Hack attack on a hospital IT system highlights the risk of still running Windows XP

January 22 2016, by Robert Merkel, Monash University

An out of date operating system can let the hackers in to your computer network. Flickr/Don Hankins, CC BY

A virus attack on the computer system of one of Melbourne's largest hospital networks is cause for concern because it affected machines running Microsoft's Windows XP, an operating system no longer supported by the software giant.

A report this week in The Age said a "computer virus" has affected Windows XP systems across the hospital, interfering with the delivery of meals and pathology results. Staff have resorted to "manual workarounds", telephones, and fax machines to ensure continued delivery of these services.

A statement from the Royal Melbourne Hospital said IT staff at Melbourne Health, the network that runs the hospital, were doing all they could to "restore the remaining Windows XP computers" as soon as possible.

While the virus has been disruptive to the organisation, due to the tireless work of staff we have been able to minimise this disruption to our patients and ensure patient safety has been maintained.

While critical patient treatment is, according to the hospital, unaffected, it has clearly been a major inconvenience for the already hard-worked staff of a busy hospital.

Further, existing patient data could have been compromised by the breach, as The Age reports:

When asked if the virus would jeopardise the safety and privacy of patient's records, she made no comment.

Health-care providers are hacker targets

While all IT systems are targets for hackers, health-care IT systems have not traditionally been thought of as attractive targets for cybercriminals. But the data they hold is highly lucrative in the hands of crooks.

When you enter a hospital, a great deal of basic personal information, such as your name, age, date of birth, marital status, a variety of contact details, and possibly billing information including health insurance provider and banking details, is recorded. Cybercriminals can use this information to commit identity fraud.

Identity fraud encompasses a wide variety of crimes in which a criminal pretends to be you for financial gain. According to the Australian Federal Police, such crimes can include applying for and using credit cards in your name, gaining access to your bank accounts and even applying for government benefits in your name.

Cybercriminals operate well-organised global black markets in illegally obtained information, as well as tools for obtaining and exploiting it. Both the computer company Dell and journalist Brian Krebs have described how collections of data from health-care providers are bought and sold on these markets.

The reported information on the Melbourne Health attack makes it impossible to judge whether this was a deliberate attempt to steal patient data for profit. Regardless, hospitals and other health-care providers are and will continue to be the target of skilled and well-resourced criminals.

The end of Windows XP

But let me return to the issue of the affected systems running Windows XP. This version of Microsoft's Windows operating system was originally released in October 2001.

Over more than 12 years, Microsoft regularly released updates that fixed bugs in XP, including many security related patches. In any large software system, the number of bugs is never zero, and they can remain present but unknown for many years.

For instance, the Shellshock bug which affected Unix systems was at least 20 years old when discovered in 2014.

Microsoft advised in 2008 that Windows XP support would end in April 2014, and stuck precisely to this schedule. Its announcement warned of the security consequences of continuing to use XP:

> *Without critical Windows XP security updates, your PC may become vulnerable to harmful viruses, spyware, and other malicious software which can steal or damage your business data and information. Anti-virus software will also not be able to fully protect you once Windows XP itself is unsupported.*

Antivirus software vendor Symantec also said that its products are not sufficient to protect a system running XP.

XP unpatched

Since April 2014, several serious security faults have indeed been found in Windows XP, which have not been patched. Some of these faults allow a hacker to take full control of an XP system remotely.

While a few specialised variants of XP used in "embedded systems" such as ATMs are still supported, all consumer and mainstream business versions are now unsupported by Microsoft. This includes versions with Service Packs installed, as well as the Professional Edition.

Some large customers, including the US Navy and several Australian government departments, continue to pay Microsoft for custom support. While these support contracts are negotiated privately with Microsoft, media reports indicate that the price of supporting XP, and its cousin OS Windows Server 2003, is steep, and doubles each year.

It's unclear whether the Melbourne Health computers affected by the security breach were covered by a support contract with Microsoft. Even with support, XP lacks a number of security features present in more recent versions that make it harder for hackers to take advantage of any security bugs.

Time to let it go

Web access statistics suggest that roughly 2.5% of Australia's desktop computers still use Windows XP. While a few will have some protection due to support contracts from Microsoft, the vast majority are now completely unprotected.

Anybody who uses such a computer connected to a network is a sitting duck for hackers, who can and will attack them.

All users with an unsupported copy of XP, even if they have antivirus software, are vulnerable and should cease using the operating system as soon as possible. Organisations storing large amounts of private information are particularly likely to be attacked.

Home and small business users still using XP are likely to find that they will require a new PC if they wish to continue to use the latest version of Windows. Fortunately, low-end Windows PCs are cheaper and more capable than ever.

Alternatives such as tablets and Chromebooks can be a viable, low-cost and lower-maintenance option for users with basic computing needs.

But if you do nothing, and continue to run Windows XP, then you'll have no excuse when your system gets hacked. The malware used against Melbourne Health can, and almost certainly will, be used against others.

Provided by Monash University

Citation: Hack attack on a hospital IT system highlights the risk of still running Windows XP (2016, January 22) retrieved 10 May 2024 from https://phys.org/news/2016-01-hack-hospital-highlights-windows-xp.html