

## **Network Box white paper: Forgotten Security Part 4: Keeping up-to-date**

Many vendors now have a rigorous attitude towards patching and updating their systems. These days, Microsoft is frequently used to demonstrate best practice and other manufacturers are following suit to provide regular updates to their systems.

However, there are many places where this admirable policy is not being followed, or may not be feasible. A good example is routers: the devices at the very front of any LAN and - you would think - a vital part of any network. And yet, sitting as they do outside the firewall, they are frequently ignored. Routers have had a number of vulnerabilities over the years. If they are compromised, the company can experience denial of service (DoS) attacks, or the router can act as a foot in the door of the network to hackers.

In our experience, there are two common questions IT teams ask:

### ***Does my equipment need updating?***

Many companies are not aware that some of their systems needs to be updated to protect them. While vendors strive to keep their customers informed, there is so much information assailing the IT department that their warnings are often (and easily) overlooked or ignored, or - more likely - just given a very low priority. This year, we have seen a number of hospitals fall victim to Conficker many months after patches were made by the manufacturer that would have made those very systems immune to the infection.

### ***Is the update relevant to my device?***

For instance, in a small network, the router may be the firewall and may have wireless. If the company does not use the wireless and it is disabled, then should they update their router with a patch specifically for the wireless? Many people take the view that there's no harm in updating. But this requires a risk assessment by the IT manager, and can lead to the issues outlined below.

### **To patch or not to patch?**

In order to ensure your system is up to date with the latest security patches, use the following checklist:

1. Make sure you know whether your vendor provides the patch as part of their service, or whether you need to buy a service contract.
2. Where do you get the patch, and which one is compatible with your company's system? This is important to get right - installing the wrong patch could easily crash a system, making it inoperable. This obviously can have a serious impact on productivity.
3. Test the patch. Once the patch has been downloaded, it has to be tested with the option of rolling back if a mistake has been made. Ideally this is done on a separate but identical device to the one that is in use. This allows the IT department to download, install and test the patch before putting it into production. Cost limitations mean it is not always possible to have a spare sitting around gathering dust so the production system sometimes has to be used.

4. Arrange for a time for the system to be taken offline so the patch can be installed and tested. Of course, this can have a serious impact on uptime. But, if the patch causes a problem, disruption to service can also be significant. The result is that major updates are usually done after hours – which can result in overtime costs. If a mistake is made, production time will be lost once the workforce comes back online.
5. What happens if the system goes wrong? What are your replacement agreements with suppliers, and how long will it take to get a replacement? Are there additional costs for delivery? Consider your rollback options.

### **Assessing risk**

Which brings us back to the risk assessment: is it worth taking up the patch that the vendor has made available? What is the risk and is it worth the possible pitfalls? It is easy to see why many companies don't bother, and leave themselves vulnerable.

Patching and updating security is vital. The sooner it is done, the better. But, if it is done without care, it can result in the same downtime that the company is hoping to prevent by installing the patch in the first place.

### **Buyer's checklist**

These are all issues that should be considered at the point of buying a system, service or device. Ask the following questions:

- How easy is the system to update?
- What do the vendors do to make you aware of any issues?
- Where can solutions be downloaded and installed?
- How can you test the patch?
- Can you roll back to how the system was before installation?

Failure to carry out updates in a systematic way can result in downtime, reduced productivity or even compromise the network. Getting it right at the point of purchase can save major headaches later on.

**For more information on securing your company network, visit**

**<http://www.network-box.co.uk>, or  
call James Mackie on 0800 107 6098**

**To keep up with news from Network Box, see Simon Heron's blog:**

**<http://blog.network-box.co.uk>; or follow him on Twitter:  
<http://www.twitter.com/networkbox>.**