Case Study

mimecast

How Derry and Strabane District Council secured essential services against a growing cyber threat

Derry City and Strabane District Council provides essential public services for around 150,000 people and more than 5,000 businesses across the Derry City and the Strabane District area of Northern Ireland.

Many of those services rely on the council's technology infrastructure in one way or another so keeping the council's network up and running is a vital task, explained Paul Jackson, Digital Services Manager.

"Our network is really important," he explained. "It needs to be up 24/7.

If it's not, then people can't work and services suffer, which is bad for the community and bad for the council's reputation. In addition to this we do our own payroll, so if the network is down, we can't pay people or our suppliers."

At a Glance

- Supports 650 email users in multiple sites across Derry City and the Strabane District area of Northern Ireland.
- The Council required sophisticated protection against advanced email threats including impersonation and ransomware attacks.
- It wanted to make more efficient use of IT support time and protect continuity of Council services, by defending email as a primary communication and collaboration tool.

Company:

Derry City and Strabane District Council provides essential public services for around 150,000 people and more than 5,000 businesses across the Derry City and the Strabane District area of Northern Ireland.

Products:

Email Security

Benefits:

- Highly effective defence against sophisticated email borne attacks – blocking impersonation attacks, weaponized attachments and malicious URLs.
- In one week, the Mimecast platform filters up to 40,000 emails, rejecting around 30% of inbound messages.
- Easy deployment and responsive support helped to accelerate ROI.
- IT team freed from manual, time consuming remediation, and able to concentrate on higher value activity.

A Vital Business Tool, Under Attack

Late in 2018, the security of the council's email system was reevaluated.

Paul said: "Email security is very important, though it's not just email security. It's security of the whole network and one of the main entry points to the network we need to keep secure."

A new breed of sophisticated cyber-attack techniques was not only putting the council's on-premises email system under strain, they were also threatening the integrity of the entire network – and given that the council has around 650 email users across 30 sites, managing that threat was essential.

"We've definitely seen an increase in things like impersonation and ransomware attacks," Paul said. "In some ways, the public sector is more open to that kind of attack. We're a public body so the names of our key staff are in the public domain which makes it easy for someone to set up a fake email account and ask for a payment to be made."

Running to Catch Up

Naturally, the council had email security systems in place, with Mimecast Email Security having proved highly effective in defending against more traditional malware and spam.

"If you think about it, everybody in the area will send emails to the council at some stage, so if you look at our stats, we get 30,000 or 40,000 emails a week," Paul said. "Of them, 20 to 30% are held by Mimecast because they are carrying malware or are spam."

"However, new, more sophisticated attacks like emails containing malicious attachments and URLs, delayed exploits, or impersonation emails are designed to avoid that kind of security.

That was compounded by the fact that we have so many users over so many sites, some of them very small. We wouldn't necessarily get to hear about a user clicking on a link or whatever until maybe we got a virus alert."

"It's peace of mind for me because I know we're on top of things. I know what's out there and I know what Mimecast is blocking, so now we know we're safe and secure"

Paul Jackson,
Digital Services Manager at Derry City and Strabane District Council

As a result, Paul's team was on occasion, reacting to incidents, which took up valuable time that could have been spent on higher value activities – in fact, that manual approach was ineffective even when specific threats were known.

"Say a local company or institution got compromised," Paul explained. "We'd see the same email coming in to maybe 100 people in the council. We'd then have to manually warn staff not to open it. By then, 10, 20 people might have clicked on a bad link or opened an attachment, so we'd have to remotely scan or go around and scan all their machines."

A Ready-Made Solution

That security gap along with the increased focus on public sector security following attacks on the NHS, plus the potential impact of a successful attack, was giving Paul cause for concern.

"A successful attack could see employees and suppliers going unpaid. We would also not be able to deliver services such as waste collections, economic development work, and even council meetings could be affected. It could take us a few hours or days to get back up and running, so there would definitely be an impact."

Help was at hand, however, as Paul knew that he could call on a ready-made solution from Mimecast – an extra layer of security specifically designed to detect and disarm these more sophisticated attacks.

Mimecast Targeted Threat Protection (TTP) uses a range of analysis techniques, attachment sandboxing and on-click URL scanning to defend organizations against spear-phishing, ransomware, impersonation and other targeted attacks.

"Mimecast actually contacted me to offer a free trial," Paul said. "So, we ran a test for a month and looked for user feedback, which was positive. They'd not noticed any real change in the user experience, and we knew from the admin console stats that it was working very well to protect them which helped me sleep better at night."

Outstanding Support Delivers Rapid ROI

Based on that trial, Paul and his team decided to roll TTP out to all 650 users, and the support he received from Mimecast was vital to maximizing the value of that investment quickly.

"The deployment was actually really straightforward," Paul explained. "But where Mimecast really added value was in helping us to configure and understand the solution in detail. They didn't just deploy it and leave us to it; the support team was absolutely focused on making sure we made the most of it.

"So, we had lots of help configuring the solution. There were lots of screensharing sessions, lots of advice on what options to select, and why. It wasn't just 'tick this', 'tick that', there was a whole lot of explanation about what each option was and what it did. Then there were follow up calls to make sure there were no issues. Mimecast looked at the email flow regularly to see if there were any pain points we needed to address."

According to Paul, that guidance, the insight and control it gave him and the team, was incredibly valuable: "It was really important to maximizing ROI and doing it quickly," he said.

Proactive Protection

Mimecast TTP has proven a highly effective defense against sophisticated email borne attacks, blocking more than 100 impersonation attacks, sandboxing around 20,000 attachments and securing around 6,000 in email URL clicks every month.

"It's working incredibly well," Paul confirmed. "Mimecast scans every email, even those from people we know, so any bad attachments or URLs, and a lot of impersonation attacks, are being blocked. Even if it's a delayed exploit, with the URL only pointed at malware later, that's caught too, because all links are scanned 'on click'."

"Before, users wouldn't tell us until there was a problem. Now, we can see what's going on, who is clicking on bad links and so on. Plus, any malicious URLs are blocked anyway, so even if they do click, it's not an issue."

All that means the team is spending a lot less time scanning and rebuilding machines. "We're able to be more proactive," he explained. "Looking at server management, patch management and so on."

On the Front Foot

Meanwhile, Paul has access to a wealth of data via the Mimecast Administration Console and weekly reports, which has also proven very useful.

"Before, we didn't know what was going on until we had a report from a user or the originating company when they realised they had been compromised," he said. "We had to react. Now we are more proactive. Mimecast alerts me to people clicking on bad links - so we we're not sitting blind any more. We know the people who are having issues and we can target training and advice for higher risk users"

"At the same time, I get lots of information on how email and the network is running. That allows me to plan my email strategy for the next couple of years, everything from threat trends and server capacity, to longer term issues like whether Office 365 is the right move for us."

Peace of Mind

Summing up the difference Mimecast TTP has made, Paul said: “It’s peace of mind for me because I know we’re on top of things.

I know what’s out there and I know what Mimecast is blocking, so now we know we’re safe and secure.”