novatia

Helping to harness ICT excellence for education in a constantly evolving digital world

Novatia Note 012: Cyber Security in Schools and Trusts

Key Points

11 measures to ensure cyber security:

1. **Restrict individual access**
2. **Stop malware jumping from host to host**
3. **Up-to-date antivirus software**
4. **Develop School policies for data transfer**
5. **Test your backups**
6. **Get experts to test the integrity of your network**
7. **Ensure everyone knows about cyber security**
8. **Check firewall logs and action them**
9. **Password strategies**
10. **Ensure authentication tools are in place for remote access**
11. **Latest software releases**

As a School Leader there are a number of precautions you can put in place now to limit the chance of your School or Trust being targeted by cyber threats and 'ransomware' attacks. These should be considered in any strategic review of your procedures and systems.

The first and most important step is to ensure you carry out regular backups of your system. Trusts and Schools should also review their backup policies and procedures. Schools should not only include backup to disk as part of their routines but make sure backup schedules are sufficient and are incremental, e.g. daily, weekly, monthly or termly. Off-site backup provided through cloud services should be explored and then implemented. In addition, off-site storage of backup media should be in a secure fire proof location to mitigate risk of site loss.

Other preventative measures:

1. **Restrict what any individual can access across the School's network.**

Restricting access reduces the effect of any encryption process as a result of ransomware. Does the IT department really need access across all data when they log in or do they just need to see what they're working on? Does the maths department need to be able to immediately access data in the languages department? Also ask yourself, can students infect each other's work?

Not everyone needs access to all data when they are logged in.

2. **Configure the network so that malware can't jump from host to host**

This prevents the infected software from finding another machine that is vulnerable to exploit. By using different virtual local area networks you can minimise how a virus

may spread around the network. A single 'flat' network allows all client machines to access all servers and data, making it easier for viruses to spread to other devices.

3. Use up-to-date antivirus software

Good security mechanisms should alert you to anything that is happening and minimise impact on the network. Viruses and malware morph really quickly. Often viruses may only have a small window of opportunity before they are fully detected. It does not take much for the virus creator to update and release a newer version quickly. Keeping your anti-virus software up-to-date and looking at regular updates to critical systems more often than daily will help reduce the risk of losing data or access to the network.

4. Develop School policies for the transfer of data

Good security mechanisms should alert you to anything that is happening and minimise impact on the network. Viruses and malware morph really quickly. Often viruses may only have a small window of opportunity before they are fully detected. It does not take much for the virus creator to update and release a newer version quickly. Keeping your anti-virus software up-to-date and looking at regular updates to critical systems more often than daily will help reduce the risk of losing data or access to the network.

5. Test your backups

Lots of schools do backups blindly never testing whether the backups or tapes actually hold the data or that you can actually retrieve the information. You need to do some disaster recovery testing, say to yourself, "Let's imagine we just lost everything…can we reinstate everything? How much do we get back?" It's better to test it in advance rather than find out, when you need to, that it doesn't work.

6. Get experts to test the integrity of your network

Get an external company to come in with specialist cyber security skills to test your networks. Essentially you're requesting them to do an internal network test and an external penetration test; asking them to *legally* hack into your systems.

7. Ensure everyone knows about cyber security

Ask yourself, are all our people trained and aware? You can have a great policy that says "*if you don't know what this email is… "*, 99 people out of a 100 might follow it but one might not, and that is all it takes to break into a network.

Most organisations are good at protecting their outside networks with firewalls. Cyber-criminals now focus on getting staff to open up "dirty" emails and bring in infected data to the organisation for them. Make sure people are vigilant, if they do not deal with finance, then there should be no reason why they open up emails with invoices attached. Similarly, if they are not in HR, there is no reason to open up emails with CVs attached. These are common ploys to get people to open compromised files.

8. Check firewall logs and action them

Check your firewall logs regularly. Understand what is being blocked, and where from. Knowing how the network runs 'normally' helps to understand what to look for when things go wrong.

9. Develop password strategies

You do not have to have long, complex passwords which are difficult to replicate. Good pass-phrases help to create long passwords. Longer passwords are more difficult to crack than just complex ones. Try to avoid using common passwords as attackers will use dictionary and rainbow -table tactics to break passwords. Make sure your users understand that just changing the last digit each time isn't creating a secure password. Always change default passwords, and if possible accounts, for network equipment and applications.

The more hoops that hackers have to jump through, the less likely they are to spend too long on a network.

10. Ensure authentication tools are in place for any remote access

Do not just rely on user-names and passwords for remote access. Whilst account locking is useful for brute-force attacks, if hacker has a valid username/password combo then the system will let them login.

For remote access think about using a second authentication tool, like a 1-time token which can only be used by the person holding the key. There lots of systems available, some free, which can be used to help secure remote access. Because the token creates a unique key, it makes it very hard to hack.

11. Make sure all systems are updated with latest software releases

It's very important to have a regime and process for regular patching and updates of your servers, desktops/laptops, firewalls, switches and anything else on the network. Suppliers will release software and firmware updates which 'patch' vulnerabilities which can reduce or even stop some attacks from happening. If you have older operating systems or network devices which are no longer supported by the manufacturer you should consider replacing and updating them.

So how much will this cost you?

Remember, it is a lot cheaper to protect your network today, rather than try and recover all your data if you lost everything tomorrow.

Additionally, if you lose any personal data after the new EU General Data Protection Regulations (GDPR) come into force on 25 May 2018, you could be looking at a heavy fine from the Information Commissioner's Office (ICO) for not taking the right steps to safeguard your records.

For further information about our ICT Security Audits, see our website www.novatia.com or contact us on 01962 832632 or info@novatia.com.