Forcepoint

Kundenbericht

Forcepoint NGFW unterstützt die Universität Münster dabei, ihr Netzwerk offen und sicher zu halten

Die Universität Münster verlässt sich auf Forcepoint, um ihre Firewalls effizient zu verwalten, ihr Netzwerk offen zu halten und sich vor Ransomware-Angriffen und anderen Aktivitäten von Cyber-Kriminellen zu schützen.

Artikel 5 des deutschen Grundgesetzes garantiert die Freiheit von Wissenschaft, Forschung und Lehre als Grundrecht. So wird sichergestellt, dass die deutschen Universitäten in Forschung und Lehre einen Spitzenplatz einnehmen. Es ist aber auch eine Herausforderung für die Sicherheitsteams, welche die ständig präsenten Cyber-Sicherheitsbedrohungen abwehren müssen. Die Verteidigung gegen gezielte Angriffe von Cyber-Kriminellen und die Absicherung des Netzwerks der Universität Münster ist eine große Herausforderung für das kleine IT-Team. Doch während andere Universitäten in Deutschland aufgrund von Ransomware-Angriffen wichtige Systeme und Dienste abschalten mussten, konnte die Universität Münster dank Forcepoint NGFW mit IPS den Betrieb sicher fortsetzen.

KUNDENPROFIL:
Eine der größten Universitäten Deutschlands mit rund 45.700 Studenten und 7.100 Mitarbeitern, darunter 5.300 Wissenschaftler.

BRANCHE:
Bildung

HAUPTSITZ:
Deutschland

PRODUKT:
Forcepoint Next Generation Firewall (NGFW)

Öffentliche Einrichtungen in Deutschland, insbesondere Universitäten, sind häufig das Ziel von Cyber-Kriminellen, die entweder den Zugriff auf Dienste verweigern und beeinträchtigen, personenbezogene Daten oder geistiges Eigentum stehlen oder Geld erpressen wollen, indem sie den Bildungsbetrieb unterbrechen. Leider sind Universitäten für spezialisierte Hacker-Netzwerke und ausländische Organisationen ein verlockendes Ziel. Diese Institutionen verfügen oft über moderne, leistungsfähige und weitreichende Netzwerke, über die sich Malware sehr schnell verbreiten lässt. Die Kultur der offenen Netzwerke bedeutet aber auch, dass es schwierig ist, leistungsfähige Sicherheitskontrollen einzurichten. Aufgrund ihrer herausragenden Stellung in Forschung und Entwicklung beherbergen Universitäten auch einen reichen Datenschatz – ein weiterer Anziehungspunkt für Cyber-Kriminelle. In den letzten Jahren waren mehrere deutsche Universitäten gezwungen, große Teile ihrer IT-Infrastruktur für eine gewisse Zeit abzuschalten, so dass Benutzer keinen Zugriff auf E-Mails oder Remote-Verbindungen hatten.

Dies führte teilweise zu massiven Störungen und zeigte, wie schwierig es ist, die Freiheit des Netzes mit den notwendigen Sicherheitskontrollen in Einklang zu bringen. Der Universität Münster ist dies aber sehr gut gelungen. Das IT-Team war sich der Risiken frühzeitig bewusst und hat mehr als 15 Jahre Erfahrung im „Schutz des Unschützbaren" gesammelt.

Die Suche nach einer neuen Firewall mit IPS führte zu einer Lösung, die mehr als 10 Gigabit pro Sekunde verarbeiten kann

1588 als Jesuitenkolleg gegründet, spielt die Universität Münster eine bedeutende Rolle für die Stadt Münster, das Land Nordrhein-Westfalen und das intellektuelle Leben in Deutschland. Die Universität ist in mehr als 300 Gebäuden in der ganzen Stadt untergebracht und beherbergt auch die medizinische Fakultät der Universität Münster.

Als eine der renommiertesten Universitäten in Deutschland hat das Netzwerksicherheitsteam die Sicherheit immer zur Priorität gemacht. Seit 2004 verfügt die Universität über ein Intrusion Prevention System (IPS) zur Abwehr von Eindringversuchen und eine Firewall, aber 2012 wurde bereits mit der Suche nach einer neuen Lösung begonnen. Das Team zog mehrere Anbieter in Betracht und führte mit einigen von ihnen Machbarkeitsstudien durch. In den Machbarkeitsstudien erwies sich Forcepoint (damals unter dem Namen „Stonesoft") als die am besten geeignete Lösung.

Eine der kritischen Anforderungen war der Bedarf an einem IPS, welches das von der Universität geforderte Volumen und die Geschwindigkeit des Datenverkehrs – mehr als 10 Gigabit pro Sekunde – bewältigen konnte. Die Universität hat inzwischen ihre externe Internetanbindung auf 30 Gigabit pro Sekunde aufgestockt und benötigt einen vollständigen IPS-Schutz für all diese Daten, ohne dass der Datenverkehr verlangsamt wird. Forcepoint zeigte, dass es die Last bewältigen konnte, und nach einer erfolgreichen Machbarkeitsstudie führte das Team seine Arbeit mit Forcepoint NGFW und mit Avency, dem Partner für Systemintegratoren, fort.

Das Forcepoint NGFW Security Management Center hat sich bewährt

Heute verfügt die Universität über vier NGFW-Appliances in zwei Clustern, die sechs virtuelle Kontexte bilden. Sie haben sichere Netzwerkbereiche für das Rechenzentrum und die Arbeitsstationen, Voice-over-IP, Gast- und Fernzugriffsdienste, das Internet der Dinge und das interne Management eingerichtet und werden bald einen Bereich für das Verwaltungspersonal hinzufügen. Durch diese separaten virtuellen Kontexte kann das Team je nach Funktion und Anforderungen des Bereichs benutzerdefinierte Sicherheitsrichtlinien, Regeln und Kontrollen festlegen. Die IPS-Konfiguration ist jedoch in allen Kontexten nahezu gleich und fast der gesamte Datenverkehr durchläuft die Module der detaillierten Paketüberprüfung.

Ermöglicht wird die Einrichtung und einfache Konfiguration der virtuellen Kontexte durch das NGFW Security Management Center (SMC) von Forcepoint. „Das SMC ist einer der Hauptvorteile der Firewall-Lösung von Forcepoint – es war ausschlaggebend dafür, dass wir uns für Forcepoint entschieden haben", erklärt Guido Wessendorf, Leiter der Netzwerksicherheit. „Die Konfiguration und Überwachung des ganzen Systems ist bei dieser Lösung sehr intuitiv."

„Es war weitaus besser als die Management-Tools der anderen Anbieter, die wir damals in Betracht zogen", so Markus Speer, Leiter der zentralen Netzwerkdienste.

Herausforderungen

Eine Kultur der Freiheit für Wissenschaft und Lehre bedeutet, dass das Netzwerk offen bleiben muss.

Ein IPS für mehr als 10 GB Internetverkehr ohne Verlangsamung ist erforderlich.

Datenschutzbestimmungen verhindern Sicherheitskontrollen auf persönlichen Geräten von Studenten, Lehrkräften und Mitarbeitern.

Komplexe Ransomware-Angriffe legten andere deutsche Universitäten lahm.

Strategie

Implementierung von Forcepoint Next Generation Firewall mit Intrusion Prevention System.

Das SMC erleichtert die Verwaltung der Firewalls unter anderem durch die API-Funktion. Forcepoint hat an den deutschen Universitäten eine tatkräftige Community aufgebaut, in der sich Sicherheitsprofis vernetzen und Tipps und Tricks zur optimalen Verwaltung ihrer Forcepoint Firewalls austauschen. Einer dieser Tipps war die Verwendung von empfohlenen IP-Blacklists. Die Anwender-Community tauschte Skripte aus, wie diese über die Forcepoint-API in das SMC importiert und installiert werden können. Dies führte dazu, dass es an der Universität Münster täglich zu 100 Millionen Sperren (Firewall-Abbruch oder Denials-of-Service gegenüber böswilligen Hosts) allein aufgrund der IP-Blacklist kam – von insgesamt 150 Millionen Sperren pro Tag.

„Da wir nur ein kleines Team sind, brauchen wir Systeme, die einen Großteil unserer täglichen Aktivitäten automatisch verwalten", erläutert Wessendorf. „Der Import der Blacklist, der automatische Empfang von Forcepoint-Updates und die Richtlinien zur Abwehr von Eindringversuchen helfen uns, unsere Firewalls effizient zu verwalten."

Selbst in einer ungewöhnlich schwierigen Sicherheitsumgebung unterstützt Forcepoint die Universität Münster dabei, frei von Ransomware zu bleiben

Erschwerend für das Team kommt hinzu, dass ein Großteil der PCs, Laptops, Smartphones und Tablets, die von den Studenten, Dozenten und Mitarbeitern genutzt werden, von den Benutzern und nicht von der Universität verwaltet werden. Das bedeutet, dass es keine spezifischen Kontrollen an den persönlichen Systemen geben kann. Häufig nutzen Firewalls die HTTPS-Entschlüsselung, um Datenpakete aus dem Internetverkehr zu untersuchen und bösartigen Code zu finden. In diesem Szenario ist dies aufgrund von Datenschutzbeschränkungen zum Schutz der privaten PC-Nutzer jedoch nicht möglich.

An einem normalen Studientag sind rund 20.000 Benutzer gleichzeitig mit ihren eigenen, ungeschützten Laptops, Tablets und Smartphones mit dem WLAN der Universität verbunden. Diese Geräte und alle anderen ca. 30.000 registrierten Endsysteme der Universität könnten mit Ransomware infiziert werden, die zur Aktivierung zusätzliche Schlüssel oder Software herunterladen muss, aber von der Firewall-Lösung von Forcepoint daran gehindert wird.

„Die IP-Blacklists, die wir zusammen mit den integrierten Forcepoint-Blacklists importiert haben, die Aktualisierungen des Forcepoint ThreatSeeker Intelligence-Netzwerks und die IPS-Funktionen greifen ineinander und stoppen die Versuche von Schadsoftware, auf Befehls- und Kontrollfunktionen unserer Systeme zuzugreifen und lokal Ransomware zu installieren", so Wessendorf. „Daher gehen wir davon aus, dass wir bisher noch keine Ransomware-Zwischenfälle hatten."

Eine engagierte Universitäts-Community bietet Vorteile für Forcepoint-Kunden

Es kommt vor, dass Kollegen in ähnlichen Sicherheitsfunktionen um eine Bewertung von Forcepoint NGFW bitten. „Normalerweise lade ich sie ein, an meinen Arbeitsplatz zu kommen und sich die Lösung anzusehen", so Wessendorf. „Im SMC sehen sie, wie einfach die Bedienung, Konfiguration und Verwaltung ist – eine solche Demonstration sagt mehr als Worte."

Die Universität Münster ist eine der ersten in Deutschland, die Forcepoint NGFW ausgewählt und implementiert hat. Auch die Langlebigkeit dieser Beziehung verdeutlicht, welchen Wert sie hat. Das Netzwerksicherheitsteam der Universität schätzt die Möglichkeit, sich mit dem Forcepoint Firewall-Produktentwicklungsteam in Finnland auszutauschen. „Wir haben die Möglichkeit, Wünsche für neue Funktionen zu äußern und Input zu geben, welche Anforderungen wir in den kommenden Jahren haben werden", informiert Speer. „Dieser direkte Kontakt und die enge Arbeitsbeziehung zu Forcepoint ist ein klarer Vorteil."

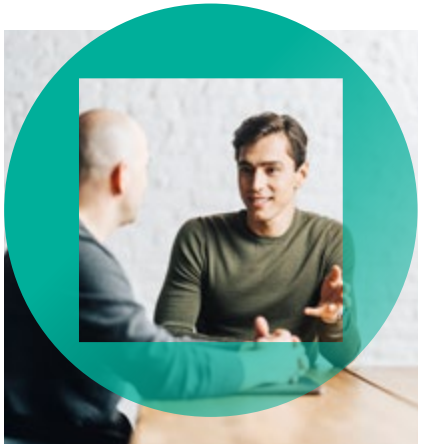
Neben dem Produkt selbst ist auch der Support von Forcepoint und die Community, die rund um die deutschen Universitäten mit NGFW aufgebaut wurde, einzigartig. Laut Wessendorf sind alle Mitglieder Experten im Umgang mit NGFW und dem SMC, was die Community zu einer sehr wertvollen Ressource macht.

„Ich muss sagen, dass diese Art von Unterstützung und Zusammenarbeit in anderen Universitätskreisen nicht bekannt ist. Die Vorteile für die Mitglieder sind wirklich greifbar", so Speer.

Forcepoint

Ergebnisse

- Die Firewall sperrt pro Tag **150 Millionen** Verbindungen.
- Keine erfolgreichen Ransomware-Angriffe.
- Teil einer engagierten deutschen Universitäts-Community, bei der die Netzwerksicherheit von Forcepoint im Mittelpunkt steht.



„Ich muss sagen, dass diese Art von Unterstützung und Zusammenarbeit in anderen Universitätskreisen nicht bekannt ist."

MARKUS SPEER, LEITER DER ZENTRALEN NETZWERKDIENSTE