Protecting the delivery of legitimate email

Osborne Clarke case study

At Osborne Clarke, one of Europe's most respected and dynamic law firms, email has become the hub for all business activity and is the main form of communications with clients. As such, a resilient email infrastructure is vital in supporting a 24/7 business operation.

Context

Osborne Clarke is one of Europe's most respected and dynamic law firms. Their success, recognized by the UK Law Firm of the Year award, 2006, is the result of delivering excellent, business-focused legal advice in an energetic, straightforward and efficient way.

Supporting their clientele and business operations, which includes over 700 people active in 18 locations across Europe and an office in the US, requires considerable investment in technology. Email has become the hub for all of Osborne Clarke's business activity and is the main form of communications with clients.

Nathan Hayes, Head of Infrastructure and Technology at Osborne Clarke elaborates: "Email has always been central to our line of business applications. Exchange is the communications hub for our content management system, client management system and many of our legal applications. As early adopters of unified messaging technologies, faxing to and from desktop is done via Exchange, even voicemail is accessed via our people's inboxes. As such email is a fundamental mechanism for all forms of communications with our clients."

Challenge

Like most businesses, Osborne Clarke was experiencing increased volumes of spam. In late 2006, they became a target of a significant email-based distributed denial of service attack, receiving a massive 1.5 million spam emails in a day.

The existing on-premise anti-spam software was under severe strain, but it was the ISP relay that had trouble with extreme peaks of spam traffic, causing the email service to slow to an unacceptable level, not to mention the near complete utilization of bandwidth. Nathan Hayes decided a new solution was required to maintain an acceptable level of risk. He started to evaluate outsourced email security technologies which were more resilient and scalable.

Previously all spam that was quarantined would be filed into each user's spam folder on their PC. Significant time was spent by users on both managing the spam as well as searching through the quarantine folder for legitimate email that had been wrongly quarantined. This increasing problem known as 'false-positive email', heavily impacted on user productivity and satisfaction.

At a glance

Company

- Osborne Clarke (www.osborneclarke.com)
- Industry: Legal
- Employees: 1,000+

Infrastructure

- Microsoft Exchange
- 4 Locations
- 20 domains

Results

- Eliminated spam and latency problems
- Increased user productivity and user satisfaction
- Reduction in help desk queries
- Increased control over email infrastructure
- Access to a carrier-grade infrastructure
- 'Always-on' email facility
- Predictable, per user annual cost

Solution

Osborne Clarke comprehensively evaluated Mimecast and a traditional Managed Service Provider. Mimecast became the obvious choice for Osborne Clarke, as it provides 'unified email management' delivered via the Internet. Mimecast unifies the three major elements of email management: security, continuity and archiving into a single online system controlled in real-time via a rich web console.

Benefits

Moving to Mimecast meant Osborne Clarke could take advantage of a triple resilient, carrier-grade infrastructure and eliminate its spam issue. Mimecast's CEO Peter Bauer explains: "Mimecast's security approach to email operates by applying multiple real-time security tests on-the wire or in protocol. If the email is spam, the connection is dropped and the spam is left undeliverable at source."

Mimecast's approach pays off in a big way: "Traditional email / security technologies use on-disk methods whereby all mail is accepted to disk before applying security checks. Consequently any influxes in spam cause delays and place severe processing strain on internal infrastructure. However, Mimecast's on-the-wire approach means 99% of spam is dropped, and our customers are unaffected by increased volumes of spam and email-based denial of service. Quite simply, spam is left with the spammers," explains Peter Bauer.

Nathan Hayes highlights: "By moving to an online service, we are able to remove the burden of managing hardware and software onsite. Most importantly, Mimecast gave us the results we were looking for during our extensive evaluation. We were brought onto the service within days, and instantly received the protection we required to eliminate spam and latency problems. In the first week the service was stopping in excess of 1.5 million spam messages a day. We have freed up time and resource that had been locked in battle with spammers. For example, we no longer need to manage any quarantine, and upgrades to the system are performed by Mimecast."

About Mimecast

Mimecast is a leading provider of essential cloud services for Microsoft Exchange. Mimecast delivers enterprise email management services that include security, continuity and archiving. This suite of services provides total end-to-end control of business email, while minimizing risk and reducing both cost and complexity. Founded in 2003, Mimecast serves thousands of customers worldwide and has offices in Europe, North America and Africa.

> **"By moving to an online service, we are able to remove the burden of managing hardware and software onsite….We were brought onto the service within days, and instantly received the protection we required to eliminate spam and latency problems."**
>
> Nathan Hayes
> Head of Infrastructure and Technology
> Osborne Clarke