proofpoint.

HISTORIC UNIVERSITY TAKES PROACTIVE APPROACH TO CYBERSECURITY

CHALLENGE

- Stop ransomware, spam, and phishing attacks from entering users' mailboxes
- Improve the university's email reputation score
- Increase situational awareness
- Reclaim time spent remediating the impact of cyber threats for more proactive projects

SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection and integration with Palo Alto Networks Wildfire

RESULTS

- Stops 300,000 to 500,000 pieces of ransomware per week
- Significantly reduced phishing emails and clicks
- Reduced compromised accounts from 200 per month to fewer than 12
- Gained detailed visibility into threats, impact, and trends

How does a historic university with more than 16,000 students and scholars, more than 4,000 faculty members, and a wide array of programs, departments, and affiliated organizations protect its mission? By taking a proactive approach to cybersecurity and the threats that come against it.

When one school's chief information security officer arrived on campus in 2011, he saw that it needed an enterprise-class email gateway. He looked to Gartner for advice. When he saw Gartner's review of Proofpoint and learned more about it, including impressive customer references, he chose Proofpoint Email Protection.

COMPLEMENTING THE CLOUD

The university was also migrating some of its systems to the cloud. It had moved its email system to Microsoft Office 365 to reduce the cost, support requirements, and data center footprint associated with Exchange servers. Proofpoint Email Protection is deployed behind the university's Palo Alto Networks Wildfire solution and in front of Office 365. That arrangement gives the security team much greater email defense and better situational awareness.

"The change was dramatic," the CISO said. Spam disappeared as the school fine-tuned spam identification filters. Then it turned on outbound protection to eliminate persistent reputation score problems.

"It made a huge difference," he said.

TARGETING PHISHERS

With outbound email protection in place, the security team focused on reducing phishing attacks and their effects. At the time, phishing emails led to more than 200 compromised accounts per month. The CISO lobbied for deploying Proofpoint Targeted Attack Protection (TAP); his request was approved quickly. The university integrated TAP with Palo Alto Networks WildFire using simple API key-based activation. By combining the two solutions, both companies' cloud-based malware analysis can automatically align protection across the Proofpoint email gateway and the Palo Alto Networks firewall.

Right away, TAP reduced account compromises from 200 a month to fewer than 12. For the few phishing emails that got through, the school opened a support ticket with Proofpoint so that the email would be documented and added into TAP protection for everyone's benefit.

"If someone complains about getting a phishing email, I can show them the math," the CISO said. "As just one example, we saw 200,000 phishing attempts this month, and only 21 got through."

"Proofpoint serves us well by keeping ransomware out of our systems environment. We are pleased by how much ransomware Proofpoint effectively protects us from."

Chief Information Security Officer, Historic University

STOPPING RANSOMWARE

Beginning in 2016, the school saw a surge in ransomware attacks. The security team sees 300,000 to 500,000 pieces of ransomware per week trying to get into its network. In just one seven-day period in mid-2016, it received almost 500,000 pieces. Proofpoint instantly quarantines suspicious email, sandboxes it, and then determines if it is malicious.

"Proofpoint serves us well by keeping ransomware out of our systems environment.," the CISO said. "We are pleased by how much ransomware Proofpoint effectively protects us from."

VISIBILITY FOR EFFECTIVE ACTION

In the past when a phishing attack occurred, the security team sent everyone across the entire school and asked if anyone had actually clicked on the email. Accurately gauging the impact of any given email was difficult.

Proofpoint reporting capabilities give the team instant visibility with detailed data for rapid response. Now if a phishing email gets through, the team knows exactly who and how many people received it. They can contact anyone affected or lock their accounts for safety. Proofpoint lets the team control phishing impact, immediately respond in exactly the right place, and avoid wasted time and communications. Compromised accounts are now a rare exception. This shift has freed the security team to work on more advanced security efforts.

"Proofpoint is tactical and precise," the CISO said. "It's made incident response a manageable event. I'm very comfortable using the technology. It's easy for me to navigate, find exactly what I'm looking for, generate reports, and study trends over time."

IMPACT ON THE FUTURE

Although the security team protects the university 24 hours a day, the growing volume and variety of threats still pose a tremendous concern. And they are also attacking other higher education institutions, corporations, and law enforcement agencies.

"Sometimes people consider security concerns to be overzealous," the CISO said. "But sometimes conditions develop that are serious and impactful. We have to respond. We can't just sit here until someone figures out why these forces want to attack us. We have to mount a defense and protect the mission of the university. Proofpoint helps us with that."

The CISO hates seeing bad actors attack institutions that do good, honorable work that benefits society. He feels a responsibility to share what he's learned, so that together, higher education institutions can work together to more effectively fight cyber threats. He encourages his peers at other institutions to take a close look at Proofpoint because he knows firsthand how effective it is.