

CASE STUDY

HIGH POWER TECHNICAL SERVICES

LOUISVILLE, KY – USA

CYREN EMAIL SECURITY PLUS

CYREN

Email Security Assessment Highlights Need For Additional Protection

High Power Technical Services installs and maintains satellite television systems for DISH Network in over 3,500 homes each week with a team of 300 employees. High Power is headquartered in Louisville, Kentucky, with twelve regional offices serving Kentucky, Ohio and Indiana, all supported by a very lean IT team. Email is the key communications tool that connects the employees in the offices and the engineers and technicians on the road.

HIGH POWER
THE TECHNOLOGY EXPERTS

“ The native security provided with Office 365 was not quite as robust as expected. ”

John Wells,
IT Infrastructure Manager,
High Power Technical Services

RAPID RESPONSE TO A BEC ATTACK

For its corporate email, High Power was running on-premises Microsoft Exchange with an AppRiver email security service, all managed by a third-party service provider. One day they suffered a successful Business Email Compromise (BEC) attack, which resulted in a rapid response to remediate the threat. The leadership and IT team mobilized and put in place appropriate measures to counter and recover from the attack. They then began considering options to prevent it from happening again.

TRAINING AND TRANSITION TO OFFICE 365

John Wells, High Power's IT Infrastructure Manager, recognized that no email security can be 100% effective. This is especially true of evasive phishing attacks like the BEC attack, so as an initial measure he implemented a training program using a phishing simulation service. Through continuous reinforcement this has achieved positive results, but preventing malicious and unwanted emails reaching users in the first place continued as the primary goal.

Prior to the incident, John had already been considering a migration to hosted email with Office 365, with the additional attraction of gaining embedded security. The current managed email server and security infrastructure was costly, and the financial benefits to be realized from a migration would be significant.

SUPPLEMENTING THE NATIVE SECURITY OF OFFICE 365

Unfortunately, following the migration to Office 365, it became clear that the native email security was not quite as robust as expected. It was not performing as well as the previous AppRiver service, and High Power's users were noticing that they were receiving not just malicious emails, but additional spam. Having users sifting through higher volumes of spam and phishing emails had a detrimental impact on productivity. John at this point recognized that he needed an additional layer of email security.

During his thirteen years at High Power, John had built up trust with the leadership and had the necessary support to do what was needed to secure the business. An easy option considered was to return to at least pre-Office 365 migration security levels by reinstating AppRiver, but John decided to also research the market for alternative cloud-based email security services.

PROVING VALUE WITH A REAL-WORLD PERFORMANCE ASSESSMENT

Webinars are John's primary mechanism for keeping up-to-date with new technology. Having attended a Cyren webinar on how to supplement the native security provided by Office 365, he engaged with Cyren's security specialist team. He was assigned a dedicated systems engineer who recommended conducting a two-week assessment of their live email traffic to classify and quantify what unwanted and malicious email was slipping through.

The Email Security Gap Analysis was quickly set up by creating a transport rule in Office 365 that copied to Cyren all emails already considered clean and delivered to users. Cyren would then evaluate the emails and discard those it agreed were clean, and reclassify all identified malware, zero-day threat, phishing, spam and newsletter emails. These were dropped into folders, on a dedicated email platform, for High Power to monitor. The results were immediate and compelling. The assessment detected, during the period, 1841 unwanted or malicious emails, including 1262 spam, 449 unwanted advertisements, and, most critically, 130 malicious emails that were either phishing attacks or carrying malware attachments.

DRAMATIC REDUCTIONS IN INCIDENTS AND STAFF TIME

High Power licensed Cyren Email Security, Cyren's cloud-based secure email gateway service, and had it deployed in thirty minutes. It continues to provide quantifiable results.

Since deploying Cyren, they have not suffered a single security incident, whereas one used to occur every other month and that would take two days to remediate. John suggests that this might seem trivial, but given the IT infrastructure team consists of just two people, these incidents were a serious diversion.

The second quantifiable benefit realized is the time spent managing the email security infrastructure – 50% less time than before Cyren was deployed. Active Directory integration makes life easy and helps ensure all users are protected immediately they are onboarded, with no manual changes to the email security service.

In addition, inbound email delivered to users has been reduced by about 30%. This significant reduction in unwanted emails has led to an increase in user productivity, as they no longer have to sift through them, deleting spam and phishing emails.

THE CHALLENGE

High Power Technical Services required a robust email security service to supplement the native security offered by Office 365 and complete its email security defence-in-depth strategy.

THE CYREN DIFFERENCE

- Proven effectiveness before purchase with a free Email Security Gap Analysis assessment
- In just two weeks, Cyren detected 1841 malicious or unwanted emails that Office 365 had delivered to users
- Reduced inbound emails delivered to users by 30%
- Serious security incidents reduced from one every two months to zero
- Saved, on average, a full day each month remediating incidents
- Spend 50% less time managing the email security infrastructure
- Increased user productivity