IDARION
networking & security

Case Study

SWITCH

WEGWEISENDE IT-SECURITY FÜR DAS **SWITCH-OFFICE-NETZ**

Performance, Verfügbarkeit, Sicherheit: Um das interne Office-Netz wirksam vor Gefahren zu schützen, setzt SWITCH auf hochleistungsfähige Zonen-Firewalls von Fortinet – und auf Funktionen wie Multicast-Routing, IPv6-Support und hochgradig gesicherte Netzwerksegmentierung.

«Synonym für die Vernetzung der Schweizer Wissenschaft» – auf diesen einfachen Nenner bringt SWITCH das weitreichende, seit der Geburtsstunde des Internets offerierte Dienstleistungsangebot. Zu Recht, denn die Partnerin der Schweizer Hochschulgemeinschaft verbindet mit ihrem Hochleistungsnetzwerk die Internetnutzenden der Schweiz untereinander sowie mit Europa und dem Rest der Welt. Die für Lehrende, Forschende und Studierende entwickelten Internet- und Security-Dienste bietet die Non-Profit-Organisation SWITCH auch ausgewählten kommerziellen Kunden an. Dazu gehören namentlich Finanzinstitute, die E-Banking-Lösungen betreiben und auf eine hochkarätige Beratung und forensische Abklärungen angewiesen sind.

Zur Absicherung ihres internen Office-Netzes hat sich SWITCH im Rahmen einer breit angelegten Evaluation mit der Erneuerung und Optimierung ihrer IT-Security-Infrastruktur auseinandergesetzt. Laut Thorben Jändling, Security Engineer, galt es dabei, eine integrale Security-Appliance zu evaluieren, die sich nicht nur für den Netzwerkschutz am Perimeter eignet, sondern auch einen hochgradigen Schutz der internen Bereiche ermöglicht. «Unsere diversen internen Anspruchsgruppen beziehungsweise Abteilungen sind heterogen, die individuel-

FORTINET

len Security-Policies entsprechend vielschichtig. So hat etwa die Finanz-Abteilung andere sicherheitsrelevante Bedürfnisse als die Bereiche HR oder Kundensupport. Auch die Server- und Applikationslandschaft präsentiert sich variantenreich und benötigt individuelle Security-Vorkehrungen. Vor diesem Hintergrund haben wir bei der Firewall-Evaluation grossen Wert auf die konsequente Umsetzung eines granularen Zonenkonzepts gelegt, das die einzelnen Abteilungen und Benutzergruppen klar voneinander trennt. Dank dem nun realisierten VLAN-Konzept basiert jedes Team auf einem eigenen Netz (virtuelles LAN mit eigenem Sub-Netz). Dies führt dazu, dass die einzelnen Gruppen auf Netzwerkbasis voneinander getrennt sind und dass allenfalls in einer Zone eingeschleuster Schadcode andere Bereiche nicht infizieren kann.»

MODERNE BEDROHUNGEN ABWEHREN

Dass SWITCH die Beschaffung einer neuen Security-Infrastruktur angegangen ist, liegt in den sich drastisch ändernden Bedrohungsformen begründet. Zeichneten sich frühere Angriffe hauptsächlich durch eine breite Streuung von Viren, Trojanern und unspezifischen Attacken aus, sind moderne Angriffsmethoden wesentlich gezielter, subtiler und professioneller. Die organisierte Internetkriminalität hat Werkzeuge und Malware entwickelt, die das Potenzial haben, Infrastrukturen lahmzulegen, Finanzapplikationen zu hacken, Verschlüsselungssysteme und Zertifikate auszuhebeln, Daten im grossen Stil zu stehlen ...

Das Einschleusen von Schadcode, der sich im Zielsystem einnistet, kann bereits durch den Besuch einer verseuchten Website erfolgen. Diese «Drive-by»-Attackenn sind oft der Ausgangspunkt einer Verseuchung des Rechners. Web2.0-Anwendungen und «Social Engineering»-Strategien eignen sich bestens dazu. Moderne Angriffsmethoden (oft mit «Modern Malware» bezeichnet) führen dazu, dass konventionelle Firewalls nicht in der Lage sind,

> « Mit der umfassenden Unterstützung von Next Generation Networking-Technologien wie IPv6 ist Fortinet dem Markt definitiv voraus.»
>
> **THORBEN JÄNDLING**
> Security Engineer, SWITCH

eine umfassende Sicherheit zu gewährleisten. So lassen sich User, Systeme und Programme nicht mehr klar definierten IP-Adressen oder TCP-Ports zuordnen. Folglich reichen für deren Kontrolle konventionelle Technologien wie Paketfilter, VPN-Gateway, Content Filter oder IDS/IPS nicht mehr aus. Benötigt wird vielmehr ein übergreifender, konsolidierter Ansatz mit integralen Konfigurations-, Analyse- und Kontrollfunktionen. Diese bilden die Voraussetzung dafür, firmenweite beziehungsweise zonenspezifische Security-Policies zu definieren und durchzusetzen.

GLASFASER UND IPV6 SEIT JAHREN REALITÄT

«Wir betreiben das wohl modernste Netz der Schweiz.» Diese von Security-Experte Jändling gemachte Aussage könnte treffender nicht sein. Dank der durchgehenden Nutzung von Glasfasern weist das SWITCH-Office-Netz beispielsweise einzigartige Datenraten auf. Ebenso beeindruckend ist die Verwendung des IPv6-Protokolls. Was in anderen Unternehmen erst vage zum Thema wird, ist bei SWITCH seit Jahren Realität.

Faktoren dieser Art hätten die Evaluation der neuen Security-Appliance nicht gerade einfach gemacht, äussert sich Jändling zum Auswahlverfahren. So konnten viele der betrachteten

Appliances die geforderten Leistungsmerkmale nicht erfüllen. Zahlreiche Systeme unterstützen beispielsweise das IPv6-Protokoll (noch) nicht. Auch das Vorhandensein mehrerer 10-GB-Ports oder eine Hardware-Performance, die auch bei Volllast eine nahtlose Überwachung des gesamten Netzwerk-verkehrs ohne merkbare Latenzzeiten ermöglicht, waren keine Selbstverständlichkeit – für SWITCH jedoch entscheidende Kriterien. Im Rahmen eines mehrmonatigen Auswahlverfahrens hat sich SWITCH für die Beschaffung hoch performanter Security-Appliances von Fortinet entschieden. Diese erfüllen die meisten der gestellten Anforderungen hinsichtlich Funktionalität, unterstützter Protokolle, Performance und Verfügbarkeit. Allerdings benötigte SWITCH spezifische Networking-Features, die keine der evaluierten Appliances zum Zeitpunkt der Beschaffung ohne Einschränkungen gewähren konnte. So zum Beispiel die Unterstützung der Funktion BGP-Failover auf Basis IPv6 (unterbruchsfreies Routing im Firewall-Cluster). Bei der Wahl des Lieferanten war es folglich mitentscheidend, welcher Hersteller für die spezifischen Bedürfnisse ein offenes Ohr hatte und sich bereit erklärte, Zusatzfeatures kurzfristig zu implementieren. Auch diesbezüglich erwies sich Fortinet als klare Nummer eins. Die «Feature Requests» von SWITCH wurden ernst genommen, die entsprechenden Entwicklungen vorangetrieben. Heute nun darf Fortinet für sich in Anspruch nehmen, die wohl beste Unterstützung für IPv6 zu bieten.

«Aus meiner Sicht nehmen die Next Generation Firewalls von Fortinet eine klare Führungsrolle ein. Sie verbinden Sicherheit, Performance und weitreichende Netzwerk-Features mit einem modernen Management-System.»

THORBEN JÄNDLING
Security Engineer, SWITCH

SWITCH

SWITCH ist Partnerin der Schweizer Hochschulgemeinschaft. Die Non-Profit-Organisation entwickelt und betreibt Internetdienste für Lehrende, Forschende und Studierende. Gewisse für die Hochschulen entwickelte Services bietet SWITCH auch kommerziellen Kunden an. Darüber hinaus ist SWITCH Registrierungsstelle für Domain-Namen mit den Endungen .ch und .li. Diese gehören zu den sichersten der Welt.

FÜR DIE ZUKUNFT GERÜSTET

Der von SWITCH eingesetzte Firewall-Cluster besteht aus zwei «Next Generation Firewalls» FortiGate 3950B. Dabei handelt es sich um hochleistungsfähige Appliances, die den gesamten Datenverkehr des SWITCH Office-Netzes in Echtzeit filtern und Angriffe abwehren. «Durch die neuen Firewalls stehen uns nun vielfältige Möglichkeiten zur Abwehr von ‹moderner Malware› zur Verfügung», betont Jändling.

Der redundant aufgebaute 3950B-Firewall-Cluster bietet Gewähr für ein hohes Mass an Performance, Verfügbarkeit und Sicherheit. Einen wichtigen Beitrag dazu leisten auch Upgrade- und Wartungs-Verträge, die dafür sorgen, dass Funktionen und Signaturen stets aktuell sind. Jändling ergänzt: «Zentral ist und war für uns auch die professionelle Zusammenarbeit mit unserem Security-Partner Sidarion. Dadurch profitieren wir von Erfahrung, Know-how und Engagement.»

SIDARION
networking & security

FIREWALL-APPLIANCE **FORTIGATE 3950B SETZT BESTMARKEN**

Die Next Generation Firewall FortiGate 3950B beinhaltet sämtliche heute denkbaren Features, um den gesamten Datenverkehr beziehungsweise User, Devices und Applikationen in Echtzeit zu überwachen, zu visualisieren und auf Basis definierter Security-Policies und stets aktualisierter Signaturen Gefahren wirksam abzuwehren. Dazu stellt die Appliance weitreichende Features wie Firewalling, Antivirus, IPS, URL-Filtering, Spam-Filtering und VPN-Terminierung zur Verfügung. Ebenso sind Funktionen wie «Application Control» und «Client Reputation» unterstützt. Diese «Content Security»-Funktionen leisten beispielsweise bei der Überwachung von Peer-to-Peer-Netzwerken und Social-Media-Plattformen wertvolle Dienste. Zudem ermöglichen sie eine komfortable Umsetzung sogenannter «User based Policy Enforcements». So ist es beispielsweise möglich, https global freizugeben, kritische Anwendungen hingegen zu blockieren oder zeitabhängig zu steuern.

FortiGate-3950B «Next-Generation Firewalls» bieten für grosse Enterprise-Netzwerke, Managed Service Provider und Datacenter ein Maximum an Performance, Skalierbarkeit und Sicherheit. Zu den wichtigsten Leistungsmerkmalen zählen:

- Modulare, ASIC-beschleunigte Architektur (FortiASIC-Prozessoren) mit Platz für bis zu fünf Fortinet Mezzanine-Karten (FMC-Einschübe) zur Beschleunigung dedizierter Aufgaben. Auf der verwendeten FMC-XH0-Karte dient der Content-Prozessor CP8 beispielsweise der Performancesteigerung bei Funktionen wie AV, IPS und Web Filtering. Der FortiASIC-SP3 Service Prozessor beschleunigt den IPv6-basierenden Datenverkehr.
- «Klassische» Firewall-Funktionen sowie Content-Security und Application-Control in einem System (Next Generation Firewall)
- Möglichkeit zur Analyse verschlüsselter Daten, die über Protokolle wie HTTPS, POP3S, SMTPS und IMAPS transportiert werden, sowie von P2P- und IM-Anwendungen, die via Tunnel kommunizieren
- Unterstützung sämtlicher relevanter Protokolle und Funktionen wie IPv6, BGP-Routing, Multicast-Routing etc.
- Mehrere 10 GBit-Ports sowie latenzfreie Firewall-Durchsatzraten von bis zu 120 Gbps
- Bis zu 64'000 VPN-Tunnels mit einem Durchsatz von bis zu 50 Gbps
- Bildung von Zonen beziehungsweise virtuellen LANs (VLANs); ermöglicht Trennung und gegenseitigen Schutz definierter Bereiche
- Komfortable Definition und Durchsetzung granularer, User- und Zonen-spezifischer Security-Policies
- Administration über ein einfach bedienbares, grafisches Web-Interface sowie Remote Management, verschlüsselt über HTTPS und SSH
- Minimierte Beschaffungs- und Installationskosten sowie reduzierte Aufwendungen für Unterhalt, Support und Upgrades dank Einbindung sämtlicher relevanten Sicherheitsfunktionen in einem System

SIDARION AG
Rikonerstrasse 21
CH-8307 Effretikon
Tel.: +41 43 544 10 66
www.sidarion.ch