Making resilient systems even stronger

Kingston University first opened its doors back in 1899 as the Kingston Technical Institute. Now, the university has four campuses serving around 19,000 students, including 5,000 international learners from 140+ countries who are supported via the university’s dedicated International Study Centre. The university has four faculties offering 260 undergraduate, postgraduate and apprenticeship degrees from fashion to entrepreneurship and from nursing to engineering. It has extensive research interests and strong links with the business community and industry partners.

Serious about cyber security

“We have adopted a variety of technologies to deal with evolving security threats and deployed them at various levels from endpoint devices through to the IT network and server infrastructure and applications.”

“Serious about cyber security

“We’ve got industry leading patch management platforms, next generation firewalls and good network segmentation. Ongoing training and awareness raising have helped us embed a culture of good online behaviours.”

Ravi Jeyanolipavan, cyber security manager, IT services, Kingston University

The COVID-19 lockdown probably didn’t make the attack more likely, but it did make diagnosis more difficult,” says Ravi. When they discovered the attack Kingston University’s IT services team got together immediately over MS Teams, but it wasn’t easy to identify the problem. Like all Jisc members, Kingston University’s subscription provides network-level distributed denial of service (DDoS) mitigation so Ravi called the Janet Network CIRT team less than half an hour after spotting the problem. The firewall logs showed a transmission control protocol (TCP) SYN flood, a common form of DDoS attack seen in the sector. The Jisc team applied mitigation within two hours to stabilise the situation.

Later, it proved to be a carpet bomb type attack, targeting every destination in a number of subnets. This made it harder to detect and to mitigate.

While Jisc’s specialists worked on this, it was important to free up bandwidth and to make sure only malign packages were dealt with so services could keep running for Kingston University’s students and staff. Jisc’s specialists were working on the problem alongside the university’s team day and night during that initial attack phase.

“Things were fully back to normal within three days,” says Ravi. “But we were worried it could happen again and, with clearing around the corner, we couldn’t risk that.”

Critical services protection (CSP) was the obvious answer and Kingston University looked into the solutions provided by Jisc as well as by several commercial companies.
"Clearing at Kingston University is as busy as the Black Friday sales"

"Jisc’s offer was the clear winner because you can mix and match to get the protection you need,” comments Ravi. “And the commercially available alternatives seem less flexible and more expensive.”

Protecting the university’s contact centre was the immediate priority. “Clearing is as busy as the Black Friday sales for us. A service that protects our phone connections so that potential students can apply for places pays for itself pretty quickly,” says Ravi.

Kingston University opted to protect other key services too, including finance systems, the VPN, student management systems, the domain name system (DNS) and access management gateway, purchasing four months of cover to get them safely through the clearing window.

Has adding an extra layer of protection slowed traffic and reduced user satisfaction?

“Having used Jisc’s CSP for a while now we can say that traffic doesn’t slow down. CSP is seamless because everything happens on the Janet Network,” says Ravi. “We’d know if it caused delays because we’d be inundated with alerts.”

Following the initial four-month cover period Kingston University decided CSP was a long-term strategic investment, giving the reassurance of ‘always on’ mitigation to protect against ever more sophisticated and frequent cyber attacks. It’s a challenge that faces all organisations operating in the UK’s higher and further education sector. The Jisc cyber impact report, published in November 2020, revealed that more than 1,100 denial of service attacks took place on the Janet Network between August 2019 and August 2020, targeting 236 of our members.

“These attacks aren’t going away, and they’re not just being perpetrated by determined loners or small groups; we are facing nation-sponsored threats,” says Ravi.

“We’ve taken out CSP for the next three years as part of a wider roadmap of new security services. When we spot something suspicious Jisc have usually seen it too and they’re already working on it. Alerts are going from Jisc to us and from us to Jisc, which helps us stay safe and also provides intelligence that supports the wider sector.”

To find out how Jisc can support your organisation, please:

Contact: securityservices@jisc.ac.uk

or visit jisc.ac.uk/critical-services-protection