LESSONS IN SECURITY

Jack Porter *looks at how universities can improve their defences in the face of mounting attacks*

Universities are increasingly a target for attackers because of their societal impact, with attackers resorting to extortion and ransomware to steal research data or knowledge and using the university's infrastructure to monetise assets or disrupt and destroy. They're particularly attractive to nation states and activists, as demonstrated by the recent attack on the Janet network in February. A distributed denial of service (DDoS) attack was launched against the mass data-sharing platform used by researchers and is reported to have affected numerous higher education institutions including Cambridge University. Anonymous Sudan claimed responsibility, citing the UK's stance on the Israel/Palestine conflict and bombing in Yemen as the reasons for the attack.

The attack against Janet highlights some of the unique challenges experienced by these institutions. On the one hand they have to ensure access is as open as it can be to facilitate learning for their students and the sharing of ideas and knowledge by researchers. But on the other the intellectual property they generate needs to be secured and protected. Balancing the two can be difficult due to the size and sprawl of these institutions' systems which creates a massive potential attack surface. But action is urgently needed, with half of higher education establishments reporting they are subjected to an attack or suffer a breach on a weekly basis, according to the government's Cyber Security Breaches Survey 2023. What's more 75 percent of those said the issue had resulted in a negative impact.

Universities should not underestimate the resources and effort required to maintain a strong security posture

Consequently, there is now a renewed focus on the need for universities to improve their cyber resilience. The Universities UK (UUK), Joint Information Systems Committee (Jisc), and the National Cyber Security Centre (NCSC) jointly released the Cyber security and Universities: Managing the risk (2023 update) report towards the end of last year, with Jisc Chair, Professor Paul Boyle, stating the sector: "ought to be doing more to reduce risk". The report itself serves as a call to arms and focuses on three key actions for senior leaders who are urged to: review the security posture to improve defences, focus on business continuity to improve response and recovery, and maintain momentum by sharing threat intelligence and expertise.

In order to improve the security posture, the report recommends focusing on four interrelated pillars: governance, assurance, technology and culture. For governance, the report recommends a corporate approach should be adopted to manage cyber security risk using Jisc's 16 questions to assess security posture. Responsibility for data should rest with assigned persons, with the executive team taking ownership and the principal investigators and deans being held largely accountable for controlling data. For assurance purposes, risk frameworks should be used to assess and benchmark areas for improvement, although the report concedes that those belonging to the Janet Network are already compelled to carry out annual self-assessments and many also adhere to the Cyber Essentials, Cyber Essentials Plus and ISO 27001 standards.

With respect to technology, the report advises a range of technical controls should be put in place as part of a defence in depth (DiD) approach and emphasises the need to move away from legacy solutions. A variety of controls are advocated from preventative, to detective, corrective, compensating (ie makes up for weaknesses in other controls) and deterrent. Detection, however, is singled out as a primary objective to prevent attacks through the gathering, sharing and analysing of attack types and techniques. Key functions include the ability to monitor and create alerts in response to incidents and issues, and the report specifically advises that technological investments should include vulnerability scanning to detect unpatched systems and a Security and Incident Event Management (SIEM) platform.

Using a SIEM enables the university to investigate and respond to incidents, but next-generation SIEMs also incorporate threat hunting and are mapped against the MITRE ATT&CK framework, providing insights into tactics and techniques used by adversaries and helping analysts stay one step ahead. The information collated can also be used for threat intelligence sharing, allowing universities to pool their collective knowledge. For example, it's possible to create comprehensive reports on ongoing and finalised security cases to share with stakeholders, making it easy to inform others on threat developments and trends and to collaborate over defence.

A SIEM can also prioritise response and, when combined with Security Orchestration Automation and Response (SOAR), can automate that response using playbooks aligned to threats specific to the sector. If we consider the insider threat, for instance, which is a large part of the threats faced in the sector, the SIEM can assess user account and system privileges and access and use this information to identify an attackers' presence in the network. With playbooks, analytics and case management in one central platform, problematic behaviour is quickly identified, and the appropriate response recommended. It's also easy to perform forensic analysis and investigation, enabling the university to present compliance evidence and determine the root cause of breaches.

THE INTELLECTUAL PROPERTY UNIVERSITIES GENERATE NEEDS TO BE SECURED AND PROTECTED

The final one of the five pillars is culture. This refers to the need to embed security awareness throughout the institution and among all those that use its digital services. The report recommends security awareness training and suggests that the NCSC's guide to maintaining a sustainable, strengthened cyber security posture can be used to avoid staff burnout among security professionals. It stresses the need for a top-down approach and that a no-blame culture needs to be developed to encourage reporting but at the same time there also need to be clear expectations set around behaviour, acceptable use and negligence when it comes to protecting data.

Together, these pillars can help bolster the resilience of the organisation, but importantly the report iterates the need to maintain momentum through continual improvements. It warns that universities should not underestimate the resources and effort required to maintain a strong security posture. So, to understand some of the challenges universities face as they attempt to apply defence-in-depth (DiD), threat detection and incident response (TDIR), and user awareness, it's worth looking at some real use cases.

Lancaster University, for example, faced real issues with legacy infrastructure, making it difficult to collect and analyse log data. Before it could even begin to address security issues, it had to deal with log management because data logs were mostly held as text files within various systems and siloed in departments and teams with differing retention periods. In order to carry out a security operation, the team would have to request the logs which were all in different formats and reformat them for analysis, a time consuming and lengthy process.

To address the issue, the Lancaster team began collating and centralising log data and applying uniform retention policies. But they also wanted to correlate log sources and enrich log data as well as giving system owners access to their own logs. The IT security team realised they could use the analytics and correlation capabilities of a SIEM to do both, increasing operational efficiency and providing them with the capability to carry out analysis and investigations more speedily.

However, as university networks handle such an enormous amount of traffic and have very noisy systems this made it very difficult for the team to find a workable solution. SIEM vendors typically price on traffic volume, which would have been cost prohibitive as the team needs to be able to work to a predictable budget. A change or reconfiguration of a firewall, for instance, could lead to a rise in data volumes and corresponding SIEM throughput costs. For this reason, it's vital that universities look at licensing models and opt for a per-node charge to keep costs down without restricting their network monitoring.

RISK FRAMEWORKS SHOULD BE USED TO ASSESS AND BENCHMARK AREAS FOR IMPROVEMENT

Since implementing the SIEM, the Lancaster IT security team has gained greater central visibility and can enrich logs with information on identity. This has enabled them to spot privilege misuse, observe trends, investigate and to take pre-emptive action, allowing issues to be addressed before they can escalate into a possible breach or attack.

At Bedfordshire University, the security team were experiencing high false positive alert rates, putting the staff under pressure and making it difficult to prioritise response. The issue was made more complex by the fact the university offers ethical hacking courses, so had to be able to determine if internal activity on the network was malicious or benign. It had been using an open source network monitoring solution, but this was no longer up to the task as the team were seeing more and more compromise attempts fragmented over logs, so the decision was made to invest in a SIEM platform.

The SIEM needed to be able to ingest log data from numerous systems and correlate these to look for indicators of compromise (IOCs) and patterns of threatening behaviour but, because of the size of the network, it was important that it's components could be split to reduce the potential load on the network. The aim was to get the SIEM to do the heavy lifting, prioritising high-risk alerts and thereby freeing up human resource to focus on investigation and remediation.

Initially the team wished to capture and analyse authentication attempts and so used the SIEM to assess the seriousness of issues such as failed authentications due to bad username/password combinations, concurrency, user access time limits or too many failed password attempts. But it's since been used to assess asset utilisation and to carry out more detailed profiling of the devices, applications and operating systems users bring on to the network, an increasing problem for universities due to the demand for remote access by staff, students and researchers.

Both the Lancaster and Bedfordshire cases reveal how universities are looking to improve their cyber security posture and TDIR, but also the challenges they face from limited budgets and expansive networks. In fact, the reality is that universities do not operate in isolation. They are all part of a much larger digital ecosystem which sees them interconnected and interdependent. This means the sector as a whole needs to tool-up and work in partnership to threat hunt so that it can achieve the ultimate objective named in the report: the ability to defend as one ●

Jack Porter advises organisations to help them overcome cyber security challenges using SIEM and SOAR technologies. For the past four years, he has worked for Logpoint, where he is responsible for working with customers across all sectors. He has a particular focus and expertise working with the public sector in the UK&I and Benelux regions.

There needs to be clear expectations set around behaviour, acceptable use and negligence when it comes to protecting data

Picture credit: Logpoint