spezifischen Richtlinien gegeben und schon einen Tag später bekamen wir ein komplettes Set passender Policies."

ROBERT GRUPPE, GNZ FIREWALL ADMINISTRATOR

Die Notwendigkeit, Forcepoint neben der alten Plattform zu integrieren, wie zu Beginn befürchtet, erwies sich als unnötig. Zum Glück, denn wenn zwei Gateways laufen, führt das häufig zu Routing-Problemen. Durch die bereits zuvor erhaltenen Policies konnte das GNZ die alte Lösung problemlos gegen die Next-Generation Firewall von Forcepoint austauschen.

Weniger Bedrohungen und Kosten

Das GNZ hat die NGFW in vier Einrichtungen in weniger als zwei Wochen erfolgreich implementiert. Mit zwei Minuten war die Ausfallzeit recht gering und innerhalb des Netzwerks merkte niemand den Wechsel zur neuen Firewall. Das SMC ermöglicht dem Gemeinsamen Netzwerkzentrum von einem einzigen Standort aus, das Netzwerk zu verwalten und weitere Einrichtungen der MPG in Berlin-Brandenburg hinzuzufügen, sollten sie sich für die Nutzung der NGFW entscheiden.

Robert Gruppe hat die Blockierfunktionen voll ausgeschöpft: Er verwendet eine Mischung aus privaten und öffentlichen Blacklists, um über vier Millionen IP-Adressen pro Tag vom unbefugten Zugriff auf das Netzwerk abzuhalten. Außerdem hindert die NGFW die Netzwerk-User jede Woche am Besuch von 10.000 Webseiten, die auf einer Blacklist stehen. Im Anbetracht der Tatsache, dass

die Einrichtungen Bring-Your-Own-Device erlauben, ist dieses Vorgehen sehr wichtig, denn nicht immer kann das GNZ den Schutz auf alle mit dem Netzwerk verbundenen Geräte anwenden.

„Die Wissenschaftler profitieren von den Einsparungen, die wir durch unsere Next-Generation Firewall erzielen. Das Geld fließt wieder in die Forschung"

ROBERT GRUPPE, GNZ FIREWALL ADMINISTRATOR

„Die Wissenschaftler profitieren von den Einsparungen, die wir durch unsere Next-Generation Firewall erzielen. Das Geld fließt wieder in die Forschung", betont Robert Gruppe vom GNZ, das die starke Unterstützung durch seine Partner magellan und Forcepoint genießt. Durch den schnellen Support der Herstellers und die Bereitstellung neuer Signaturen konnte das Gemeinsame Netzwerkzentrum die integrierte IPS-Funktionalität aktivieren, um die Ausnutzung des Log4j-Bugs zu entschärfen. Das IPS hilft bei der Identifizierung der Angriffe und blockiert automatisch die IP-Adressen der Angreifer.

Ansatz

- Deployment der NGFW von Forcepoint
- Nutzung des Migrations-Tools zur automatischen Migration von etablierten Policies der vorhergehenden Lösung
- Teilnahme an einer zweitägigen Schulung zur Nutzung der neuen Plattform mit dem Forcepoint-Partner magellan

Ergebnisse

- Die erfolgreiche Migration auf NGFW in nur zwei Wochen
- Blockierung von 4 Millionen IP-Adressen pro Tag und 10.000 bösartigen Web-Adressen pro Woche
- Nahtloser Wissenstransfer dank der ähnlichen Funktionsweise der Plattformen
- Maßgebliche Verringerung der geplanten Downtime durch Wartungsfenster
- Hervorragender Kosten-Nutzen-Faktor im Vergleich zu anderen marktführenden Anbietern