Postini™ Security Overview:

How Postini Protects and Secures Its Customers' Email

Introduction

Because email is such a vital communications channel, email systems have become an important intellectual property component for organizations of all kinds. While Internet email is a fast, convenient, efficient and cost-effective communications vehicle, its universal access makes companies who use it vulnerable to an increasing onslaught of spam, viruses and other email-borne threats.

As the largest and top-rated managed service provider[1] for email security and spam filtering, Postini has a significant advantage in fighting spam and viruses, and protecting critical intellectual assets from malicious attacks. More than 3,600 customers trust Postini to preemptively processes their email; the company handles more than 400 million SMTP connection requests per day.

Postini's award-winning services combine advanced technologies with industry-standard policies and best practices to protect its customers' communications. Postini's security policies and programs are designed to maintain the availability, integrity and confidentiality of its systems and of its customers' data. This paper looks at Postini's multi-layered security strategy, which encompasses the following components:

- Organizational security
- Physical security
- Network security
- Application security
- Host security
- Operational security
- Privacy and data integrity

Organizational Security: Policy Protections

Organizational security is the keystone of Postini's security architecture. It is the security staff and the policies they develop that define and maintain the effectiveness of the physical, network, application, host, operational, and privacy components.

Postini employs full-time, experienced Information Security staff that directs the company's information security program. They are responsible for developing, documenting, and implementing security policies and standards and reviewing all system-related security plans throughout the company's internal and production networks. The security staff is also responsible for monitoring compliance with established policies by conducting security risk assessments and internal audits on a regular basis. As part of its security program, the security staff has established a computer security incident response program so the company can quickly and effectively recognize, analyze, and handle information security incidents and threats.

Postini's information security policies and program are based on the ISO 17799 standard[2], the most widely accepted IT security standard in the world. This international standard consists of a comprehensive set of controls comprising best practices in information security, and provides a solid framework for building a secure infrastructure. The ISO 17799 standard serves as the benchmark for commercial enterprise conducted over the Internet.

[1] - HTTP://WWW.POSTINI.COM

[2] - HTTP://WWW.ISO17799SOFTWARE.COM

In addition, Postini has received independent verification of its operational integrity and security best practices from two auditing standards. Postini is WebTrust certified[3] and has received its SAS-70 Type II audit report[4]. These audits certify that Postini has disclosed its business and security practices, and been audited to verify it follows those practices.

Physical Security: Building Infrastructure Protection

Postini currently maintains four production systems. Each system comprises a primary-secondary pair of data centers to provide disaster recovery and business continuance in the event of a failure. These data centers are located in two co-location facilities. The four primary data centers are located in the Savvis Communications facility in Santa Clara, California, the same highly secure facility that Amazon, Google and eBay use. The four secondary data centers are located at the highly secure Equinix facility in the greater-Chicago area. These secondary data centers are designed as dedicated backups with remote switch-over to allow authorized personnel to switch over operations if necessary. The geographic location was carefully chosen to limit overlap of catastrophic events. The Chicago facility resides on a different tectonic plate for earthquake protection and is serviced by a different power grid and Internet loop to mitigate the risk of massive power outage or Internet network failure.

All data center buildings are engineered with special protections and environmental controls to safeguard equipment and systems. Protections include water and heat connected to HVAC temperature controls, backup power supplies and generators, and fire suppression systems. Raised data center floors and seismically-protected equipment protect against earthquake damage.

All facilities feature onsite 24x7 security guards, augmented with external and internal closed-circuit TV video surveillance and comprehensive access controls. Postini has its own locked cages in these facilities, and only select authorized Postini employees have authority over access to the cages. Digital key and hand-scan geometry verification[5] checks are required for entry to each facility.

Network Security: Hardware System Protection

The network architecture supporting the email processing system is designed for maximum reliability and uptime. The production network consists of multiple autonomous database/processing/storage instances that support different groups of customers. The production network's instances are duplicated at the backup site, configured to mirror all mailflow operations. The processing instances are internally load-balanced to evenly distribute processing and communications activity across network links and CPUs for best I/O performance and traffic throughput.

Subsystem redundancy within the clusters provides a high degree of fault tolerance to counteract unexpected hardware or software failures. If one computer system or component fails, a duplicate system or component automatically takes over.

Application Security: System Architecture Protection

Postini fundamentally provides email security protection through its advanced, patented pass-through technology that processes email in memory, in real-time, through a highly secure system architecture.

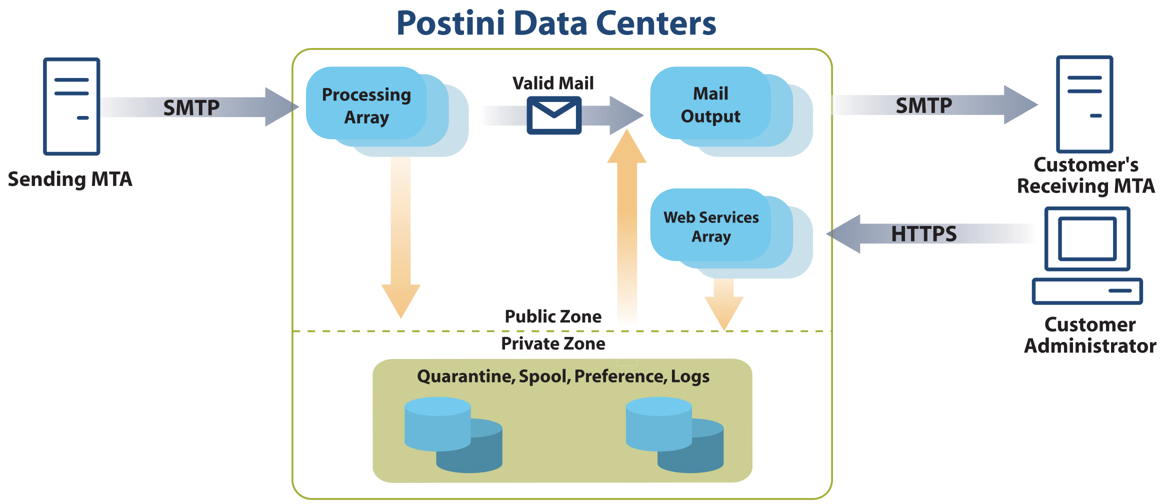
As shown in Figure 1, the system architecture is divided into public and private security zones. The public Internet zone processes the flow of email and handles customer web access. During pass-through processing, legitimate email is instantly delivered to each customer's destination mail server, from memory, unless it is suspected of harboring a virus or fits a spam profile. Depending on customer preference, suspicious email is either tagged and delivered, or quarantined to a web-accessible storage area for client (administrator and/or end user) review. Access to the web-based administrative console, for company administrators, or to the message center for end-users, is handled through Secure Socket Layer (SSL) sessions, an industry-standard public key cryptography methodology for authentication and encryption. Passwords are encrypted during network transport and also stored encrypted in databases.

[3] -http://www.cpawebtrust.org

[4] - http://www.sas70.com

[5] - http://www.biometricgroup.com/reports/public/reports_hand-scan.html

Figure 1 **Postini Data Center System Architecture**



The private zone is reserved for storing quarantined messages and customer profile and preference information. All user information, not just highly sensitive information, is protected in this area, and user configurations are processed automatically by software. Only authorized services are allowed to traverse the two networks, and only authorized personnel are allowed access to the private network.

Postini quarantines suspect messages in a proprietary database/file system called RDDB. RDDB uses fixed record lengths, meaning that if someone were to somehow access a record, they would not be accessing a whole message. Further, RDDB stores message headers and bodies separately from each other, making it still more difficult for a would-be snoop to access quarantined messages. Finally, all quarantined messages are written to disk four times. They are written to two redundant RDDB servers, both of which use mirrored storage. This design virtually eliminates the possibility of message loss.

There are three instances where valid email might be written to disk. The first two result from false positives in quarantined email or from email delivery delays (caused by extremely large message attachments). Both constitute an extremely small percentage of messages processed. The third instance, disaster recovery mail spooling, is a by-request option that allows Postini to store a customer's email in the event the customer's mail servers are unavailable for any reason. Messages are stored in a secure database until the spooling feature is deactivated by the customer.

Host Security: Software System Protection

As mentioned previously, the processing software is proprietary to Postini. Systems and system upgrades intended for the production network are built using an automated process. The automated build scripts deliver consistency, eliminate human and administrative error, and include tests to verify post-processing integrity after installation.

Third-party software applications are closely evaluated by the security staff before implementation. All third-party software security patches and upgrades are thoroughly vetted and tested before they are applied to production servers.

Postini's security team strengthens the system security through vulnerability management implementations. These programs conduct test exercises against the email processing and database servers to identify and correct areas of potential exposure. The programs also include a repair management process that tracks system restoration against a repair timeline.

Operational Security: People Protection

Postini's security policies and procedures also cover the company's personnel policies and daily operations. Depending on their position within the company, Postini conducts criminal, personal reference, education and financial background checks on employees prior to employment. At time of hire, employees are provided security awareness education that details the company's policies and procedures, and information security training is provided quarterly at a minimum.

Physical access to the data centers, as well as network access to the private zone, is restricted to authorized administrative personnel. Data center system administration is conducted over encrypted SSH (secure shell) connections that provide authentication protection for secure remote communications.

Operations employees are thoroughly trained on processes and procedures before they are cleared to conduct them, and disaster recovery and switch-over processes are rehearsed by all relevant personnel at least twice a year.

Privacy and Data Integrity

Postini understands the sensitive nature of the emails that pass through its network, and its security policies and procedures are designed to protect the confidentiality of its customers' sensitive information. Privacy is protected first and foremost by Postini's unique pass-through processing system. The entire process is fully automated. No manual processing is carried out on emails that pass through or are quarantined in the network without customer consent.

It is important to note that hundreds of financial institutions that must comply with the 1999 Gramm-Leach-Bliley (GLB) Act protecting consumers' personal financial information, as well as medical institutions and insurance companies who must comply with the U.S. Department of Health information privacy rules (HIPAA), rely on Postini to protect their highly sensitive and confidential email transactions.

Postini is also committed to honoring the privacy of users. The following excerpts are taken from its privacy policy statement[6], and demonstrate its professional code of integrity and responsibility:

- Postini does not require users to provide personal contact or demographic information. Customers can deactivate services at any time by turning application settings off.
- Postini never sells or makes available individual names, lists of users, or aggregate data to any third parties for gain.
- User configuration information provided to Postini is used explicitly to deliver services that match the client's requirements and not for any other purpose.
- All user-specific information and email message information, including content, addresses, categorizations, and IP addresses, is kept strictly confidential.

Summary

When you entrust your company's email to Postini for virus and spam protection, you can feel confident that the privacy and integrity of your communications are secured through a multi-layered security strategy that combines information security policies and best practices with patented, state-of-the-art processing technology. Postini adheres to three essential security principles-availability, integrity, and confidentiality-in its stated policies and procedures and professional conduct. With Postini, you can be assured that your sensitive intellectual property is in secure, professional hands

[6]– HTTP://WWW.POSTINI.COM/COMPANY/PRIVACY.HTML

About Postini

Postini, Inc. is the industry's leading provider of email security and management solutions that protect email communications infrastructure by preventing spam and other SMTP attacks from reaching the enterprise gateway. Postini's patented managed services model utilizes exclusive preEMPT™ technology to eliminate spam and viruses, stop DoS and directory harvest attacks, safeguard content, and improve email performance. Founded in 1999, Postini processes more than one billion email messages per week for more than 3,600 companies. By blocking spam, viruses and attacks before they can reach the enterprise email gateway, Postini Perimeter Manager™ assures complete email security while saving bandwidth, conserving server capacity and minimizing administrative costs.

postini®
PREEMPTIVE EMAIL PROTECTION

Headquarters
Postini, Inc., 510 Veterans Boulevard, Redwood City, California 94063
Toll-free 1-866-767-8461
Email info@postini.com
Web Site www.postini.com

For more information or to see if your organization qualifies for our free 30-day, no-risk trial of Postini Perimeter Manager, call toll-free 1-888-584-3150, email us at sales@postini.com, or visit us online at www.postini.com.