Case Study

mimecast

MAZARS

Mimecast Helps Mazars Strengthen Cyber Resilience and Prepare for GDPR

Protection against advanced email borne cyber threats like ransomware keeps customer data safe and puts the firm on a proactive data security footing.

Context

Mazars is an international, integrated and independent organisation, specialising in audit, accountancy, tax, legal and advisory services. The firm's offices in the Netherlands employ a staff of 600 people who work hard every day to make a difference to their clients.

As a professional services firm dealing with often sensitive and personal client data, the firm has always been acutely aware of its security responsibilities.

As IT director Frank Keessen puts it: "It's unthinkable that we should allow our clients' information to fall into the wrong hands. In fact, guarding our IT systems against cyber threats is crucial to our reputation and to client trust."

At a Glance

Company

- Mazars Netherlands
- Industry: Accountancy
- Email users: 600

Objectives

- Protection against data loss and advanced security threats
- Email system that supports Dutch retention laws and GDPR compliance
- Minimal overheads and administration

Benefits

- Proactive 'cyber resilient' security posture
- Attachment Protect blocking on average 44 bad attachments per month
- URL Protect blocking an average of 209 bad links per month

New Threats

However, Mazars extensive use of email to communicate with clients and colleagues, coupled with the emergence of an array of new email borne threats has made managing email security a lot more challenging.

"The days when email security issues were limited to spam and general malware are gone," Frank said. "Hackers have got much more sophisticated and, over the past couple of years, we've seen a large rise in ransomware attacks, mainly delivered via email attachments or malicious links in emails."

Amlified Consequences

On top of that, the potential impacts of a successful attack are set to become much more significant under GDPR, for instance with loss of customer data punishable with huge fines.

"If our commitment to client confidentiality and data security wasn't enough to make us take emerging risks seriously, then the punishments that can be levied under GDPR would certainly focus the mind," Frank explained.

Close At Hand

Mediclinic already had an operational mail and tracking solution in place, so the return on investment offered by Mimecast needed to be substantial enough to justify its deployment.

Key Points

- Mimecast blocks 44 bad attachments per month
- Mimecast is blocking an average of 209 bad links per month

"Our ROI goes far deeper than just financial return," explains Thomas, "and the value offered in terms strengthening our governance process to suit our operations in the Middle East as well as containing potential reputational risk is immeasurable."

Advanced Protection

Frank and his team initially deployed two elements of Mimecast Targeted Threat Protection. Attachment Protect automatically sandboxes all attachments as they pass through the Mimecast secure email gateway, which all but eliminates the threat from malicious attachments.

"Mimecast gives us excellent protection against weaponised attachments, scanning every file at the Mimecast cloud to identify and block threats before they even get to our network," Frank explained. "Attachment Protect is defending us against a lot of ransomware attacks, blocking on average 44 bad attachments per month."

Similarly, URL Protect, inspects and rewrites every link passing through the gateway in real time – and scans on-click – protecting all devices from delayed exploits.

"We're simply not seeing any bad links getting through any more," Frank said. "Mimecast is rewriting thousands of links, and blocking an average of 209 bad links per month. I'd glad to say that ransomware events like WannaCry simply passed us by."

Cyber Resilient

Mimecast doesn't only give Mazars the protection it needs today. Frank also feels its proactive stance on emerging threats helps to future proof its defences – giving it a degree of the cyber resilient that the boardroom increasingly demands.

"Issues like GDPR plus events like WannaCry and Petya have really pushed cyber security up the boardroom agenda, so it's great to feel we are one step ahead. That's down to the advanced protection we get from Mimecast, as well as its focus on addressing threats before they become issues for us. For instance, we are currently looking at adding Impersonation Protect to our set up, to guard against CEO fraud-style impersonation attacks."