National Cyber Security Centre Alert

Further targeted ransomware attacks on the UK education sector by cyber criminals.

By now many of you will have already seen, the **National Cyber Security Centre's (NCSC)** alert regarding Further targeted ransomware attacks on the UK education sector by cyber criminals. The Education Sector has become a growing target for cyber criminals, with the NCSC previously acknowledging an "***increase in ransomware attacks on the UK education sector during August and September 2020***", and since late February 2021 this has increased further prompting the NCSC to alert the sector of the growing threat.

You can download a PDF version of the NCSC's Alert here, which is designed to be read by those responsible for IT and Data Protection, but "***It is also important that senior leaders understand the nature of the threat and the potential for ransomware to cause considerable damage to their institutions in terms of lost data and access to critical services***", so here's a quick summary of what you need to know:

The alert focuses mainly on the rise of **Ransomware** Attacks which as the alert states is "**a type of malware that prevents you from accessing your systems or the data held on them. Typically, the data is encrypted, but it may also be deleted or stolen, or the computer itself may be made inaccessible**".

> ***"In recent incidents affecting the education sector, ransomware has led to the loss of student coursework, school financial records, as well as data relating to COVID-19 testing."***

The document then goes on to talk about various **infection vectors (i.e. ways of getting access)** that malicious attackers are using to gain access to or exploit vulnerable systems and the dangers **of Lateral movement and privilege escalation** (having acquired initial access to a network, navigating around it, and increasing their privileges or identifying high-value systems).

The final page briefly goes on to talk about **Mitigation** and summarises some techniques for both prevention and recovery, but mainly provides links to further documentation and advice, much of which is again lengthy and targeted at those responsible for IT and Data Protection.

Below is a summary of our recommendations for ways to prevent as well as recover from a Ransomware attack, and how Computeam can help with each step!

Computeam Ltd
Suite 443 Broadstone Mill
Stockport, SK5 7DL

0800 826 0123
info@computeam.co.uk

Preventing Ransomware

The best form of protection is prevention. It is better to try and stop an attacker than to have to fix or clear up their mess! Below are some examples or preventative measures to help protect against Ransomware and generally improve your Cyber Security.

- **Patching and Software Updates**
  A key part in protecting your network, is to ensure that devices have the latest operating systems, update patches or Firmware installed. When a vendor becomes aware of a security flaw which could be exploited by an attacker, they will usually release a software update to protect its users. If you do not install these updates, it is like leaving the door open for the attacker. **Computeam offer Remote Management and Monitoring services, which can not only ensure your devices are kept up to date, but can also provide regular reporting and update activities to give you added peace of mind.**

- **Effective and up-to-date Anti-Virus/Endpoint Protection**
  Antivirus and Endpoint protection systems are installed on user devices (e.g. laptops, desktops) to ensure that if an attacker does get through, or if a user accidentally brings malware into the network, these systems will attempt to prevent it from running on the device and achieving is malicious goal. Not all Antivirus/Endpoint Protection solutions are equal, and they are only effective if they are kept up to date and effectively managed. **Computeam can offer advice on which to use and why, as well as supply and or manage solutions for you to ensure they are effective.**

- **Gateway and Perimeter Protection**
  Ideally, an attacker would not get as far as a user device or network server. To try and prevent access to the network, a secure firewall should be used at the network perimeter to manage the flow of traffic in an out of your network. Modern firewalls can include many extra security features such as Gateway Antivirus with Advanced Threat Protection (ATP) and Intrusion Detection/Prevention Systems (IDS/IPS). **Computeam offer fully managed Firewall Solutions with a host of Security features and options to suit any network.**

- **Secure Configuration**
  Incorrect or badly configured devices and software is great news for a malicious attacker. There are thousands of tools, which attackers can use to exploit badly configured devices, even search engines, to help them find your network as a target. These weaknesses also greatly increase the risk or lateral movement and privilege escalation once an attacker has made it inside your network. **Speak to Computeam about our consultancy and audit services which can help to identify mis-configured devices and unsecure networks, as well as help you to plan for greater security in the future.**

Computeam Ltd
Suite 443 Broadstone Mill
Stockport, SK5 7DL

0800 826 0123
info@computeam.co.uk

- **Securing Access - Using MFA**

  Secure access is essential to protect your network. Did you know that many user credentials, are already available for attackers to download and access on the dark web!? Head to the site haveibeenpwned.com to see if your email or password has been involved in data breach at some time. Even if you have password complexity rules in place to ensure stronger passwords which are harder to crack, many people re-use passwords that they think are secure. Attackers use a technique known as "credential stuffing" to try passwords that have been discovered elsewhere on systems they are attacking. Just because your credentials don't appear on the above site, it doesn't mean they haven't been leaked! To protect against this, Multi-Factor authentication requires another form of authentication in addition to your password, such as a passcode sent to a mobile phone by text, or a number generated by an app or fob. In addition, where MFA is not available or appropriate, Conditional Access can be deployed to provide an additional layer of security, allowing authentication only from specific devices or locations - for example from inside your school network. **Computeam can advise and assist with implementing both MFA and Conditional Access Solutions for your network.**

- **Training and User Awareness**

  The weakest link in even the most secure of networks is often its users. While you can put in place tools and measures to protect from external attack, networks are often much less secure from an internal one! Phishing emails are a common source of attack and often provide an attacker with an initial foothold into a network. The best way to ensure that your users don't unintentionally compromise your network and data is to make them aware of the risks and teach them how to spot them and respond to them appropriately. **Computeam can offer Training services as well as a platform to manage Cyber Security Training, GDPR and Policy Compliance, ensuring that staff are kept up to date with any changes, and keeping track of who has or has not completed any mandatory training.**

Recovering from Ransomware

It is all very well knowing how to protect your network, but sometimes the inevitable happens, and what you need is a solution. Below are some measures that will help you to be ready to recover from a Ransomware or other Cyber Security Threat should the worst happen.

- **Backups**

  A backup will likely be your primary tool to recover from an attack, however these are not impervious to an attack themselves. Many organisations have found themselves in a situation where they have realised that not all their information was being backed up. Others have inadvertently overwritten their backups with encrypted data after a Malware attack has taken place. For this reason, it is vitally important, not only that you have a backup solution in place, but also that it is appropriately specified and configured to protect all your data and systems, as well as to retain sufficient copies of your data to avoid overwriting your backups. **Computeam can offer advise as well as supply and manage backup solutions, to meet the needs of any school.**

- **Disaster Recovery Planning**
  Having a backup is great and may well be the critical factor in an effective recovery but knowing what to do and how to recover is also vitally important. This is not only about how to restore your data, but also to stop further spread of any Malware and ensure it is removed, before data is recovered, to avoid reinfection. **Our team of Consultants and Account managers can help you to define and document a Disaster Recovery Plan, which will detail what to do and in what order to ensure the situation is effectively handled.**

- **Business Continuity Planning**
  In addition to Disaster Recovery, an often-overlooked consideration is Business Continuity. Could you afford for your institution to be closed or offline for a week or more while your Disaster Recovery Plan is being implemented? As above **our team of Consultants and Account managers can help you to define and document a Business Continuity Plan, identifying which systems and processes are critical to the running and operation of your organisation, and how they can be protected and prioritised to keep things running should the worst happen.**

- **Testing**
  The final essential measure is testing. Having all the above in place is useless if it does not work! Many organisations do not identify flaws in plans or overlooked systems until they try to implement their DR and BC plans. **Computeam can review these systems and plans and assist with testing them and mitigating any effect on users.**

If you have questions about what you've read or just want to discuss your organisations Cyber Security further, please get in Touch with your account Manager, or reach out to us at info@computeam.co.uk or give us a call on 0800 862 0123