Re-thinking cybersecurity in education

The increase in scope, scale and sophistication of cyberattacks, are having severe impacts on education institutions globally. As one of the most targeted segments, these institutions are having to re-think their cybersecurity strategies.

- Reports indicate the recent shift to cloud-based virtual learning has given hackers new opportunities to exploit education networks.[1]
- Between August and September 2021, educational organisations were the target of more than 5.8 million malware attacks globally, or 63% of all such attacks.[2]
- 2022 data indicates education and research are the most targeted sectors with:
    - Australia/New Zealand as the most attacked region, followed by Asia and Europe
    - And Latin America experiencing the largest increase in weekly cyberattacks.[3]

5.8 million malware attacks globally

Education institutions are also disproportionately targeted with ransomware attacks, causing students and faculty to lose valuable classroom time and putting educational goals at risk.

- In September 2022 a ransomware attack on Los Angeles Unified School District (LAUSD) prompted an unprecedented shutdown of computer systems that led to ongoing disruptions to email, computer systems and applications[4]
- In May 2022, 157-year-old Lincoln College in Illinois shut its doors after a financially debilitating ransomware attack[5]
- In 2021 UK cyberattack shutdown email, phone and website communications at 15 schools, bringing online learning to a halt[6]
- In 2021 a large-scale cyberattack on the Universidad El Bosque in Bogotá, Colombia, compromised institutional, academic and financial platforms for three days[7]

It's time to think outside the box

Traditional approaches to network cybersecurity, on their own, are no longer enough.

- In 2022, the National Cyber Security Centre in the UK found that 78% of schools analysed had been hit by at least one cybersecurity event, even though 99% had antivirus solutions in place and 100% had a firewall[8]
- As the internet and handheld devices dominate, the network edge now extends beyond the physical campus perimeter
- A Zero Trust Network Access (ZTNA) cybersecurity strategy trusts no user, no device and no application. It assumes:
    - The network is hostile
    - External and internal threats are always present
    - Location is not enough to determine trust

78% of schools analysed had been hit by at least one cybersecurity event

With the right approach to implementing a cybersecurity strategy, educational institutions can focus on teaching and learning, rather than technologies and threats.

Source:

1. America's Schools Face Mounting Threats from Cyberattacks. RealClear Education, May 2022.
2. America's Schools Face Mounting Threats from Cyberattacks. RealClear Education, May 2022.
3. Education sector seeing highest volumes of cyber attacks. SecurityBrief New Zealand, August 2022.
4. Los Angeles school district warns of disruption as it battles ongoing ransomware attack. TechCrunch+, September 2022.
5. Ransomware attack shutters 157-year-old Lincoln College. CBS News, May 2022.
6. Cyberattack shuts down online learning at 15 UK schools. zdnet.com, March 2021.
7. The Universidad El Bosque has regained control of its digital platforms. NewsBeezer.com, July 2021.
8. Cyber Security Schools Audit 2022, National Cyber Security Centre, 2022.

Learn how ALE education solutions can help your institution develop a zero trust network cybersecurity strategy, or contact us today to discuss your specific needs.