MELIUS CYBER SECURITY

FUTUREPROOF

Cybersecuirty in the education sector

CYBERSECURITY SERVICES FOR THE EDUCATION & HIGHER EDUCATION SECTORS

What is Cybersecurity?

BACK TO BASIC PRINCIPLES

Cybersecurity is the defence of your networks, data and financial information from malicious attackers who seek to use the information gained for future financial gain.

Education is fast becoming a prime target for cyber attacks, with more than 200 institutions reporting over 1,000 attempts last year to steal data or disrupt services.

In August 2020 Northumbria University was subjected to a cyber attack which took six weeks to rectify, disrupting all activities and teaching throughout the campus.

THE LANDSCAPE

There are 11.7 million students in the UK education system from primary through to higher education. In addition there are over 500,000 school teachers (excluding support staff) and just over 500,000 staff employed in higher education.

This represents a huge attack surface for cyber criminals across a variety of skill sets with varying levels of IT skill and institutional security.

In addition the data, intellectual property and financial records held across the sector is incredibly valuable.

As students and staff bring multiple devices into schools/campuses the sheer range of connections to the infrastructure and beyond to other institutions; means that the security teams do not have the opportunity to ensure every device is secure.

In many cases the security can resemble a Swiss cheese due to the number of holes.

All of these factors create a huge and diverse pool for attackers to choose from, which increases their chances of success.

There are four key reasons why education is a target for cybercriminals:

1. **Data theft**
   Personal data, names addresses are a typical cyber theft for either immediate sale or extortion.

2. **Financial gain**
   Online portal payments and other gateways, for trips, fees and extra curricular activities are now very common and contain access to debit card and bank account details.

3. **Denial of service**
   Typically to extort money denial of service hacks can also come from the student community either as a prank or a protest.

4. **Espionage**
   Higher educational institutions are often engaged in research and development, this intellectual property can be very valuable.

THE METHODS

Cybercriminals have a vast array of tools and methodologies to attack networks and institutions. They typically employ a range of tactics to infiltrate a system and once inside move around to gain access to other sensitive areas.

A recent study of IT professionals within higher education highlighted the most common ways education networks are breached:

1. Phishing
Phishing scams often take the form of an e-mail or instant message designed to trick the user into trusting the source in a fraudulent attempt to access their credentials.

2. Ransomware/Malware
These attacks prevent users from accessing the network or files and cause disruption, more advanced forms of this threat can see attackers hold files/data for ransom.

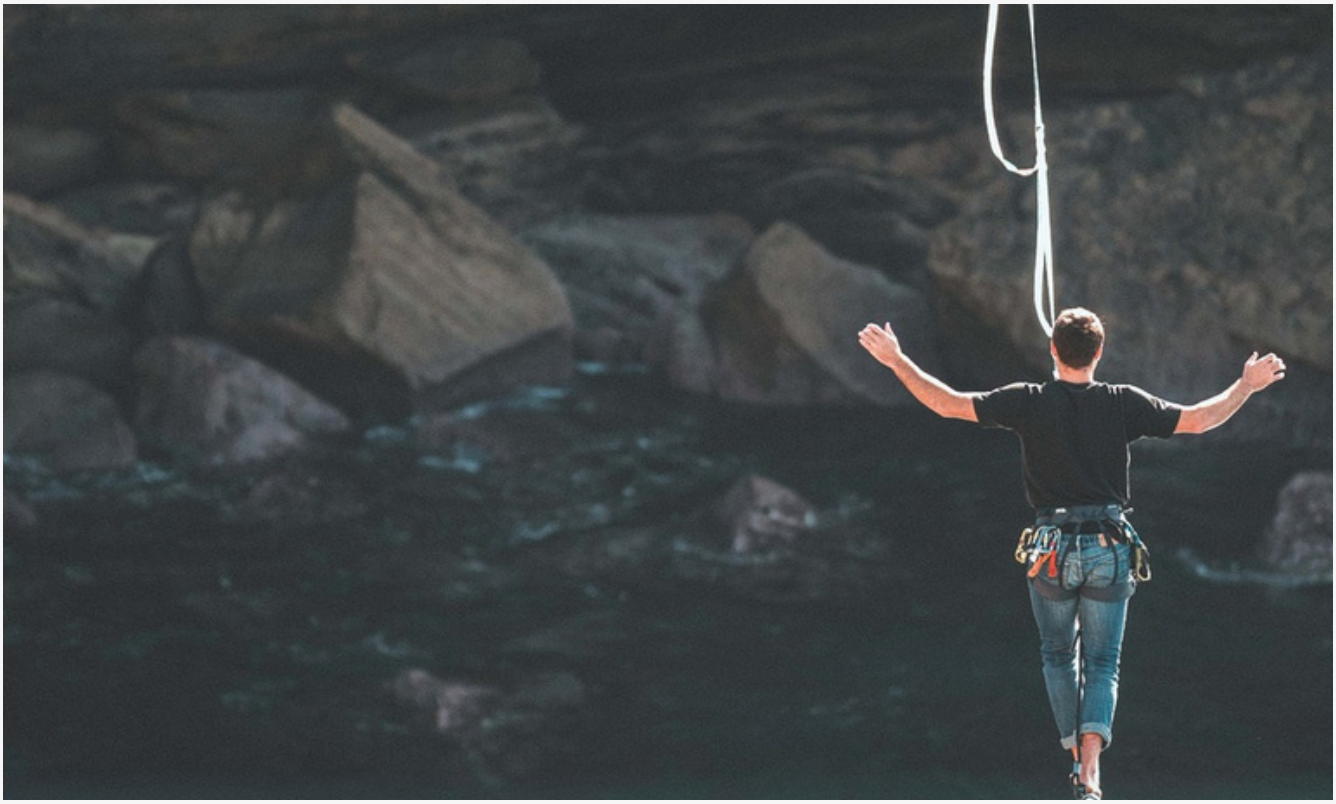
3. Network exploitation
With some many devices connected to a network and the increase in remote learning and home study the maintenance of network integrity is paramount, cybercriminals typically exploit open ports or connected devices to gain access.

4. Brute force
A brute force attack uses limited public information and then attempts multiple logins using automated password/login combinations. Attackers typically find names and e-mails though social media and then use this information to build a brute force assault.

5. Patching policy
Patch management is key tool in cyber defence regular bug fixes are released by Microsoft and other software providers, where devices are not rebooted and patches implemented vulnerabilities can exist and provide an entry point for an attacker.

6. Technological deficit
Budgegary constraints can mean that hardware may be out of date and/or unsupported, this can lead to vulnerabilities and further issues as providers cease to provide patches for end of life devices.

THE RIGHT BALANCE?



Education is unique; due to the demands of modern learning (exacerbated by Covid) institutions are expected to provide online learning to all of their stakeholders across multiple mediums to an array of personal devices that may already carry viruses or spyware. At the same time the sector is expected to keep everyone safe and cybersecure whilst balancing budgets and time constraints.

Our aim is to put the security of pupils and stakeholders at the centre of everything you do without compromising on accessibility and doing some at a pricing point that fits your budget.

Our management team are experienced in working in public sector environments, across a wide range of government institutions including; Ministry of Justice, Ministry of Defence and various Police forces. In addition we have provided consultancy services to various schools and academies around the IT estate and security over recent years.

We pride ourselves on providing solutions that are best in class for cost backed up by a dedicated service desk that can assist on all levels of tech and security.

KEY QUESTION

HOW TO STRIKE THE CORRECT BALANCE BETWEEN WHAT YOU ARE SPENDING ON CYBERSECURITY AND THE TANGIBLE BENEFITS

At Melius we recognise the threat to all sectors / businesses and the need for a cost effective solution. Therefore, we developed a cybersecurity product at a pricing point where it makes no sense to say no. Our bespoke MELCaaS product puts you in control for less than £10.00 per day. MELCaaS is a holistic solution that brings all the elements of cybersecurity into one product capable of delivering value and balance.

MELCaaS delivers:

- Daily scanning for over 100,000 vulnerabilities (growing daily)
- Password testing
- Remote policy setting
- Cloud app evaluation
- E-mail phishing
- Antivirus monitoring and configuration
- Patch monitoring and configuration
- Daily reporting

MELCaaS account holders have access to an easy to read dashboard where vulnerabilities and cyber speak are reported and then broken down into plain “What does that mean for me” English. We provide support and back up through our dedicated tech team. We ensure that you are protected and the balance is correct.

www.melius-group.co.uk