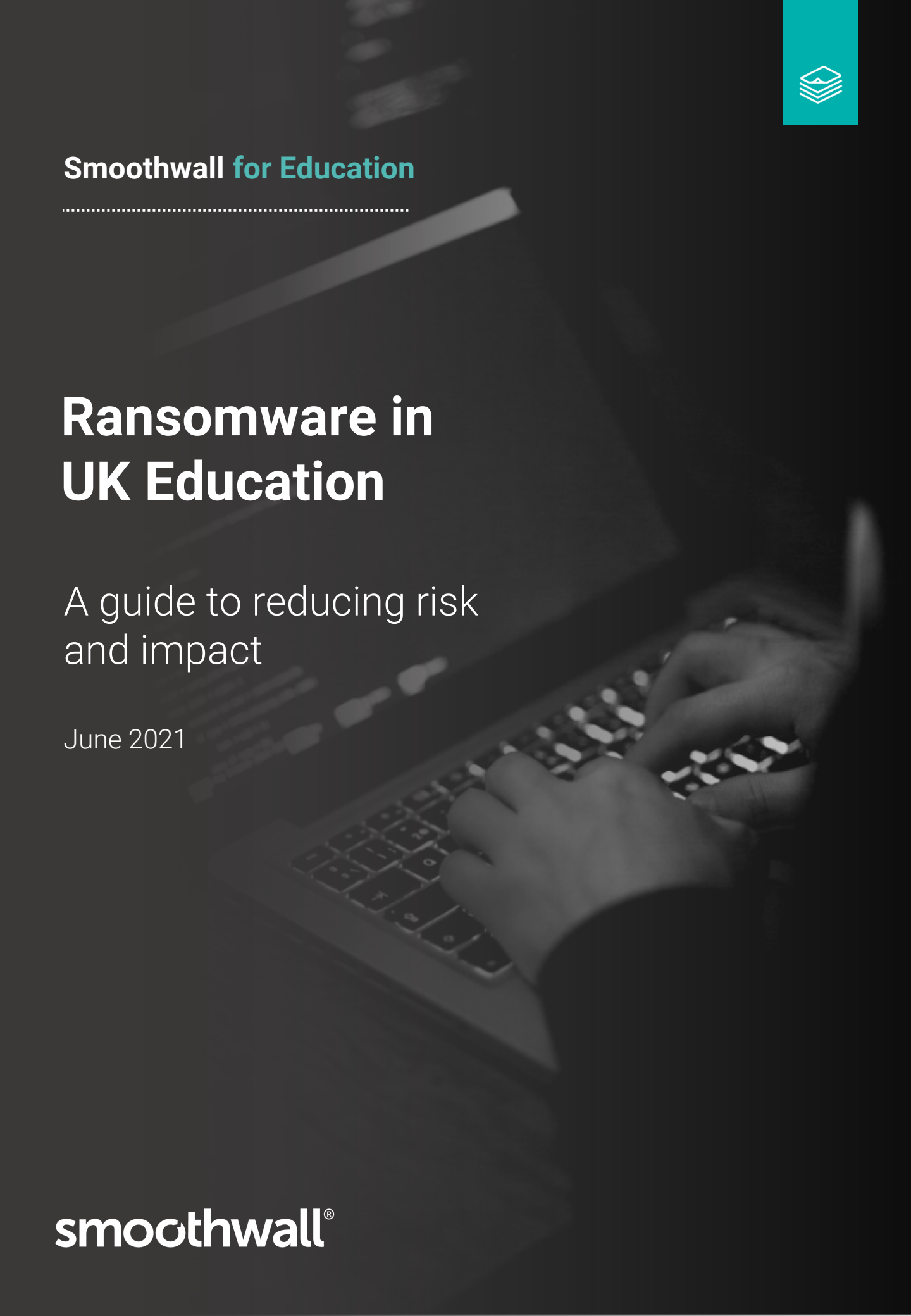

Smoothwall for Education

Ransomware in UK Education

A guide to reducing risk and impact

June 2021

smoothwall®

Introduction

There is no better defence against ransomware than prevention.

There is no better defence against ransomware than prevention. But in case your defences are breached, it's just as useful to stop the spread and be ready to recover.

In this paper we discuss ways schools can better defend themselves against attacks and what to do if the worst happens.

It's a practical guide written from the operational and financial perspective of schools, colleges and MATs.

Authors

Tom Newton
Head of Product, Smoothwall

Rob Faulkner
Technical Authority, Smoothwall

Tim Hobson
Network Manager
Sherburn High School

Essential reading for:
Anyone responsible for IT and data protection at education establishments within the UK.

What's the Problem

In the beginning there were viruses – now there is ransomware.

In the beginning there were viruses. Viruses often used your computer for sending spam, or mining bitcoin, but rarely did too much harm to your data.

Most recently, one of the most potent online threats, is ransomware. It robs individuals, businesses, and entire towns of billions of dollars every year. And now it seems it's the turn of education.

There has been a significant growth in attacks. As recent as June 2021, the UK National Cyber Security Centre (NCSC) is investigating yet another increase in ransomware attacks against schools, colleges and universities in the UK.

These days, personal data is more valuable than gold.

Ransomware tries to monetizes your data by locking you out of your network, encrypting, or stealing your data, then sending a ransom note demanding payment to recover it.

They will typically use an anonymous email address (for example ProtonMail) to make contact and will request payment in the form of a crypto currency.

Why schools and why now?

It is unlikely that schools are being targeted specifically, since they are less likely to pay than larger corporates, and rarely have ransomware insurance.

The spate of attacks is more likely a result of increased breadth of automated attacks looking for systems to encrypt.

In a recent webinar, the NCSC noted a shift in the way ransomware enters organisations.

Pre-pandemic, the most common ingress point was email. Though email is still an important vector, as more organisations rapidly opened up remote access systems during lockdown, open remote desktop (RDP) services have become an easier access point.

Of course schools were among the hardest hit by the need for 'remote work' with many opening up a range of new services.

What can you do?

Schools need a solid, practical and affordable response.

What's the current advice?

The current advice around ransomware involves financial investment:

'Upgrade your firewall.'
'Buy a SIEM.'
'Spend on backups concentrating on the 'offline' rule and the '3-2-1' rule.

All pretty good advice provided you have a limitless pot of cash and a team of people to spend it.

Unfortunately this is not the reality for most schools, colleges and MATs. They have neither the budget nor the headcount to adopt a blue sky approach. And, with no money on the horizon from the public purse either, they need to figure out a viable response and quickly.

'The 3 Avoids'

Having worked with UK schools for two decades, we understand how to help them achieve best practice with limited resources. Below is our suggestions for solid, practical and affordable response. We're calling them 'The 3 Avoids'.

1. **Avoid** getting ransomware
2. **Avoid** ransomware spreading
3. **Avoid** ransomware hurting

What can you do?

Prevention isn't important — it's imperative.

1. Avoid getting ransomware

- As we mentioned before, email is still an important vector and so **effective cloud based anti-spam is essential**. Email attacks usually rely on some user interaction – opening attachments or suspicious links. User training can be very effective here.
- **Patching:** it's not always possible to patch everything, all of the time, but in education it can be a high value strategy. Let's remember we're not patching banking or health systems here which are extremely downtime sensitive. Get all servers and clients patched as often as you can, and automate it if possible.
- Additional **anti-phishing products** can be effective to double down on email protection. But our advice would be to consider these after other interventions, as they can be expensive.
- **Block certain file type attachments** in your email system.
- **Segment your network** – keep servers away from clients if at all possible.
- **Close ports, firewall ports, choose non-standard ports, and use VPNs - for remote access**. VPN plus authentication is the gold standard.
- Try to **avoid services such as RDP** without protection, as these can be common targets. A non-standard port can only give you some limited protection against automated attacks
- **Consider geo-blocking** in email and firewall rules. But bear in mind that while geo-blocking can quickly squelch a lot of automated attacks it's not always accurate and can lead to over blocking.
- **User training and awareness** – problems are exacerbated by user ignorance on the subject. The NCSC has some good resources. Check them out. Stay informed.
- **Limit the capability for software install on managed devices**: Download software only from reliable websites and app stores.

.

What can you do?

Prevention isn't important — it's imperative.

1. **Avoid getting ransomware** - continued

- **Encourage the use of 2Factor Authentication** and use password managers to prevent re-use of passwords.
- **Sign up to the** NCSC's early warning service. It is free and designed to inform your organisation of potential cyber attacks on your network, as soon as possible.
- **Consider risk assessment tools like PingCastle** (https://www.pingcastle.com/) It queries Active Directory and gives a report on areas that need attention or could be improved.
- Similiarly, tools like NCSC Exercise in a Box https://www.ncsc.gov.uk/information/exercise-in-a-box can help you **find out how resilient you are to cyber attacks** and help you practise your response in a safe environment.
- **Use breached password testers** such as 'Have I Been Pwned'. It's a free resource and allows you to quickly assess if your data has been put at risk due to a compromised account or "pwned" from a data breach.
- If you must have open services **consider using tools like** 'Fail2Ban' **or** RDPGuard to monitor the logs on your server and detect patterns in authentication failures.
- **Don't compromise on Backups.** It's an obvious point but backups are not always done well. It's no use if ransomware can infect a local backup server, or encrypted files can immediately overwrite your remote backup.
- **Consider Air Gap back ups**. Storing backup data offline and completely separate from the production environment makes it much harder for malicious parties to access your data remotely and sabotage or delete it – not forgetting to archive correctly!

What can you do?

If ransomware does get in, you need to ensure your network is set up to stop the infection spreading.

2. Avoid ransomware spreading

- **Limit use of Administrator accounts** (e.g. Don't configure your Smoothwall's AD link with it!)
- **Avoid routine logins** as a privileged user.
- **Close internal shares** and links between servers that aren't needed.
- **Configure file screening on local file shares** to prevent users downloading malicious file types once the ransomware is in the network.
- **Adopt network segregation** (VLANs) for valuable assets and guest networks.
- **Have fewer on-site servers**. Active Directory and Exchange are easier to encrypt, and easier to use to spread malware. AAD, Gsuite, and other managed cloud systems offer better protection.
- **Ensure up-to-date AV** on all systems, (it's an oldie, but it still works).
- Consider using a **DNS provider which blackholes known C&C** so payloads cannot 'contact home'.
- **Configure your Software Restriction Policies** to maximise restrictions. Tools like AppLocker can help by allowing you to create rules to allow or deny apps from running based on unique identities of files and to specify which users or groups can run those apps.
- **Use individual 'Service Accounts'** for specific applications.
- **Limit who can enable the Remote Desktop Protocol** onto machines and servers. You can configure security settings on servers (as desktops) and in Group Policy to prevent unauthorised access. It's possible that any user can gain access to a server via RDP especially if it's running Active Directory or contains sensitive information. Properly configured RDP policies on servers can help mitigate risk.
- As a last attempt to stop the ransomware from encrypting everything **consider enabling File Server Resource Manager** with a tool called CryptoBlocker-maste: (https://github.com/nexxai/CryptoBlocker) and the file types are pulled from here https://fsrm.experiant.ca/api/v1/get.

What can you do?

The next job is to minimise the pain of the infection.

3. Avoid ransomware hurting

- Remember Restores. Restore is backup's kid brother who everyone ignores. If you don't know how you will restore, you have no backup.

  What's the first thing you need to restore? How long will it take to restore a remote backup over your link? Figure these things out.

- Test your backups! If your backup hasn't been working since 1999, or it can't be restored, you'll feel the pain.

- Consider a heterogeneous cloud environment. If your MIS is in the cloud it's impossible for local ransomware to encrypt its disk remotely, and much harder to leak data from that position.

  You're outsourcing some of the work to the provider – and you could potentially get hit by their issues, hence, heterogeneous. Having a number of cloud suppliers balances risk.

- Think about GDPR data storage limitation. If you haven't got it, they can't leak it. The more data you can say 'we don't need to hold that' the less you've got to ransom.

- Know where your data is – this is a great precursor to a backup strategy, and likely done as part of data protection exercises. Use your colleagues around the school, such as data officers, to help.

What can you do?

Invest wisely – where not to spend.

In our view there are two areas that are probably not a good use of your budget.

Fancy firewalls. They only really protect on-network devices, and since everyone's taking everything home, the effectiveness of the cleverest "NGFW" tools is much reduced.

Additionally, with most traffic encrypted, firewalls can see less than ever, making IDS/IPS much less useful.

SIEM. Although real-time visibility across your organisation's information security systems might seem like a sensible investment, they're probably more applicable to corporates who have teams for monitoring.

Every penny spent here needs three pennies spending in human costs for management, monitoring and response. This is outside a school's budget, and as such spend on SIEM alone will likely offer poor ROI.

Further information

Thank you for reading.

If you would like to add to this article or share an experience please contact us. We'd love to hear from you.

Glossary

SIEM – Security Incident and Event Management. It is a log-aggregation and alerting platform to try and correlate and spot security incidents in your network.

Ransomware – Any malware which uses the threat of data loss (usually by encryption) or data leak to extort money.

NGFW – Next Gen Firewall, firewalls from circa 2010 started building in signatures to classify network traffic.

C&C – Command & Control – the way malware calls home to ask "what next".

More help & documentation

Cyber security training for school staff - NCSC.GOV.UK

Cyber Security for Schools - NCSC.GOV.UK memo-what-we-urge-you-to-do-to-protect-against-the-threat-of-ransomware17.pdf (documentcloud.org)

Have I Been Pwned: Check if your email has been compromised in a data breach

Quad9 | A public and free DNS service for a better security and privacy

RdpGuard - RDP Protection, Stop Brute-Force Attacks on RDP, POP3, FTP, SMTP, IMAP, MSSQL, MySQL, VoIP/SIP. Fail2Ban for Windows. Stop RDP, MSSQL, FTP brute-force attacks on your Windows Server.

Terminal Services Protection. https://www.fail2ban.org/

Ransomware warning: There's been another spike in attacks on schools and universities | ZDNet

Smoothwall
Avalon House
1 Savannah Way
Leeds Valley Park
Leeds
LS10 1AB

www.smoothwall.com

T: +44 0800 047 8191
E: enquiries@smoothwall.com

Smoothwall Inc
1435 West Morehead Street
Suite 125
Charlotte,
NC 28208
USA

us.smoothwall.com

T: 800 959 3760
E: inquiries@smoothwall.com

smoothwall®