NEN – The Education Network

Technical Strategy Guidance Note 4:

e-security: issues & questions to consider

March 2013

Keeping school networks safe and secure is a complex challenge. New risks and threats continue to emerge daily. New initiatives such as bring your own device (BYOD), where personally owned devices such as smartphones and tablets are allowed to connect to a school's network, can provide many benefits, but can create a plethora of security issues and incidents if not implemented properly.

This guidance note provides a brief overview of the range of e-security issues for schools to think about and some questions to ask broadband service providers. As with all e-safety and e-security considerations, unfortunately there is no "silver bullet": effective network security depends not only on technical measures, but also upon the existence of appropriate policies and procedures, as well as effective user education for learners and staff. All of these different elements must be reviewed and updated regularly to ensure currency and relevance.

The range of issues to consider includes:

- Physical security of network equipment (facilities & buildings)
- Mobile device security and management – encryption of sensitive data, antivirus to prevent the spread of malicious code and software
- User management & account security – authentication, authorisation, password policies
- Information handling & data security[1]
- Network & Internet security – firewalls, filtering[2] and monitoring, access control

Some questions to ask broadband providers when considering connectivity options:

- What network-level monitoring in place to detect malicious software (viruses, worms, Trojans)? The most common current attack vectors are probably code hidden in websites (drive-by downloads), email attachments and USB devices, all of which are used to exploit vulnerabilities in a user's operating system and/or other software.
- What measures are in place to protect the institution's network from intrusion and attack? Appropriate network security devices (e.g. firewalls) should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the institution. The security and configuration of network equipment (e.g. switches, routers, firewalls) should be regularly reviewed and maintained. Security features, service

[1] Also see http://www.nen.gov.uk/files/NEN_Guidance_Note_1_protecting_school_data.pdf

[2] Also see http://www.nen.gov.uk/files/NEN_InfoSheet_3_Differentiated_Filtering.pdf

levels and management requirements of all network services should be identified and included in any network services agreement, whether they are provided in-house or outsourced.

- Firewalls and routing: how will traffic to/from the institution's network be controlled? What router management and connection monitoring and support services are available? Each institution should have their own means of controlling traffic to and from their network. If an institution has procured its own broadband connection this would usually mean maintaining its own firewall and/or a series of firewalls at strategic locations in order to prevent unauthorised network traffic. Only authorised traffic should be allowed to traverse the network and so it is advised that access is only allowed from necessary locations and only to necessary services.

- Where does responsibility for network administration reside? Network management and control should ensure the security of information in networks and the protection of connected services from unauthorised access. Responsibilities for network management should therefore be clearly assigned and all networks should be managed by suitably qualified and experienced staff.

- Are any managed security solutions offered, such as firewalls and intrusion detection systems? Security features of services could be technology such as authentication, encryption etc. or procedures to restrict access to services or applications.

- Is any segregation of network traffic possible? Ideally network traffic should be appropriately segregated with routing and access controls between the domains. This could include, for example, separating traffic on untrusted, "public" networks, from that of staff and students. Thought may also be given to segregating critical assets where the loss or compromise of that asset would have a big impact on the operation of the unit. Demilitarized zones (DMZs) could be used, for example, to protect access to major services such as mail servers, web servers or domain controllers. Consideration should also be given to the segregation of wireless networks from internal and private networks.

- What support is provided for user and account management? Authentication and password policies will need to be developed and maintained locally if not selected as part of an RBC- or local authority-provided service.

- What filtering and monitoring is available to protect against malicious or undesirable web and email content (drive-by downloads, spam, phishing attacks)?

(Adapted from The University of Oxford's Information Security Toolkit, http://www.ict.ox.ac.uk/odit/Information_Security_Toolkit.pdf)

Guidance Notes explain concisely a particular aspect of the broadband services required by schools to deliver education. The Education Network cannot accept responsibility for the application of these ideas to individual schools and local expert advice should be sought.
Audience: Bursars, Network Managers, Technical Support Staff.

For further information and updates, see http://www.nen.gov.uk