Bild: zVg

DOSSIER E-MAIL-SECURITY
IN KOOPERATION MIT BOLL ENGINEERING

Geschickt gesicherte Post

ahe. E-Mails sind nach wie vor ein beliebtes Kommunikationsmittel. Das gilt für Mitarbeiter im Unternehmen genauso wie für Spammer und Malware-Anbieter. Berühmt-berüchtigt sind Phishing-Mails, die je länger desto echter ein Finanzinstitut als Absender vorgaukeln und damit versuchen, an Konten- und Kreditkartendaten ahnungsloser Empfänger zu gelangen. In Firmen ist es deshalb sinnvoll, solche unerwünschten «Mitteilungen» herauszufiltern, bevor sie beim Empfänger im Posteingang landen. Dabei kommen oftmals dedizierte Systeme zum Einsatz, die auf die Mailfilterung spezialisiert sind. Diese Sicherheits-Appliances untersuchen ankommenden und ausgehenden Postverkehr auf Legitimität. Zweifelhafte E-Mails bleiben hängen und gelangen gar nicht bis ins Postfach des Benutzers.

Allerdings ist diese Aufgabe vergleichbar mit einem Katz-und-Maus-Spiel. Denn die Absender von Spam- und Fishing-Mails werden immer raffinierter, sodass auch die Abwehrtechniken ständig verfeinert werden müssen. Zudem muss die Appliance leistungsfähig genug sein, um mit dem Verkehrsaufkommen mithalten zu können.

Bei der Universität St. Gallen müssen monatlich rund eine Million E-Mails verarbeitet werden, schätzt Roman Handl von der IT-Abteilung. Die eingesetzte Appliance zeichnet sich gemäss dem Informatiker durch eine hohe Genauigkeit bei der Erkennung aus: «Wir bekommen nur relativ wenige Anfragen bezüglich nicht zugestellter E-Mails oder Fehlern bei der Spam-Filterung. Ich gehe daher davon aus, dass unsere Nutzer sehr zufrieden sind.» Damit trägt die Appliance nicht nur zu einer sicheren Kommunikation bei, sondern erhöht auch die Zufriedenheit der Mitarbeiter an der St. Galler Universität.

> **Seite 30**
Die E-Mail-Sicherheit verbessern

> **Seite 32**
Roman Handl, Universität St. Gallen: «Wir bekommen nur wenige Anfragen wegen nicht zugestellter Mails»

Die E-Mail-Sicherheit verbessern

Im Bestreben, Firmen und Mitarbeitern einen maximalen Spam- und Malware-Schutz zu gewährleisten, spielen sogenannte Secure E-Mail-Appliances eine wichtige Rolle. Sie konsolidieren Funktionen wie Anti-Spam, Anti-Phishing, Anti-Malware, Data Leakage Prevention (DLP) und Identity Based Encryption (IBE) und machen die E-Mail-Kommunikation nachhaltig sicher. Patrick Michel

E-Mails stellen ein grosses Gefahrenpotenzial hinsichtlich Einschleusung von Schadcode dar. Zudem verschleudern Spam-Mails enorme personelle und systembezogene Ressourcen. Vor diesem Hintergrund ist es ratsam, Malware und Spam-Mails so früh wie möglich zu erkennen beziehungsweise zu blockieren – noch bevor sie in die Mailbox des jeweiligen Empfängers gelangen. Auch ausgehende E-Mails sollten entsprechend geprüft werden, bevor sie das Firmennetzwerk verlassen. Ansonsten kann es passieren, dass die eigenen IP-Adressen in entsprechenden Reputationsdatenbanken landen und die ausgehende E-Mail-Kommunikation gestört wird. Unterstützung bieten dabei dedizierte Secure-Messaging-Plattformen, die den gesamten ein- und ausgehenden Mail-Verkehr auf Viren und Spam überprüfen. Dies ist bei mittleren und grossen Unternehmen, die gut und gerne mit mehreren Hunderttausend oder gar Millionen E-Mail-Nachrichten pro Monat konfrontiert sind, ein anspruchsvolles Unterfangen. Es setzt an die Secure-E-Mail- beziehungsweise an die Secure-Massaging-Plattform hinsichtlich Performance, Support und Funktionalität höchste Anforderungen.

Performance und Funktionsvielfalt

Heute stehen leistungsstarke Secure-Messaging-Appliances zur Verfügung, die in der Lage sind, mehrere Hunderttausend E-Mails pro Stunde zu prüfen. Die führenden Produkte beinhalten dazu einerseits eine hochperformante Engine für den umfassenden Viren- und Spyware-Schutz. Andererseits überzeugen sie durch fortschrittliche Spam-Erkennungs- und Filter-Methoden. Dazu gehören beispielsweise regelbasierte Filter wie IP-Reputation, Body-URLs, Body-Kontakt-E-Mail, Object Checksum und Greylisting ebenso wie Content-Filter, heuristische Filter sowie globale und benutzerbezogene Black/White-List-Filter. In aller Regel bieten die Appliances bereits in der Grundeinstellung einen hochgradigen Spam- und Malware-Schutz, der sich in Umgebungen mit einem überdurchschnittlich hohen Spam-Aufkommen über entsprechende Filtereinstellungen erhöhen lässt.

Innovative Plattformen beinhalten ferner diverse Funktionen, die dafür sorgen, dass sich unerwünschte Nachrichten ohne zeitaufwendige Detailanalysen abwehren lassen. Dazu dient beispielsweise eine kontinuierlich und automatisch aktualisierte IP-Reputationsdatenbank, die dafür sorgt, 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, ein wichtiges Feature. Von Bedeutung sind zudem tiefgreifende Header-Analysen sowie das Erkennen von Bildinhalten.

Damit der Spam- und Virenschutz auch im Zeitverlauf keine Schwächen zeigt und dass neueste Attacken schnell erkannt und wirksam abgewehrt werden, sind entsprechende Anti-Spam-Services beziehungsweise das kontinuierliche Einspielen neuer Signaturen notwendig.

Abgewehrte E-Mails bleiben 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 die sogenannte Quarantäne-Funktion ein weiteres wesentliches Leistungsmerkmal innovativer Plattformen. Diese sorgt dafür, dass abgewiesene Nachrichten in einem eigenen Bereich gespeichert werden und für einen späteren Abruf durch die jeweiligen Nutzer 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 Nutzer in der Regel via spezifischer E-Mail-Reports, die einen direkten Zugang zu den Quarantäne-Mails ermöglichen.

Die Quarantäne-Funktion ist ein Leistungsmerkmal, das in aller Regel für die Beschaffung und Installation einer eigenen Secure E-Mail-Appliance spricht. Dies im Gegensatz zur Nutzung von «E-Mail-Security-as-a-Service»-Dienstleistungen, wie sie von

Patrick Michel ist Head of Sales bei der Boll Engineering AG, Wettingen.

ZENTRALE LEISTUNGSMERKMALE INNOVATIVER SECURE E-MAIL-APPLIANCES

Innovative Secure-Messaging-Plattformen bilden in Kombination mit Managed-Antispam-Service für Netzwerk und Mail-Server eine hoch effiziente Gesamtlösung zur Abwehr von Viren und Spam-Inhalten. Zu den wichtigsten Leistungsmerkmalen dieser auch mit «E-Mail-MTA» (Message Transfer Agent) bezeichneten Lösungen gehören:

- Nahtlose Überwachung sämtlicher ein- und ausgehender E-Mails
- Fortschrittliche Antispam-Filter (Zugangsrechte-Filter, Content-Filter, globale und benutzerbezogene Black/Whitelist-Filter, heuristische Filter, Body URL, Body Kontakt E-Mail, Object Checksum, Greylisting Filter) inkl. Reputation-Schutz-Technologie mit flexiblen Konfigurationsmöglichkeiten
- Zertifizierungen (ISCA Labs Antispam Certified / VBSpam Certified / Common Criteria EEAL Certification)
- Support für mehrere Domains
- HA-Unterstützung
- Integriertes policy-based E-Mail-Routing und Queue-Management
- Quarantäne-Funktion
- Konfigurierbare Reports und geschützter Zugriff auf Quarantäne-Datenbank via Web-Mail und POP3
- Erweiterbar mit «Advanced Thread Detection» bzw. «Sanbox»-Funktionalitäten zur Erkennung von unbekanntem Schadcode, die weit über herkömmliches Antivirus-Scanning hinausgehen

Nicht nur ankommende E-Mails sollten auf Schadcode untersucht werden, auch ausgehende E-Mails sollten entsprechend geprüft werden, bevor sie das Firmennetzwerk verlassen. Bild: Fotolia

diversen Serviceprovidern angeboten werden. Services dieser Art beinhalten in der Regel keine Quarantäne-Datenbank, was dazu führt, dass auf falsch identifizierte Nachrichten vom jeweiligen Empfänger nicht mehr zugegriffen werden kann. Die Quarantäne-Funktion bietet sich namentlich bei Filtern an, die auf «False positive»-E-Mails sensitiv sind.

Optionale E-Mail-Verschlüsselung

Nebst der Abwehr von Spam und Malware ermöglichen einige am Markt erhältliche Secure-E-Mail-Appliances auch die Verschlüsselung und Entschlüsselung von Nachrichten. Basiert die Verschlüsselung auf der sogenannten «Identity Based Encryption» (IBE), also auf Basis einzelner Nutzer und Nutzergruppen sowie auf spezifischen, in der E-Mail enthaltenen Wörtern, lassen sich E-Mails ohne Administrationsaufwand verschlüsselt übertragen. Zudem wird weder auf Sender- noch auf Empfängerseite eine zusätzliche Client-Software benötigt.

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 Secure-E-Mail-Appliance. Ist der Empfänger mittels LDAP im Unternehmensdirectory gelistet, kann er die Nachricht nach der Eingabe seiner Log-in-Daten umgehend lesen. Ohne LDAP-Einbindung ist dazu eine einmalige Anmeldung mittels Username/Password auf der Appliance notwendig.

Einfache Installation

Secure-E-Mail-Appliances lassen sich auf unterschiedliche Arten ins Kommunikationsnetz des jeweiligen Unternehmens einbinden. Im Transparent-Modus werden 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 sogenannte 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. Diese Form der Gateway-Integration weist zahlreiche Vorzüge auf. So zum Beispiel die einfache Einbindung in die bestehende Infrastruktur, die seitens der Nutzer keinen Konfigurationsaufwand verursacht und seine gewohnte Mail-Umgebung nicht antastet. Von Bedeutung sind zudem einfach konfigurierbare Routing-Funktionen oder die Unterstützung unterschiedlicher E-Mail-Domains mit der Möglichkeit, individuelle beziehungsweise domainspezifische Filterregeln zu definieren.

«Wir bekommen nur wenige Anfragen wegen nicht zugestellter Mails»

Roman Handl ist bei der Universität St. Gallen für die IT-Infrastruktur zuständig. Er erklärt im Interview, weshalb das Bildungsinstitut das Sicherheitssystem für den Mailserver erneuerte und die rund 4000 Nutzer damit mehrheitlich zufrieden sind. Interview: Christoph Grau

Herr Handl, welchen Umfang hat das Mail-System der Universität St. Gallen?
Wir betreuen momentan zirka 4000 Mailkonten und unpersönliche Adressen. Dabei haben wir einen Durchlauf von fast einer Million E-Mails im Monat. Bei dieser Zahl sind In- und Outbound schon zusammengefasst.

Mit welcher Lösung schützen Sie Ihren E-Mail-Verkehr?
Seit letztem Herbst nutzen wir die Lösung Fortimail von Fortinet. Die Implementierung hat Sidarion vorgenommen.

Wie lange benötigten Sie für die Implementierung?
Ursprünglich hatten wir für die Umstellung drei Tage veranschlagt. Die direkten Arbeiten an unserem System konnten aber in weniger als einem Tag abgeschlossen werden, was uns positiv überrascht hat. Im Vorfeld hat Sidarion unsere Bedürfnisse durch einen Fragebogen abgeklopft, um die Lösung vorzukonfigurieren. Die Implementierung ging danach sehr schnell und problemlos über die Bühne. Die Arbeit konnten wir sogar an einem normalen Werktag durchführen, da unsere alte E-Mail-Lösung noch parallel weiterlief.

Warum haben Sie sich für eine neue E-Mail-Lösung entschieden?
Unser altes Programm war schon in die Jahre gekommen. Mit den Anforderungen an den gestiegenen E-Mail-Verkehr konnte dieses nicht mehr mithalten. Beispielsweise hatten wir mit häufigen Abstürzen zu kämpfen. Die alte Lösung war ausserdem ausschliesslich für Windows-Server geeignet. Für die Zukunft wollten wir aber eine systemunabhängige Lösung.

Warum ist Ihre Wahl auf Sidarion gefallen?
Sidarion und die Universität St. Gallen verbindet eine langjährige Zusammenarbeit. Schon unsere Firewall bezogen wir von ihnen. Aber die Entscheidung fällten wir nicht einfach aus dem Bauch heraus. Sidarion war von allen eingeholten Offerten am günstigsten. Da wir Sidarion schon als kompetenten Partner kannten und wir grosses Vertrauen hatten, ist uns die Entscheidung schliesslich nicht mehr schwergefallen.


Roman Handl ist für die IT-Infrastruktur der Universität St. Gallen zuständig.

Sind Sie zufrieden mit dem neuen System?
Wir sind sogar sehr zufrieden. Unsere Erwartungen an die Lösung wurden vollumfänglich erfüllt. Besonders die hohe Flexibilität hat uns sehr überzeugt. Daher war es uns auch leicht möglich, den unterschiedlichen Anforderungen der Institute zu entsprechen. Auch die Unterstützung von Sidarion war sehr gut. Wir haben keinen Grund, uns zu beklagen.

Welche Verbesserungen brachte Ihnen die neue Lösung?
Fortimail läuft viel stabiler und zuverlässiger als unsere alte Anwendung. Mit der alten Lösung konnten wir bereits 95 Prozent der unerwünschten E-Mails herausfiltern. Dieser Wert ist mit Fortimail definitiv nicht schlechter geworden. Da die Lösung in vielerlei Hinsicht schon vorkonfiguriert ist, sparen wir viel Wartungsarbeit. Zuletzt sollte auch nicht unerwähnt bleiben, dass Fortimail deutlich günstiger als die Vorgängeranwendung ist.

«Mit der alten Lösung konnten wir bereits 95 Prozent der unerwünschten E-Mails herausfiltern. Dieser Wert ist definitiv nicht schlechter geworden.»

In welchem Umfang nutzen Sie die Lösung?
Bei der Auswahl hielten wir uns streng an die Empfehlungen Sidarions. Aktiv nutzen wir den Anti-Viren-Scan und die Anti-Spam-Funktion. Diese beinhaltet eine IP-Blacklist, einen URL-Filter, die sogenannte Greylist, den Image-Scan und Forged IP. Einzig den Bayes-Filter nutzen wir momentan noch nicht.

Wie gehen Sie mit «False Positives», also mit Falscherkennungen, um?
Diese werden in den Quarantänebereich der User verschoben. Täglich werden die Nutzer auch über diese E-Mails informiert. Sollte die E-Mail fälschlicherweise dort gelandet sein, kann der Nutzer die Adresse selbst zu seiner Whitelist hinzufügen. Ausserdem landen alle von unseren Usern verschickten E-Mail-Adressen automatisch auf einer Whitelist, um fälschliche Zuweisungen zu minimieren. Für wichtige Sachen, beispielsweise interne Newsletter, führen wir auch eine systemweite Whitelist.

Wie bewerten Ihre User die E-Mail-Lösung?
Ich habe bisher fast nur positives Feedback erhalten. Wir bekommen nur relativ wenige Anfragen bezüglich nicht zugestellter E-Mails oder Fehlern bei der Spam-Filterung. Ich gehe daher davon aus, dass unsere User sehr zufrieden sind. Statistisch haben wir dies aber nicht erhoben.