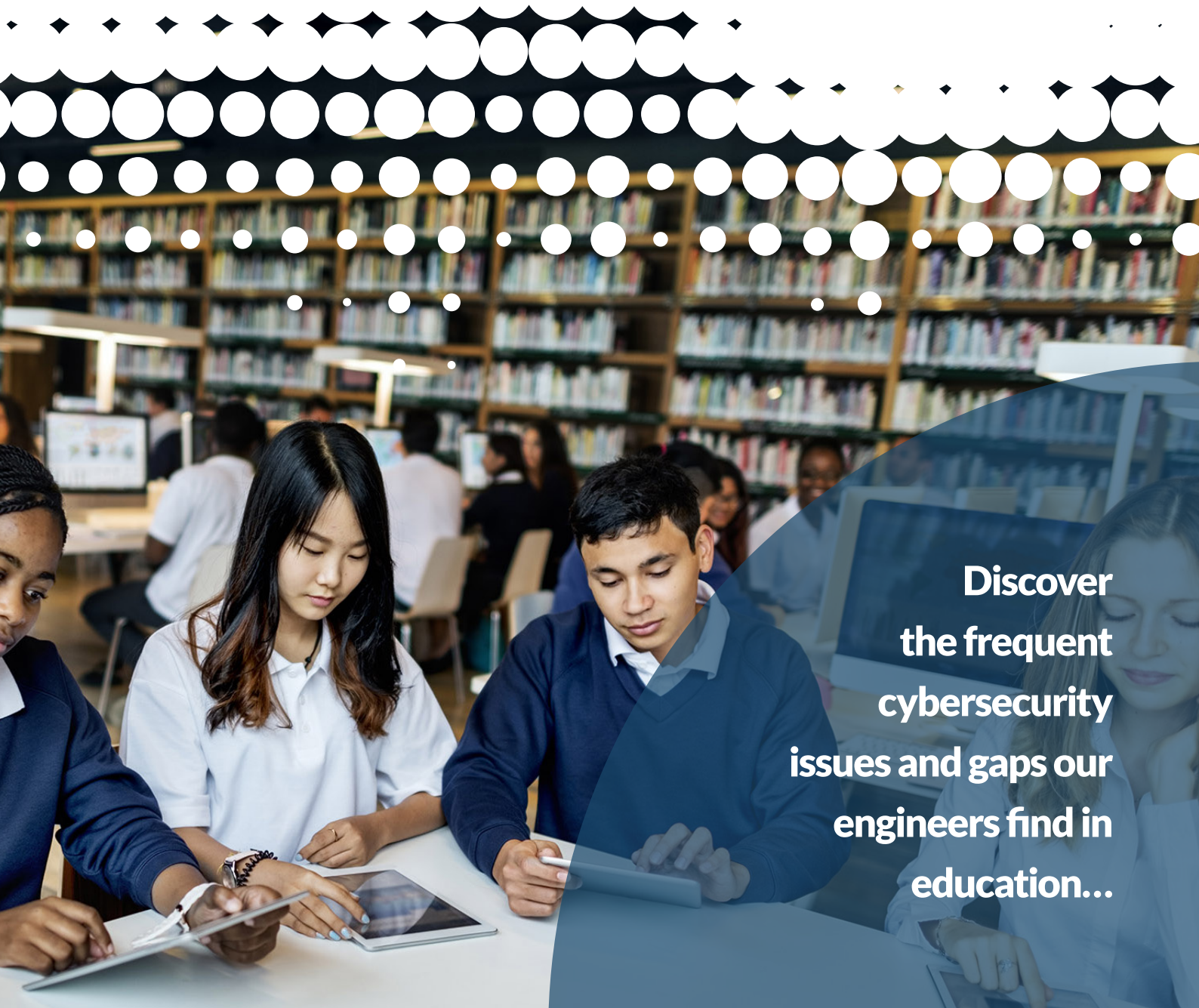
WHITEPAPER

The Top 5 Cybersecurity mistakes made in Education

With the complex security issues raised by the increase in mobile and portable device usage, and students, visitors and academic staff bringing their own devices on to campus, we're starting to see the same set of common mistakes occurring over and over again.

Foursys has more than 150 clients in the education sector protecting close to 500,000 users. Foursys provides advice, solutions and services to Schools, Colleges, Universities, Institutes and Research Councils.



Discover the frequent cybersecurity issues and gaps our engineers find in education…

In the course of our work with clients in the Education sector, our Security Engineers frequently come across security issues and gaps in the cybersecurity defences of education institutions that in this day and age are easily addressable and should be covered.

In this white paper we look at the top 5 common cybersecurity 'mistakes':

- Weak Web Filtering
- Poor Network Visibility & Control
- Not patching non-Microsoft Applications
- Lack of Encryption
- No End User Education

We also suggest some of the steps you could take in order to ensure these potentially serious security flaws can be avoided.

As a major supplier of network security solutions to the Education sector, Foursys is aware of the issues, pressures and needs of students to operate in a network environment that supports free and open access to the internet, but that is also safe, secure and risk-free.

Students need to research and learn, staff need access to teaching resources and the process used to deliver a seamless learning environment needs to be effective.

However our experiences are that these needs are too often being prioritised at the expense of what may be perceived as complex measures needed to ensure a safe and secure network environment.

This has potentially serious implications.

Taking the above into account we have provided some pointers on what we believe to be the most significant mistakes being made in education cybersecurity today.

These topics make a good starting point for security staff, and it is our hope that the information provided will guide them on the steps that should be taken.

Mistake #1: Weak Web Filtering

The challenge with web filtering is that it needs to allow genuine users to browse and share information in an open environment and to share information in safety, on whatever device they are using. At the same time a web filtering solution must scan all content – including HTTPS traffic - for malicious activity.

Foursys Recommendation

We recommend putting some form of gateway web filtering in place. To be clear, this is not to restrict students' internet browsing, but rather to protect against web borne threats.

About 85% of cybersecurity threats come from the web channel, which means that web gateway filtering should be a "standard" security measure that should be in place. It is also the best way to ensure and report to officials of your duty of care in safeguarding the students.

Modern day web-borne attacks are highly sophisticated, so strong protection is needed to fend off threats. Compromised computers are a very lucrative money maker on the black market and criminals are profiting every day.

Why weak web filtering is a risk

Approximately 30,000 new malicious URLs are discovered every day, and a majority of these will be compromised legitimate websites that play host to various forms of malware including Trojans, Spyware, Adware and Worms. The list goes on.

In order to compromise a computer an attack will usually be carried out in 5 stages:

- Entry via a user visiting an infected website and being hijacked
- Redirection of the user's browser to a malicious site
- Exploit by probing the user's device for vulnerabilities
- Payload is downloaded
- Execution when the infected device calls home

Solution

Web threats can be avoided by deploying a strong web filtering solution that has the ability to scan websites for malware and dynamically block sites that are infected.

Filtering HTTPS traffic is important, because basic URL filtering no longer matches the landscape of today's internet, with over 50% of sites using HTTPS as standard and even the most reputable website can be infected without the user knowing.

It is also important to be aware of third party applications and associated vulnerabilities. Having a web filtering solution that can help manage the use of such applications will help avoid exploitation.

Mistake #2: Poor Network Visibility & Access Control

Students and academic staff may have as many as 5 devices connecting to the network at any one time. Ensuring these devices are visible, monitoring their activity and controlling who can connect to what when they access the network is vitally important for the security of all network users and systems.

Foursys Recommendation

Foursys recommends having visibility and control of everything and anything that can connect to the network, the Internet of Things is here and it is vulnerable.

Network administrators within education need to ensure that they have visibility of everything connected to the network.

When guests log on to the Wi-Fi network, it is important to ensure that their devices are clean from infection and that all endpoints are compliant.

Why poor network visibility & access control is a risk

Without network visibility and control over the network there is a risk that unauthorised users may get on to the network.

The best network access control (NAC) systems however can scan devices to ensure their security profile is appropriate, and that they do not present a risk of introducing malware into the network.

Without the authentication and authorization functions to verify user logon information, there is no way to prevent selected end user devices that do not meet security criteria gaining network access or to restrict access to specific data sources

Solution

By deploying a NAC solution that can monitor your network traffic and integrate seamlessly with your infrastructure, you can gain visibility of devices the moment they connect.

The right solution allows you to monitor and decide who and what can connect, if they can connect where they can go and if their device does not meet security requirements, to send notifications to update their security or automate the remediation process.

Importantly, if the device is new to the network you can ensure that it is secure and free from infection.

NAC should not be just a case of Yes or No, we recommend that you can Alert & Remediate, Limit Access and Move & Disable.

Mistake #3: Not patching non Microsoft applications

The common mistake with patching, and one which we see all too regularly within education network environments, is that security patches are not always applied, especially to non-Microsoft applications. This presents cybercriminals with huge security holes and offers them an open invitation to attack your network and users.

Foursys Recommendation

Foursys recommends that IT departments within education investigate a patch management solution that will scan the network for vulnerable devices and provide fixes for machines that are either out of date or are open to zero day attacks.

All IT admins are probably familiar with the critical Microsoft security patches that are circulated every Tuesday. 'Patch Tuesday' has become part of the IT department's working week and an essential part of staying secure.

Many teams use WSUS or SCCM to aid with this – which is highly recommended.

But what about the non-Microsoft applications deployed across your network? Using a catalogue to check for vulnerabilities can take a lot of time, and does not provide information on the status or criticality level of the application. Nor will it detect end of life applications.

Solution

Some network users within education may run devices that rarely call home to receive updates. Ensuring that these devices are up to date and patched can therefore be tricky.

Letting an unpatched device – one that is not up to date with patches to its system and applications – onto the network offers an open door to anyone who wants to gain entry to exploit, profiteer or steal data/documents from the network.

Without adequate protection in place against exploits, the whole network can be vulnerable to increasingly common malware variants such as ransomware.

Vulnerability scanning and patch management should therefore not be restricted to only Microsoft applications. Patches should be applied with equal regularity and consistency to non-Microsoft software to remediate security flaws regularly.

Mistake #4: Lack of encryption

Educational organisations may underestimate the amount of sensitive data they have on their network. Information within research and exam papers, student academic records and other personal identifiable information (PII). These are at risk unless the locations where they are stored are encrypted. New EU Data Protection Law is expected to come into force imminently on this.

Foursys Recommendation

With the expected changes to EU Data Protection Law, we are recommending that the ideal solution is to adopt encryption as part of an overall data protection strategy.

In the past, encryption solutions have been difficult to install, and involved very complex data management and recovery options which took many hours to complete.

Times have changed. Encryption is easier and faster to roll out, management options are richer, data recovery is more straightforward, and enduser challenge/response is typically automated.

Encryption should be a part of every security portfolio, particularly with the growth in popularity of portable devices and cloud file storage.

Solution

Best practice in encryption involves securing data on all devices including laptops and desktops, removable devices such as network drives and USB devices and files stored in the cloud. It should also include both PCs and Macs.

Encryption solutions require little or no on-going management overhead to worry about, which is particularly important if there are hundreds or potentially thousands of end points involved.

Installation tends to be very simple, requiring the roll out of small MSI files to each hard drive, for rapid encryption.

Once the process is complete, encrypted machines report back to a central administration console where the encryption keys can be managed along with any troubleshooting or auditing that may be required.

Last but not least, with those new EU Data Laws approaching, organisations within education are advised to get their house in order and to ensure their security policies are in compliance.

Mistake #5: Not educating end users

Educating end users on safe internet use can be difficult - but changing behavior is even more difficult. People just can't resist watching a dancing pig or clicking on an attachment to see whether it really is an overdue invoice.

Foursys Recommendation

An engaging and up-to-date end user awareness program should be used alongside your organisation's technical security solutions so that the whole academic staff and student population are aware of cybersecurity risks and the simple steps they can take to stay secure.

Security technologies provide extensive data and user protection and are key to compliance. However setting data security policy and educating network users in how they should use the internet and internal resources can make a vast difference to the overall security stance of your organisation.

Solution

End user training courses, guidance and 'self education' support should be put in place with the specific aims of changing user behavior.

Network users need to be aware not just of the nature and implications of threats and how they can become victims, but also of their responsibilities and how they must comply with network policy.

By increasing awareness, adapting user behavior and, changing attitudes to the risks and dangers posed by cyberthreats, organisations within education can improve their overall security.

Computer-based training packages, workshops, seminars and training days are all available to assist.

Working with Foursys

As a major supplier of cybersecurity solutions to the education sector, we find that many organisations do not filter web traffic and remain unclear on how to tackle sensitive data.

Patching is perceived to be a pain and having visibility of what is connected to the network is a 'Golden Question'.

Because we understand the education environment, we know that it is important for students and staff to share information freely, to gain unfettered access to internet in the course of their research and studies.

Yet we also believe it is far too easy to be reactive when dealing with IT security. As a result, network security resources can be stretched.

What is needed is a much more managed and proactive approach to network security. To assist its education clients, Foursys has a dedicated team focused on servicing the Education sector.

The Foursys Education Team works with schools and colleges, sixth form colleges, academies, independent schools, school trusts, universities, research departments, research councils and institutions.

Our industry leading engineers are able to offer enhanced support, health checks, on-site and remote services plus training to help our customers deploy the best network security solutions to meet their needs.

20 Years of IT Security Excellence

For more than two decades, Foursys has operated as a UK-based network security VAR, providing IT security products, services, solutions and support to NHS, government, education, SMB and enterprise organisations. With more than 1,000 customers protecting over 2,500,000 users.

www.foursys.co.uk

Want to find out more?

This guide is designed to give general guidance, however each network is unique and we recommend a consultation with a Foursys security specialist if you have any concerns.

Contact us

Main Switchboard
+44 (0)1284 788900

Technical Support
+44 (0)1284 788901

Email
enquiries@foursys.co.uk

Head Office
Manor Park, Great Barton
Bury St Edmunds, Suffolk
IP31 2QR, United Kingdom

www.foursys.co.uk