SIDARION
networking & security

Case Study

© **Universität St.Gallen** / Fotograf: Hans-Peter Schiess

UNIVERSITÄT ST.GALLEN SCHÜTZT E-MAIL-KOMMUNIKATION MIT FORTIMAIL VON FORTINET

SECURE MESSAGING APPLIANCE

Um den Mitarbeitenden aus Verwaltung und Instituten einen maximalen Spam- und Malware-Schutz zu gewährleisten, setzt die Universität St.Gallen auf Secure-E-Mail-Appliances der FortiMail-Familie von Fortinet. Diese konsolidieren Funktionen wie Anti-Spam, Anti-Phishing, Anti-Malware, Data Leakage Prevention (DLP) und Identity Based Encryption (IBE) in einem System und setzen hinsichtlich Funktionalität, Wirksamkeit und Performance Standards.

Rund 400 000 E-Mail-Nachrichten pro Monat bei ungebrochen steigender Tendenz – so präsentiert sich die Situation bei der Universität St.Gallen (HSG) bezogen auf die elektronische Kommunikation der gesamthaft rund 2300 Mitarbeitenden sowie der rund 1500 nicht persönlichen E-Mail-Konten aus Verwaltung und Instituten. Angesichts der Tatsache, dass E-Mails ein grosses Gefahrenpotenzial hinsichtlich Einschleusung von Schadcode darstellen und dass Spam-Mails enorme personelle und systembezogene Ressourcen verschleudern, setzt die Universität St.Gallen seit mehreren Jahren auf den Einsatz einer Anti-Spam- und Anti-Viren-Gateway-Lösung. Dazu Roman Handl, Verantwortlicher Mailsysteme bei der HSG: «Es ist unser Bestreben, Spam-Mails und Malware so früh wie möglich zu erkennen bzw. zu blockieren, bevor sie in die Mailbox des jeweiligen Empfängers gelangen. Dazu setzen wir auf eine dedizierte Secure-Messaging-Plattform, die den gesamten ein- und ausgehenden Mail-Verkehr auf Viren und Spam überprüft. Die in der Vergangenheit eingesetzte serverbasierte Lösung ist in die Jahre gekommen, vermochte den wachsenden Anforderungen hinsichtlich Performance, Support und Funktionalität nicht mehr vollumfänglich zu genügen und musste erneuert werden. Diese Gelegenheit haben wir genutzt, um eine neue Secure-E-

FORTINET

Mail-Plattform zu evaluieren, und haben uns dabei im Rahmen eines detaillierten Auswahlverfahrens für zwei FortiMail 400C Appliances von Fortinet entschieden. Diese entsprechen all unseren heutigen Anforderungen und sind derart performant und flexibel, dass auch weitere, jetzt schon absehbare Bedürfnisse abgedeckt werden können.»

WEITREICHENDE FUNKTIONEN

FortiMail 400C ist eine ASIC-beschleunigte, ausgesprochen leistungsstarke Secure Messaging Appliance, die in der Lage ist, mehr als 300 000 E-Mails pro Stunde zu prüfen. Sie beinhaltet zum einen eine wegweisende Engine für einen umfassenden Viren- und Spyware-Schutz und zum andern fortschrittliche Spam-Erkennungs- und Filter-Methoden. Dazu gehören zugangsgerechte Filter, Content-Filter, benutzerspezifische Bayessche Filtermethoden und heuristische Filter ebenso wie globale und benutzerbezogene Black/White-List-Filter sowie Spam Realtime Blackhole Lists (RBL). Handl erwähnt: «Die weitreichenden Filter-Methoden und Algorithmen leisten bereits in der Grundeinstellung einen hervorragenden Spam- und Malware-Schutz. Zudem lassen sie sich granular nach unseren individuellen Bedürfnissen aktivieren und konfigurieren. Ferner beinhaltet FortiMail Leistungsmerkmale, die dafür sorgen, dass unerwünschte Nachrichten ohne zeitaufwendige Analysen abgewehrt werden können. Dazu dient beispielsweise eine kontinuierlich und automatisch aktualisierte IP-Reputations-Datenbank. Sie sorgt dafür, dass Verbindungsanfragen von Absender-IP-Adressen mit schlechter Reputation gar nicht erst angenommen werden. Vor dem Hintergrund, dass 60 bis 70 Prozent der eingehenden E-Mails dieser Kategorie zuzuordnen sind, ist dies ein wichtiges Feature.» Doch damit nicht genug: FortiMail stellt weitere, auf unterschiedlichen Layern angesiedelte Algorithmen für eine sichere E-Mail-Kommunikation zur Verfügung. So etwa tiefgreifende Header-Analysen oder das Erkennen von Bildinhalten. Für Handl steht fest: «Mit FortiMail setzen wir im Bereich Spam- und Virenschutz auf eine der führenden Lösungen.» Dass dies so bleibt und die Abwehr von Malware und Spam auch im Zeitverlauf keine Schwächen zeigt, sorgt Fortinet mit dem Service FortiGuard AntiSpam. Dieser stellt sicher, dass neueste Attacken sofort erkannt und wirksam abgewehrt werden. FortiGuard wird von einem weltweit verteilten Security-Spezialisten-Team von Fortinet rund um die Uhr und an sieben Tagen pro Woche aktualisiert und gepflegt.

© Universität St.Gallen / Fotograf: Hannes Thalmann

> «FortiMail von Fortinet entspricht sämtlichen gestellten Anforderungen, ist preislich attraktiv und ausgesprochen einfach hinsichtlich Handhabung und Betrieb.»
>
> **ROMAN HANDL**
> Verantwortlicher Mailsysteme, Universität St.Gallen

ABGEWEHRT UND TROTZDEM VORHANDEN

Angesichts der Tatsache, dass keine hundertprozentige Garantie dafür besteht, dass nur schlechte E-Mails blockiert («false negative») und nur gute Nachrichten zugestellt werden («false positive»), ist für Roman Handl ein weiteres FortiMail-Leistungsmerkmal von besonderer Bedeutung: die Quarantäne-Funktion. Diese sorgt dafür, dass sämtliche abgewiesenen Nachrichten in einem eigenen Bereich gespeichert werden und für einen späteren Abruf durch die jeweiligen User zur Verfügung stehen. Somit gehen keine fälschlicherweise nicht zugestellten Nachrichten verloren. Einen Überblick über die sich in der Quarantäne befindenden E-Mails erhalten berechtigte Administratoren sowie die jeweiligen User via tägliche E-Mail-

FORTIMAIL UND FORTIGUARD ANTISPAM – EIN STARKES GESPANN

Die Secure-Messaging-Plattform FortiMail von Fortinet und der Managed-Antispam-Service FortiGuard Antispam bilden für Netzwerk und Mail-Server eine hoch effiziente Gesamtlösung zur Abwehr von Viren und Spam-Inhalten. Zu den wichtigsten Leistungsmerkmalen des robusten und performanten E-Mail-MTA (Message Transfer Agent) gehören:

- Nahtlose Überwachung sämtlicher ein- und ausgehender E-Mails
- Geprüfte E-Mail-Antispam- und -Antivirus-Lösung, die über 20 VBSpam-Platinum-Awards in Folge gewonnen hat (ISCA Labs Antispam Certified / VBSpam Certified / Common Criteria EEAL Certification)
- Fortschrittlichste Antispam-Filter (Zugangsrechte-Filter, Content-Filter, globale und benutzerbezogene Black/White-List-Filter, Spam Realtime Blackhole List, benutzerspezifische Bayessche Filtermethoden, heuristische Filter) inkl. Reputation-Schutz-Technologie mit flexiblen Konfigurationsmöglichkeiten
- Support für mehrere Domains
- HA-Unterstützung
- Integriertes policy-based E-Mail-Routing und Queue-Management
- Quarantäne-Funktion mit separater Disk, täglichen Reports und geschütztem Zugriff via Web-Mail und POP3
- Erweiterbar mit der «Advanced Thread Detection FortiSanbox»-Lösung, die weit über herkömmliches Antivirus-Scanning hinausgeht


© Universität St.Gallen / Fotograf: Hannes Thalmann

Reports, die einen direkten Zugang zu den Quarantäne-Mails ermöglichen.
Die Quarantäne-Funktion war laut Handl mitentscheidend für die Beschaffung der FortiMail-Appliance von Fortinet. «Als Alternative zur Installation einer eigenen E-Mail-Security-Appliance haben wir auch ‹E-Mail Security as a Service›, wie dies von einigen Serviceprovidern angeboten wird, in die Evaluation miteinbezogen. Dabei wurde jedoch deutlich, dass sich anfänglich tiefere Kosten in wenigen Jahren ins Gegenteil verkehren. Wichtiger noch: das Fehlen einer Quarantäne-Datenbank führt zu markanten Nachteilen. Als schlecht identifizierte Nachrichten werden zwar markiert, aber trotzdem an die Empfänger ausgeliefert. Dies ist aus Sicherheitsgründen problematisch und strapaziert die Speicherkapazität des Mail-Servers bzw. der User-Mailbox. Zudem wären wir bei der Wahl einer entsprechenden Cloud-Lösung gezwungen gewesen, in die Basis-Definition unserer Mail-Datenbankregeln einzugreifen beziehungsweise die Filter-Regeln für sämtlich User neu zu definieren. Ein aufwendiges Unterfangen, das wir unter allen Umständen verhindern wollten.»

E-MAIL-VERSCHLÜSSELUNG INKLUSIVE

Nebst der Abwehr von Spam und Malware ermöglichen die bei der Universität St.Gallen als Cluster (aktiv/passiv) installierten FortiMail-Appliances auch die Verschlüsselung und Entschlüsselung von Nachrichten. Dabei lassen sich E-Mails ohne Administrationsaufwand verschlüsselt übertragen, wobei weder auf Sender- noch auf Empfängerseite eine zusätzliche Client-Software benötigt wird. Die Verschlüsselung basiert auf der sogenannten «Identity Based Encryption» (IBE), also auf Basis einzelner User und Nutzergruppen sowie auf spezifischen, in der E-Mail enthaltenen Wörtern.
Bei der verschlüsselten Übertragung einer E-Mail erhält der Empfänger lediglich eine Nachricht mit dem Hinweis auf die verschlüsselte E-Mail sowie den Link auf deren Speicherort in der FortiMail-Appliance. Ist der Empfänger mittels LDAP im Unternehmensdirectory gelistet, kann er die Nachricht nach der Eingabe seiner Login-Daten umgehend lesen. Ohne LDAP-Einbindung ist dazu eine einmalige Anmeldung mittels Username/Password auf der FortiMail-Appliance notwendig.

> «Das grosse Know-how und die breite Erfahrung unseres Partners Sidarion im Bereich E-Mail-Security war für unsere Entscheidung zugunsten FortiMail mitentscheidend.»
>
> **ROMAN HANDL**
> Verantwortlicher Mailsysteme, Universität St.Gallen

EINFACHE INSTALLATION, KOMFORTABLES REPORTING

Die im mittleren Leistungsbereich angesiedelte FortiMail 400C lässt sich – wie sämtliche Appliances der FortiMail-Familie – auf drei unterschiedliche Arten ins Kommunikationsnetz einbinden. Im Transparent-Modus wird sie vor den bestehenden E-Mail-Server platziert. Dadurch sind keine Änderungen an der bestehenden E-Mail-Topologie nötig. Im Server-Modus liefert die Appliance ausgewachsene E-Mail-Server-Funktionalitäten, was namentlich für mittlere Unternehmen und für vernetzte Zweigniederlassungen von Interesse ist. Und im Gateway-Modus schliesslich sorgen E-Mail-Relay-Services dafür, dass der gesamte ein- und ausgehende Mailverkehr geprüft wird und nur für gut befundene Nachrichten in die E-Mail-Serverinfrastruktur gelangen. Dazu Roman Handl: «Die von uns gewählte Gateway-Integration weist zahlreiche Vorzüge auf. Allen voran die einfache Einbindung in die bestehende Infrastruktur, die seitens User keinen Konfigurationsaufwand verursacht und seine gewohnte Mail-Umgebung nicht antastet. Dadurch waren wir in der Lage, die Basis-Installation inkl. Schulung innerhalb Tagesfrist umzusetzen.»
Handl macht auf weitere Leistungsmerkmale aufmerksam, die den Entscheid zugunsten der FortiMail 400C Appliances unterstützt haben. «Dazu gehören beispielsweise die einfach konfigurierbaren Routing-Funktionen oder die Unterstützung unterschiedlicher E-Mail-Domains mit der Möglichkeit, individuelle beziehungsweise domainspezifische Filter-Regeln zu definieren. Bedeutsam sind ferner die Clusterfähigkeit mit High Availability Support sowie weitreichende Logging- und Reporting-Funktionen.»

SIDARION
networking & security

UNIVERSITÄT ST.GALLEN (HSG)

Die Universität St.Gallen wurde 1898 als Handelsakademie gegründet und ist heute eine Hochschule für Wirtschafts-, Rechts- und Sozialwissenschaften sowie für Internationale Beziehungen. Die HSG zählt zu den führenden Wirtschaftsuniversitäten in Europa, die mit über 150 internationalen Partneruniversitäten verbunden ist. Für die Studierenden sind Abschlüsse auf Bachelor-, Master- und Doktorats/Ph.D.-Stufe möglich. Nebst Studiengängen offeriert die HSG zahlreiche Weiterbildungsmöglichkeiten. Dazu gehören unter anderem Nachdiplomausbildungen, Seminare, Kurse und Inhouse-Seminare. Von Bedeutung ist die enge Vernetzung von Studium, Weiterbildung und Forschung. So hat sich die Universität St.Gallen mit ihren über 30 Instituten und Forschungsstellen in den Bereichen Grundlagenforschung und angewandte Forschung international einen Namen gemacht.

SIDARION

Die 2003 gegründete, in Effretikon (ZH) und Baar (ZG) domizilierte Sidarion AG zählt zu den etablierten Lösungsanbietern in den Bereichen IT-Security, IP-Adress-Management, Networking, Netzwerk-Überwachung und konvergente Infrastrukturen. Das Team topausgebildeter und erfahrener Spezialisten sorgt für umfassende Dienstleistungen. Diese reichen von der Beratung und Konzeptionierung über die Planung und Implementierung bis hin zu Wartung und Support komplexer Umgebungen. Zu den Kunden von Sidarion zählen namentlich mittlere und grosse Unternehmen in der Schweiz sowie international tätige Unternehmen mit Hauptsitz in der Schweiz.

SIDARION AG
Lättichstrasse 6
CH-6340 Baar

Rikonerstrasse 21
CH-8307 Effretikon

Tel.: +41 43 544 10 66
www.sidarion.ch