Higher education top of the list for hackers

Marie Clutterbuck, Chief Marketing Officer at Tectrade, explores data management in higher education and how important it is for educational institutions to keep their research data secure


Marie Clutterbuck

Research data is, as defined by the University of Leeds, "any information that has been collected, observed, generated or created to validate original research findings… Although usually digital, research data also includes non-digital formats such as laboratory notebooks and diaries." Research data is arguably the most important kind of data stored by universities, with any losses having dire consequences. This can ring particularly true in the case of experimental data captured from lab equipment, where results are often reproducible but expensive. As such, data managers are under an immense amount of pressure from the university, funders and journal publishers to ensure that the data is safeguarded correctly. However, this is made exponentially more difficult by cybercriminals who are targeting research data at an ever-increasing rate.

According to a recent report from Jisc, higher education institutes saw a 35% growth in Distributed Denial of Service (DDoS) attacks from the first half of 2017 to the first half of 2018. Higher and further education (HE and FE) institutions are evidently aware of this fact and are increasing their focus towards cybersecurity. Around 62% of HE institutions and 33% of FE institutions now have cybersecurity budgets which is a marked improvement from the past, but still alarmingly low considering the level of threats with which they are faced. This historical lack of funding has put HE and FE institutions on the backfoot in comparison to other businesses. This lack of resources, combined with a historically poor level of cyber awareness in the education sector, is putting universities at risk in an increasingly digitalised and interconnected world.

Evidentially, education institutions seem to be both unrealistically optimistic about their breach prevention capabilities as well as largely unaware of the systems the institutions host, making them prime targets for hackers looking for easy access to valuable data. It is for this reason that a lot of universities are now engaging on a greater level with data and backup, with many universities now providing best practice guides for data storage and handling to PhD students.

However, while data best practices are incredibly important to instil, there are often times where such practices are not enough to prevent IT outages. Businesses in general are facing a greater number of cyberthreats from cybercriminals who are using more sophisticated – and dangerous – tools than ever before. And when it comes to universities, as highlighted by Jisc, many of these attacks are DDoS or ransomware – both forms of malware that are focused on taking systems offline.

> **Massive amounts of downtime is not just an operational nightmare, but it is an embarrassing event for a university to suffer.**

Data knowledge is key

Organisations of any kind, be they banks or universities, can only operate efficiently if their systems are online and available as and when they are required. No institution can operate without data, which is why every organisation needs the ability to recover essential data and get vital workloads back online when a breach or an outage does occur. Recovery is very much the best form of defence.

Before any consideration can be made to the strategy, IT administrators must be aware of all the data that is on its servers. A university could enforce rigorous auditing of its student data, but that would only tell part of the story. While research data is usually categorised as either confidential, highly confidential, or unclassified, there is far more data on the network than just those systems being used for research. IoT devices, access control systems or even something like air conditioning, are all connected to the internet and can be harnessed as an attack vector.

From a really molecular level, there are 13 types of data: big data; structured, unstructured and semi-structured data; time-stamped data; machine data; spatiotemporal data; open data; dark data; real time data; genomics data; operational data; high-dimensional data; unverified outdated data; and translytic Data. Definitions tend to get vague, but the main point here is that administrators need to know the data on the network, and what it is responsible for. That does not breach any confidentiality rules, but if an administrator can see a big chunk of data that has been listed as "classified" by a trusted account, it gives them a better idea of the data.

With this in mind, educational institutions should carry out a full system audit, and this can be achieved through disaster recover (DR) testing. A DR test puts the IT infrastructure in a worst-case scenario and provides administrators with the knowledge of how long it would take them to recover data, restore business critical applications and resume normal service. DR testing is often overlooked, but without it and the subsequent creation of a disaster recovery plan, organisations will likely see that the IT system does not perform adequately.

As a researcher, suffering an outage can be particularly painful. Not only are you losing time where you could be working, but there is a chance that you are irretrievably losing the data you have worked hard on getting. As mentioned, experimental data is capable of being replicated, but recreating the conditions and finding new subjects can be extremely time- and cost-consuming. Researchers are likely to go from being pained to being angered, should the network be hit by ransomware or DDoS because an unpatched and vulnerable PC is being used by someone in maintenance, or if a student receptionist plugs in a USB stick they found on the floor outside the library.

Massive amounts of downtime is not just an operational nightmare, but it is an embarrassing event for a university to suffer. Universities exist in an extremely competitive marketplace, and while undergraduates are often at the mercy of whoever will accept them, researchers often have more autonomy in their chosen place of work. In that scenario, researchers will turn their noses up a university that has suffered high-profile outages that have cost their peers. Ultimately, what this all means is that a university treasury which does not see the value in cybersecurity spend will see a greater cost in the long-term.

> **As a researcher, suffering an outage can be particularly painful.**

Be the best by preparing for the worst

To stop that worst-case scenario from being a reality, administrators should implement a solution that will get their systems back online quickly in the face of a disaster. The best way to do this is by adopting a zero day approach to architecture.

This type of setup allows organisations to prioritise workloads, stressing that they must be back online first in the event of any outage.

A zero day recovery architecture is a service that enables administrators to quickly bring work code or data into operation in the event of any outages, without having to worry about whether the workload is still compromised. An evolution of the 3-2-1 backup rule (three copies of your data stored on two different media and one backup kept offsite), zero day recovery enables an IT department to partner with the cyber team and create a set of policies which define the architecture for what they want to do with data backups being stored offsite, normally in the cloud. This policy assigns an appropriate storage cost and therefore recovery time to each workload according to its strategic value. Not all data is created equal, and research data at university should be prioritised ahead of, say, the POS system at the campus nightclub.

When an IT outage (malicious or otherwise) takes place, it is not the attack itself that causes the most harm but the resulting downtime of operations which will not only affect productivity and credibility of the organisation. The IT infrastructure of educational institutions therefore desperately needs to be modernised with adequate recovery systems that can allow fast access to mission critical workloads at all times without stretching their already tight budgets.

www.tectrade.com