DERBY CITY COUNCIL

AUDIT AND ACCOUNTS COMMITTEE
2 April 2009

Report of Director of Resources

ITEM XX

'CONFICKER.B' VIRUS INFECTION

RECOMMENDATION

1.1 To note the report and future actions and recommendations.

SUPPORTING INFORMATION

Background

2.1 On 4 February 2009 the Council's network was infected by the Conficker.b virus. The original infection occurred in one of our libraries, almost certainly through the use of an infected USB memory stick. This then infected one of our servers which initiated the user account attacks.

2.2 The Council's anti-virus - AV - settings did detect and remove the infection, but its aggressive replication methods meant it was able to attack machines that were fully patched and protected, along with infecting any machines that were not fully protected.

2.3 There were a number of Council PCs that did not have either the latest version of the AV software installed or the appropriate Microsoft - MS - patching level applied. This was mainly due to either a corrupted AV software installation, old PC machines running Windows 2000 below Service Pack 4, or PCs being added to the network and not being picked and identified by the AV software.

2.4 The extent and aggressiveness of the infection meant there was disruption to Council users (some users experiencing significant disruption) even though all servers and the majority of the PCs were fully protected. The main disruption was through users being unable to log on to the network due to their account being locked out by the virus.

2.5 Many organisations, both public and private sector, have been hit with the same virus. Some estimates put the infection rate at about 15 million.

Actions being taken

2.6 The following actions have been taken …

- All computers have had the latest Microsoft and AV software updates installed. Although we had rolled out and installed the required updates, some machines

were unable to receive and install the updates. Unfortunately, in some cases, the returning message - 'not applicable' - did not really indicate in a satisfactory manner that these machines were not protected. This applied to in particular the Windows 2000 PCs.

- Increased levels of scanning has been implemented to scan all write files as well as read files.
- Auto boot/run for USB and CD drives has been disabled.
- Sharing Services on PCs has been disabled.
- End of day scanning on all PCs on closedown has been implemented.
- Any infected PCs are immediately removed from the network.
- All Windows 2000 PCs below service pack 4 have now been eliminated from the network.

Lessons learned

2.7 The following key lessons have been learned …

- Too many gaps were found in the MS patching and AV cover. Gaps in patch management and AV definitions should have been more rigorously investigated.
- Inventory management and accuracy was found to be lacking. Workstations that were meant to be decommissioned were found connected to the network.
- Running an old estate of devices, well past official support deadlines for operating software, leaves the network vulnerable to virus attacks and reinforces the need for a managed desk top re-fresh programme, along with locking down the desktop with a clearly defined and controlled standard desktop image.
- Only Council issued and controlled USB memory sticks should be used on machines connected to the Council network and these memory sticks should not be connected to non Council devices.

Future actions/governance

2.8 The following areas are under review with a view to implementation …

- All workstation shares are set to read only via AV policies.
- All workstations and servers are rigorously patched. Any exceptions must have a support call raised for further investigation.
- All workstations and servers are rigorously kept up to date with the latest AV definitions. Any exceptions must have a support call raised for further investigation.
- Remote workstations (such as home workers/Councillors) must have policies to update AV definitions directly from McAfee on start up and update patches directly from Microsoft and be immediately installed.
- Inactive accounts and decommissioned PCs must be identified and be removed from access to the network.
- Policies governing the use of USB memory sticks need to be reviewed.
- Actions in paragraph 2.6 need to be reviewed and possibly amended for continued implementation.
- A more robust approach to inventory management and control is needed to be implemented both corporately and within departments.

Summary

2.9 Weaknesses in the Council's software update procedures and inventory management, coupled with an ageing PC estate, left the Council vulnerable to this determined and aggressive virus worm which installed itself on our network and which is extremely difficult to remove. This worm is technically very complex and advanced, and was of a format not seen for quite a long time with the ability to propagate in multiple ways and change its identity.

2.10 We will address these issues in conjunction with our new IT FM supplier, Serco. Improved inventory management, stricter and more rigorous procedures for patches and software updates, and the introduction of a desktop re-fresh programme will address the main issues. In addition, revised usage policies and governance framework should provide us with significantly enhanced protection from a similar attack in the future.

For more information contact: John Cornall 01332 255334 e-mail john.cornall@derby.gov.uk
Background papers: None
List of appendices: Appendix 1 – Implications

Appendix 1

IMPLICATIONS

Financial

1. We have spent around £35,000 on staffing resources, on activities to tackle the virus infection and provide better protection in the future.

Legal

2. None directly arising.

Personnel

3. None directly arising.

Equalities impact

4. None directly arising.

Corporate objectives and priorities for change

5. None directly arising.