End of Life Microsoft Products

Windows XP Service Pack 3	April 8, 2014
Office 2003	April 8, 2014
Small Business Server 2003 • Dictated by Exchange Email Module	April 8, 2014

This is the last year of extended support for a number of Microsoft products. After that time these products will no longer have security updates by Microsoft and so become an increasing risk to your company as malware targets newly discovered weaknesses of these older systems.

The risk to your company will increase as time goes by when exploits are found and activated in the wild. Your antivirus software, if it has Internet security components will mitigate but not eliminate these risks.

Small Business Server 2003

Already some components of this operating system have dropped out of support. The SQL database and SharePoint components expire from support in April and June 2013 respectively. While the SQL and Sharepoint components are possible avenues of attack the greater risk is the Exchange email system set to expire from support in April 2014.

The Exchange email system is one of the portals into your company. Good Exchange aware antivirus can assist in protection but exploits of the email system are inevitable.

Our advice is that you should be budgeting to update this software and possibly hardware to the latest version as soon as possible.

Windows XP Service Pack 3

Service Pack 3 is the last version of XP that is available. This operating system was first released in August 2001 so is coming up to 12 years old. Microsoft has decided to cease support for this operating system on the date shown above. Avenues of attack on user machines are generally through the Internet Browser but also through crafted Trojans aimed at weaknesses of the operating system. You should start to arrange an upgrade of these machines to Windows 7 or later and speak to us about strategies for maintaining these machines in the interim. These strategies can include:

- Checking they are upgraded to the last version of XP Service Pack 3 you can do this by right clicking on the My Computer Icon and going to the Properties menu item.
- If Internet access is not required then arrange to have these machines removed from Internet access.

- If email is not required on that machine remove the email client.
- Make sure antivirus is up to date on those machines.
- Check that all security updates have been applied to the machine.
- Arrange to remove install rights from users on those machines; this will slow the ability for Malware to install itself.

Our staff can assist you with an audit to determine the level of risk and update status.

Office 2003

Office 2003 includes Outlook so if you are using the Outlook email package from that version you are at risk. Email is one of the most common attack vectors, usually by Social engineering methods. We have all seen the Click Here you have Won $5000 etc type of Phishing email. Less common exploits that are in the wild use Excel spread sheets, PowerPoint presentations and Word documents that are crafted to install malware.

After this version of Office will fall out of support these methods of attack are likely to get more frequent. Mitigation options are:

- Remove Outlook from machines that do not need email.
- Make sure all Office updates have been done; this is a temporary band aid.
- If a machine does not require Office remove it from the machine.
- Upgrade to Office 2010 or later.
- If you do not require Outlook then use one of the Free Office suites such as LibreOffice. Note while the files produced by LibreOffice are compatible with Microsoft Office sometimes minor formatting variations can occur.

Our staff can assist you with an Office replacement/upgrade program.

One of the first stages is to determine what operating systems you have and the hardware platforms they are resident on. This will determine if hardware needs to be upgraded to support a later operating system. We can provide a free audit to assist you to plan and upgrade path over the next year.

Give us a call: 1300 654 783