Case Study

mimecast

Mimecast helps broadcaster Network 10 eliminate email-borne malware and false positives

Challenge

Media organizations are particularly vulnerable to outside attacks due to their high profile. Network 10 has a mature IT practice for resolving ransomware attacks, but reactive response and remediation are time and resource-intensive activities.

"In the last two to three years, we have seen a significant increase in malicious email attacks including URL-type attacks," says Jason Tuendemann, Chief Information and Technology Officer with Network 10.

Solution

Network 10 evaluated several email security solutions, and after a proof-of-concept selected Mimecast Email Security, which was appealing for its cloud design, robust email filtering, archiving capabilities and tight integration with Office 365. Importantly, the proof-of-concept showed very few false positives.

At a Glance

- Supports 1,200 email users across multiple sites
- Requirement to build a robust email filtering environment that mitigated false positives
- Improved threat detection availability and security of email as a core business tool

Company:
As one of Australia's three free-to-air TV broadcast services, Network 10 operates a fast-moving media environment that relies on online collaboration amongst its 1,200 employees.

Products:
Email Security

Benefits:

- Immediately reduced the number of malicious emails and URL-type attacks
- Timely delivery of business critical emails without the risk of false positives
- Each month the Mimecast platform filters nearly 3,000,000 emails, rejecting 80% of inbound messages and detecting over 50 malware samples and 250 potential whaling attacks
- Seamlessly integrated with Microsoft Office 365™

"We receive a lot of information from the outside, so we have to be very careful about how much we block," Tuendemann explains. "Delivery of information to the business needs to be very timely particularly with news operations. So it's a balancing act to decide how much filtering you put in place; there's nothing more frustrating for people than having legitimate email blocked."

Network 10 coupled its Mimecast implementation with training for employees to help them identify and avoid phishing scams and malicious URLs.

> **"The best fix for malware is to stop it from coming into the organization in the first place. Mimecast has done that for us. "**
>
> *Jason Tuendemann,*
> *Chief Information and*
> *Technology Officer, Network 10*

Summary

"Since implementing Mimecast we haven't suffered a single URL type incident," Tuendemann says. 80% of incoming email is blocked as spam or malicious, including 50 malware samples and 250 potential whaling attacks avoided per month. IT staff now have time to focus on other tasks, and through education Network 10 employees have a heightened awareness of the importance of security.