

Top 5

security considerations

In the last issue of myVistorm, we produced Vistorm's top 10 security considerations for 2008. We now look at the first five topics in more detail

1 Data leaks

Data leakage prevention has already been dealt with in detail, but it is worth drawing attention to increased public awareness of the issue, increased interest from the press and increased powers assigned to the Information Commissioner – particularly with respect to spot checks on government departments.

2 Client-side attacks

There has been a sustained trend in attacks: the majority are targeted at desktops and particularly the applications that they run, rather than at servers. Look at Microsoft patches in recent months. The majority have been for office applications rather than operating systems services. There have been vulnerabilities and patches for pdf, Flash, Quicktime, Firefox, among others; the list is endless.

You can minimise the risks by reducing the number of applications installed and by ensuring that your patching strategy covers all the applications you use, not just those covered by Microsoft Windows Update. Many client-side attacks are delivered via web browsing or email, so filtering of these can also assist.

3 Patching

You may have heard the quip: "Data wants to be free, software wants to be wrong" and there is an element of truth in it. If all software were perfect, most computer security would be unnecessary. Perfect software does not exist! That means applications need to be fixed when problems are found. Unfortunately, patching is not going to go away. You need to minimise the period for which vulnerable software is exposed; the time between an exploit becoming available and applying the patch to fix it.

One of the problems with releasing patches is that by comparing the code before and after the patch, it is possible to see what has been fixed, and therefore what the vulnerability was. Using this technique, the time for developing exploits has been decreasing leading to another quip: "Patch Tuesday, reboot Wednesday, exploit Thursday".

Recent work has even demonstrated the ability to automatically generate exploit code on the basis of patch files. All of which means that defenders have to apply patches more quickly.

There has always been a tension between the need for patching and the desire for stability, testing and change management. I believe the threat landscape is such that many change management policies are now out of date; the risks of not applying patches rapidly have increased, the risks of the patch going wrong have got no better, and, with improved testing strategies by the

vendors, have arguably decreased. If you have not reviewed the risk balance that informs your change management process, now is a good time to do so.

The risk balance will not be the same across all your systems. It is quite possible that the risk (measured as likelihood times cost) of a patch failure for a server is high because of the high value of that server and the bespoke software running on it. The corresponding risk for your desktops might be much lower, although the way desktops are used may expose them to a much higher risk of attack. Consequently, you may adopt different approaches for patching your servers and desktops. If you have not reviewed your patch management strategy recently, now is the time to do so.

4 Targeted phishing attacks

In the first quarter of 2008 there have been multiple reports of targeted phishing attacks, with a number of governments drawing attention to this as a real and significant threat. Examples have been:

- ▶ Emails to organisations supporting Tibetan independence supposedly containing the latest news and reports on that country
- ▶ Messages to business leaders suggesting that a subpoena had been issued against them
- ▶ Reports sent to senior managers from the Better Business Bureau indicating that a complaint had been made against their company

The sender seems plausible, the content is designed to make the receiver want to react and there is typically an attachment that, if opened, infects the recipient's machine.

This is a very difficult problem to combat without draconian measures such as blocking attachments on all external emails, which is probably not practical. Some technologies such as digital signing and gateway anti-virus may help but none gives a perfect practical solution. User training will also help, but it needs to be concentrated on the senior officers of the company, whose attention is notoriously hard to obtain.

5 Evolution of spam

In 2007, we observed a cat-and-mouse game as attackers tried different delivery formats such as pdf and even mp3 audio files and defenders responded. In 2008, we have not seen any major changes to that, though there have continued to be major spam releases from some botnets around special events and holidays with subject lines and content appropriate to the calendar.

Although Voice over IP does not yet suffer from the same level of unwanted communications as email, there is undoubtedly the potential for exploiting this new medium. It has been good to see work in the standards bodies to identify mechanisms for controlling this before it becomes a real problem.