The Hidden IT Security Threat: Multifunction Printers

(CIO Network - written by Larry Kovnat)

In March 2008, an attack known as an SQL injection was used to install spyware on Heartland Payment Systems' network, exposing 134 million credit and debit cards. The vulnerability to SQL injection was well understood; security analysts had warned retailers about it for several years. Yet, the continuing vulnerability of Web-facing applications made SQL injection one of the most common forms of attack against websites at the time.

Fast forward to 2011, when a massive breach of Sony's PlayStation Network led to 77 million accounts being hacked and millions of dollars in lost revenue for Sony. Hackers gained entry via a hole in the network that had been open for quite some time, even though analysts continually recommended identifying and applying security controls consistently across the entire organization.

What's notable about these attacks – as well as many others – is the fact that there were many warnings about the potential vulnerabilities in these networks, but nothing was done until it was too late.

So here's a warning for 2013: it's time to take multifunction printer security seriously.

According to InfoTrends, there are almost 30 million printers and multifunction devices in offices and homes throughout the U.S. and Western Europe, and most are connected to a network. This means they are just as susceptible to malware and hacker attacks as PCs -but for a variety of reasons they are often overlooked by IT professionals and used without proper safeguards by employees.

To further this point, consider these telling findings. A recent Xerox-McAfee study revealed that more than half (54 percent) of employees say they don't always follow their company's IT security policies. Also, half (51 percent) of those employees whose workplace has a printer, copier or MFP say they've copied, scanned or printed confidential information at work.

Sound familiar?

The study goes on to say that more than half (54 percent) think computers pose the biggest security threat to their company's network compared to other IT devices, while only 6 percent say it is MFPs. This small percentage is proof that employees simply do not realize their office MFPs really are true networked devices that behave the same way their PCs do – and have similar vulnerabilities. Pair these stats with the fact that the average organizational cost of a data breach is $5.5 Million and you have a pretty strong argument for taking this warning seriously.

But I know what you're thinking: none of those massive breaches are possible through an MFP, right?

Wrong.

Just about anyone can launch full-scale attacks against a network and a company's information assets through an MFP if its physical and electronic access points aren't securely controlled and protected. Those attacks can be as simple as someone picking up documents left in the MFP's output tray, to malicious worms pulling sensitive documents off the network.

Consider this example of hacking the network through an MFP: Today's combination of mobile workers, cloud printing and the continuing penetration of Android-based personal devices make it possible for an attacker to create a malware app that infects the mobile device, opportunistically attaches itself to a cloud print job, gets downloaded to a networked MFP, and from there infects the entire enterprise network, completely bypassing firewall and intrusion detection controls. In this case, it's complexity that creates the vulnerability.

There is also the issue of something called device decommissioning. Enterprise MFPs handle large volumes of data and have integrated disk drives. Unauthorized access to this stored data by both people and processes running within the MFP's operating system could reveal sensitive or confidential material – think along the lines of private documents you've scanned and sent to HR. One example of this information falling into the wrong hands was when the Buffalo, N.Y. police department sold off some older MFPs that had reached the end of their useful life. As part of an exposé in 2010 by CBS News, identifying information related to ongoing police investigations was easily discovered on the hard drives of these decommissioned machines. And this is not uncommon.

Companies need to properly lock down their MFPs, but traditionally there has been a limited availability of printer security solutions to keep them Fort Knox safe. At minimum, here is what IT administrators need to do to protect the network:

- Control access to the MFP and its functions at the group, individual, and activity level.
- Ensure data is secure at every stage of the workflow – from the data path along the network to the device itself.
- Use all available tools to protect sensitive documents from loss or theft.
- Always include MFPs in standard network security measures and policies.

To accomplish all of this in the simplest way possible, companies should consider choosing an MFP with security software integrated directly into the device that operates with a "whitelisting" method. Whitelisting allows only approved files to run, offering significantly more protection for embedded systems than traditional black listing tactics, which depend on continuous updates of signature files in order to remain current. Certain embedded security software also provides an immediate alert and audit trail to track and investigate the time and origin of security threats – and spurs appropriate action.

Moving forward we will see a push to where users are no longer scared of the "multi" in multifunction printers enabling them to do more with the devices – like network scanning. We're finally approaching a time where the MFP is considered a "true citizen" on the network rather than a rogue device or an outlier – and taking the time to protect it is an integral part of today's security imperatives.