CASE STUDY

proofpoint

WRIGHT STATE UNIVERSITY EXPELS EMAIL THREATS

MINIMIZES RISK WITH PROACTIVE DEFENSE

CHALLENGE

- Secure intellectual assets against phishing-based credential theft
- Protect thousands of email boxes against malware and ransomware
- Reduce time spent tracking threats and reimaging machines

SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection

RESULTS

- Significantly increased ability to detect malware and block access to malicious URLs
- Gained ability to proactively fight threats with detailed data
- Saved time spent fighting threats for higher productivity on other IT projects

Wright State University is located near Dayton, Ohio and serves more than 18,000 students. To advanced cybersecurity hackers, the 2,000 to 4,000 new students that arrive on campus each year look like easy marks for credential theft. Until they run into Wright State's powerful security strategy, that is.

Wright State faces a huge challenge in securing email and other communications. The campus community is highly transient; large numbers of students, faculty, and administrators come and go during the academic year. For example, 2,000 to 4,000 new students arrive at the start of each semester and receive email accounts. From a security standpoint, Wright State's IT team has its hands full.

AN IDEAL TARGET

About 100 IT staff members manage campus networks and IT services. Responsibility for securing more than 10,000 mailboxes falls to two teams: the email and collaboration software team and a systems-programming group.

"We were seeing everything from general malware infections to phishing, file locking, and ransomware attacks," said Patricia Vendt, Email and Collaboration Software Administrator at Wright State University. "The sheer volume of mailboxes targeted by credential phishing attacks was becoming overwhelming."

The school hosts thousands of email accounts, and students receive hundreds of messages. Emails arrive from administrative departments, professors, student groups, and other campus senders. Students often don't understand how university communications operate. Knowing which senders are legitimate and which aren't can be tricky.

Phishing emails closely mimic Wright State help-desk notifications and other regularly used university services. These emails look official, so students often do whatever the attackers ask—usually instructions to enter their credentials. At the same time, a growing number of international students speak English as a second language. They often don't recognize the subtleties of English that might make native speakers question an email's authenticity.

INFORMATION AT RISK

Phishing perpetrators aim to steal student credentials to gain access to copyrighted library materials and to the statewide OhioLINK network. If they're successful, they have access to 50 million books; more than 150 electronic research databases; millions of electronic journal articles; 85,000 images, videos, and sounds; and nearly 50,000 theses and dissertations from Ohio students.

When the university help-desk team received security alerts, a staff member had to scan the user's machine from the central IT department. If that wasn't possible, the technician would have to track down the user and physically reimage the machine. The staff would spend hours and days of time mitigating the effects of users falling for the malicious emails.

TECHNOLOGY, SIMPLY APPLIED

A small team just can't keep pace with high volumes of attacks on a constantly

"Proofpoint gives us a focused approach to solving specific threat problems."

Craig Woolley, Chief Information Officer, Wright State University

changing user base. So Vendt and John Meyers, Lead Systems Programmer at Wright State University, looked for technology to detect and block email threats.

Vendt attended a gathering of Proofpoint customers. She was impressed by the high-quality presentations and the caliber of other companies that use Proofpoint. Meyers networked with other schools that had similar issues. He found that they also use Proofpoint solutions.

Wright State chose Proofpoint Email Protection and Proofpoint Targeted Attack Protection (TAP) to help defend against email-based attacks. Proofpoint Email Protection defends against unwanted and malicious email, while Proofpoint TAP protects from advanced threats that use malicious attachments and URLs.

"We did a short proof of concept with TAP and were easily convinced," Meyers said. "It took only 30 minutes to activate the license and deploy. It was simple."

Today, Proofpoint is an integral part of Wright State's security strategy. It sits in the email flow behind the university's network firewalls and intrusion prevention system and in front of Microsoft Office 365. Email flow is key; more than 90% of today's targeted attacks occur through email.

WORKS BETTER, SAVES TIME

"Antispam and dynamic reputation filtering features in Proofpoint Email Protection helped tremendously," Vendt said. "We see minimal amounts of spam, and we are able to work with our small staff to investigate security alerts."

Wright State also sees a huge uptick in its ability to detect malware and malicious URLs. The Proofpoint TAP dashboard delivers near-real-time notification and detailed information about attack campaigns and internal targets. That enables the university to see patterns and tools used in attack campaigns. With this insight, the IT team can easily tell broad-spectrum attacks apart from those that target executive leadership and other high-value employees.

"TAP gives us much better information for incident response," Meyers said. "We know what we're dealing with, and we're much more proactive in reaching out to users who have clicked on an infected email."

ON-POINT SUPPORT

Vendt and Meyers are much more confident about the university's security posture and now can focus on other important projects. A Proofpoint engineer also regularly works with the team to update rules, tune configurations, and continuously make the solutions more effective.

"We're very pleased with Proofpoint," Meyers said. "Support is excellent. The Proofpoint solutions are better than similar offerings from Microsoft."

MAXIMIZING PROTECTION, MINIMIZING RISK

With robust email defense in place, Wright State has made compromising users' credentials far more difficult for bad actors. As the IT team continues to add layers of protection against cyber threats, it helps reduce risk for the university as a whole.

"Proofpoint gives us a focused approach to solving specific threat problems," said Craig Woolley, Chief Information Officer at Wright State.

For more information, visit www.proofpoint.com.