CASE STUDY

Phishing Attacks Prompt Private University to Seek Cybersecurity Help From BitLyft

BitLyft CYBERSECURITY

ORGANIZATION:
Private university in Illinois

INDUSTRY:
Higher Education

STUDENT ENROLLMENT:
4,900+ (2,900 undergraduate) students

LOG SOURCES:
30 with 10,000+ individual sources from: HP, Palo Alto, Cisco, Aruba, Nexus, Office 365 and Azure.

KEY IMPACTS:

- Identified compromised accounts
- Reduced reaction time to zero
- Generated actionable reports

"Having a partner like BitLyft eases that unsettled feeling in your mind and you can sleep better at night."
Director of Infrastructure Operations

INTRO:

In the spring of 2017, a well-known university in Illinois started to get hit with a number of phishing attempts. Over the following weeks and months, the attacks began to increase exponentially. Staff began to work a number of additional hours to remedy the situation, but the number of attacks just kept increasing. Finally, by mid-summer the university began to look to an outside source for help.

THE CHALLENGE:

Educational institutions face many challenges: large user bases, complex networks, access controls and sensitive records. This medium-sized university, with its network of 400 access locations and SMART classrooms, was no exception. At the time of the phishing attacks, the university was also being faced with staff cuts and did not have the resources to hire an additional team member. IT staff were spending hours with multiple departments working on each individual account compromise which resulted in more time at the office and less time spent at home. To help in the interim, the department formed its own security team, but its members lacked the necessary training to combat the ongoing phishing attacks. To add even more urgency to the situation, the school knew it had to resolve the situation quickly to protect the integrity of its own academic cybersecurity program.

(CONT.)

CASE STUDY

Phishing Attacks Prompt Private University to Seek Cybersecurity Help From BitLyft

BitLyft CYBERSECURITY

THE SOLUTION:

After weighing its two options of purchasing an on-prem Security Incident Event Management (SIEM) tool or hiring a cloud-based SOC-as-a-Service provider, the university chose the latter, more cost-effective route and partnered with BitLyft.

Once BitLyft installed its robust cybersecurity platform powered by LogRhythm, the university immediately began to see benefits from the enhanced visibility into their network.

"There were things we were not seeing that we should have spent time on and tried to mitigate," said the university's Director of Infrastructure Operations. "But we didn't know they were happening, so we didn't spend that time."

In addition to exposing logins from unfamiliar locations and bounces from other countries, data provided by the BitLyft team helped the university implement a process to reduce reaction time before a breach even began.

"We have closed the time down to zero on a lot of cases and are working to close it down on all of the cases," said the university's Cybersecurity Program Director.

The BitLyft team also provides a regular report to the university that outlines action items to secure its network.

"Having weekly meetings is a big benefit," continued the Director of Infrastructure Operations. "We constantly feel like we're involved rather than just working with a vendor that might stop by once a month for a 're-get to know you' meeting. We're constantly talking about issues and we've never had a case where BitLyft wasn't available or responsive."

"The thing about cybersecurity is that it's much easier to explain to your executives why you need it, than to experience a breach and have to explain why you didn't have it."

—Director of Infrastructure Operations