AKAMAI CUSTOMER STORY

Threat Intelligence Protects University

Okayama University uses Akamai for cyberattack countermeasures to keep students' and staff's devices safe from dangerous sites

22K
Devices protected from targeted attacks

DNS security prevents attacks quickly and with limited user impact

Reduced burden of phishing investigations conducted

Leading university enhances education and research activities

Established in 1949, Okayama University is a designated member of the Ministry of Education, Culture, Sports, Science and Technology (MEXT) program for promoting the enhancement of research universities, one of a handful of such institutions in Japan. Known as a "super global university," Okayama University promotes internationalization through collaboration with overseas universities and via other means to achieve world-class education and research.

Okayama University is also home to the Center for Information Technology and Management, which provides Information and Communication Technology (ICT) services to enhance education and research activities, utilizing the university's various information resources to support university administration, education, and research, in addition to promoting information literacy among undergraduate students.

Center for Information Technology and Management: Driving ICT at a global university

For some time, the Center for Information Technology and Management's Information Security Team had been handling security measures on both the personnel side and on the technical infrastructure side. With the aim of preventing increasingly sophisticated threats and strengthening the response in the event that a threat were to occur, the Information Security Team was re-launched in September 2016 as the Okayama University Computer Security Incident Response Team (CSIRT). Today, the CSIRT continues to act as the cornerstone of information security at Okayama University.

Conventional security rendered inadequate by pandemic countermeasures

Okayama University's network consists of LANs set up on the two main campuses, which are connected to each other by cables with bandwidth up to 40 Gbps. The network that connects each campus and remote site accesses the internet via the Science Information NETwork (SINET), an academic information network.

岡山大学
OKAYAMA UNIVERSITY

Okayama University
Okayama, Japan
www.okayama-u.ac.jp

Industry
Education

Solution
• Enterprise Threat Protector

Akamai

"The actual number of users connected to the network is about 16,000 students and 6,000 faculty members, including part-time teaching staff," said Masaki Murakami, Professor and Director of the Center for Information Technology and Management. "Our wireless LAN is not open to the public due to security concerns. We either have users connect via Eduroam, which enables mutual use of campus wireless LANs among primary, secondary, and higher education institutions and research institutes, or we provide a guest ID for the wireless LAN, but only if the user applies in advance."

A next-generation firewall with an intrusion prevention system was installed at the edge of the university network. For the mail server installed on campus, two levels of threat detection were employed using cloud-based and on-premises appliances to protect against infiltration from outside. However, Murakami said that with the spread of COVID-19, conventional security measures were no longer sufficient.

Phishing, ransomware, and targeted attacks

Okayama University needed to strengthen its countermeasures against malware and targeted attacks. "We allow BYOD (bring your own device) because students use their computers in class," said Murakami. "However, at present, COVID-19 countermeasures mandate that we must conduct online classes, and faculty members must telecommute using their personal devices. As more email was received off-campus and on BYOD devices without passing through the university's perimeter security, we needed to strengthen our response to ransomware and other malware."

There were also calls for attention to targeted attacks, and the team realized the importance of countermeasures. According to Keita Kawano, Associate Professor and Manager of CSIRT at Okayama University, "Targeted attacks aimed at cutting-edge technical data and other confidential information were a growing concern because they could lead to serious information leaks. In order to minimize the damage caused by Emotet and other targeted attacks that were ramping up through 2020, it was important to detect and block communication to the attackers' C2 servers as soon as possible."

Kawano continues, "It was difficult to protect the system in a timely manner with the traditional approach of manually feeding threat data provided by external organizations into the firewall." Thus, Okayama University had high hopes for a system that would automatically update threat data and block command and control (C2) servers and malware sites.

Quick and easy-to-implement DNS security solutions

The Okayama University CSIRT sought a security solution that could be implemented in a short period without greatly changing the existing environment. The team selected Akamai Enterprise Threat Protector because of its favorable cost and the fact that the effectiveness of the system had been confirmed in a proof of concept (PoC).

"I had conducted a PoC previously, out of technical interest and concern," said Murakami. "The results were wonderful, but this was before the pandemic, and there was little risk of an infected device outside the university connecting to a machine on campus, so we did not introduce the system. Under these new circumstances, we knew that Enterprise Threat Protector was the best security solution and made the decision to move forward."

The implementation process went smoothly from preparation to full operation. The actual work was limited to the configuration of Enterprise Threat Protector and the setting of a forwarder for the on-campus DNS cache server to point toward the new solution. According to Kawano, "Installation was completed with minimal configuration. The system simply operated in monitoring mode during the PoC phase and then changed to blocking mode after launch."

Installation was completed with minimum configuration. The system simply operated in monitoring mode during the PoC phase and then changed to blocking mode after launch.

Keita Kawano
Associate Professor and Manager of CSIRT, Okayama University

Fewer incident investigations and reduced workload

In addition to Enterprise Threat Protector's automatic detection functionality, the Okayama University CSIRT also uses manual allow lists and deny lists. The deny list contains dynamic DNS domains that are often used for phishing purposes and were added to the list independently by the Okayama University CSIRT. Although it is difficult to measure exact performance results due to changes in network usage, such as fewer students coming to campus in the pandemic, the operational benefits are positive.

"We have seen a decrease in the number of alerts about suspected access to phishing sites since the introduction of Enterprise Threat Protector," said Kawano. "Known threats are blocked and suspicious communications are monitored, but we rarely receive false positive reports. As the number of incoming alarms has decreased, the cost of investigations conducted in response has also decreased, which has been a big help. We greatly appreciate that we are able to improve security quickly and without impacting users."

Expanding Akamai solutions to universities throughout Japan

Over time, the Okayama University CSIRT expects these security solutions to gain a greater number of users and promote an increase in the rapid sharing of threat information. The team believes that this is an effective way to strengthen its protections.

"The more users we have, the more information we can accumulate about attacks and threats, and the more effective protection we can provide for many universities," said Murakami. "Universities in Japan are all seeking to improve their security measures despite tight budgets. We look forward to Akamai expanding Enterprise Threat Protector and other cost-effective security solutions to universities across Japan."

> We have seen a decrease in the number of alerts about suspected access to phishing sites since the introduction of Enterprise Threat Protector.

Keita Kawano
Associate Professor and Manager of CSIRT, Okayama University

岡山大学
OKAYAMA UNIVERSITY

Okayama University is a comprehensive university consisting of 11 undergraduate departments, including educational programs, eight graduate schools excluding a joint school, and four research institutes. The university has two campuses in different parts of the Okayama City area. The university Head Office is located on the Tsushima Campus with the Faculty of Letters, Faculty of Education, Faculty of Law, Faculty of Economics, Faculty of Science, Faculty of Pharmaceutical Sciences, Faculty of Engineering, and the Faculty of Agriculture. The Shikata Campus is home to the Medical School and Dental School. Sustainable Development Goals (SDGs) are one of the core pillars underlying the university's activities. The school has created the Okayama University's SDG Action Guidelines and works to contribute to education, research, and society as a whole. www.okayama-u.ac.jp

©2022 Akamai Technologies | Support | Published 03/22