technopedia

August 16, 2013

The Simple Answer to Many Major Security Breaches? Thumb Drives

By Justin Stoltzfus

Takeaway: Many of the biggest security breaches occurred through a USB stick.

Network administrators can do a lot to mitigate security risks. They can install cutting-edge anti-virus and anti-malware programs, monitor their systems for outside threats, and install authentication or multi-tiered access tools to engineer the ways that users can access data. In putting together a comprehensive security plan, IT professionals spend a lot of time looking at different ways to filter and control cyberattacks that may happen through IP connections or files sent over the Internet. What many systems aren't good at controlling is the use of small external devices. For this, IT security planners usually rely on good old-fashioned common sense.

Unfortunately, that's where they go wrong.

Most people who work at companies with a more informed view of IT security know that they shouldn't just plug flash drives into corporate workstations or other system and points. They've been trained in the dangers that these USB drives represent. However, that doesn't stop a lot of people from plugging in any old device they may find lying around in a desk drawer, or even in the parking lot. Various studies have even found that the majority of users will try out a stray flash drive, mostly just out of curiosity.

> "You can put in as many firewalls and communication security devices as you want, but as long as the end user has the ability to plug a USB device into a computer, it is possible to completely bypass them and go directly to the computer with malware," says Neil Rerup, an IT author and the founder of Enterprise CyberSecurity Architects. "You need to treat [USB devices] as untrusted devices."

It's the assumption that these little devices are harmless that has allowed them to be used in some of the biggest security breaches in recent memory. It's how Edward Snowden got the NSA's secrets.

Planning for USB and Endpoint Security

Today's tech professionals are using some specific terms to talk about how to protect sensitive data from flash drives and other small USB devices. This idea is often part of "endpoint security" which looks

Continued on next page

Continued from previous page

at how a workstation, mobile device or other hardware piece provides access to end-users.

Planners also break down comprehensive system security into several categories including data at rest and data in use. Data at rest is data that has been successfully placed in a stable storage destination. Data in use is data that is in transit throughout a system, including data that's being routed to a hardware device with available USB connections. That's where administrators start looking at how to control all of the threats that unfiltered flash drive or thumb drive connections present.

Big Problems with USB Drives

We talked to a number of different professionals to try to figure out the main challenges that network security people face, and how they are planning to deal with them. For many of those trying to protect company systems, it comes down to malware, viruses and data loss. These Big 3 threats can be parsed and categorized in different ways, but they all relate to the kinds of casual uses of removable USB that send shivers down an admin's spine.

Sure, those in charge can simply glue in USB ports, but many companies need a more complex strategy, since USB connections do provide important functionality for hardware systems.

"Plug-in devices pose two threats to a company network: They may contain malware that can then be introduced into the network, and they enable data leakage and theft," said JaeMi Pennington, a representative for GFI, a company that provides endpoint security solutions that can determine when a certain kind of protected information is coming out of corporate systems and onto root or USB drives.

"Organizations need to deploy solutions that can detect the presence of endpoint storage devices and can also detect when information is being copied to one," Pennington said, adding that companies can also use encrypted portable drives.

According to Tony Scalzitti, a business development manager at Softpath System, the problems around USB devices aren't that different from the older threats posed by floppy disks, which could also introduce viruses to yesterday's hardware systems.

"The biggest mistake an IT organization can make is to attempt to simply disable access," Scalzitti said.

That's not to say businesses don't need to proceed with caution.

"You can put in as many firewalls and communication security devices as you want, but as long as the end user has the ability to plug a USB device into a computer, it is possible to completely bypass them and go directly to the computer with malware," says Neil Rerup, an IT author and the founder of Enterprise CyberSecurity Architects. "You need to treat [USB devices] as untrusted devices."

Rerup recommends disabling USB ports through the use of active directory policies, although he notes this may interfere with other kinds of necessary computer functions. Another alternative, he adds, is to have USB ports scanned by anti-virus packages when users hook up, which can require advanced hardware detection. In addition, Rerup suggests a kind of "USB triage," where mission-critical USB ports are allowed to remain in a board, and others are shut down.

Going back to encryption, some IT professionals are recommending broader kinds of encryption strategies that can protect data as it moves through systems.

Jaspreet Singh, a co-founder and CEO at Druva, suggests that by using encryption methods like SSL, network traffic can be protected against unauthorized access. Additional data auditing tools can also be helpful, he said..

The Interface of the Future

Even with strategies like the above, the challenges of handling USB port security issues can be daunting. The big question is whether tomorrow's generation of admin professionals will have the same worries.

Continued on next page

technopedia

Continued from previous page

In looking at whether USB flash drives will be around in the future, it's helpful to look at systems and devices without USB connectivity. One example is the lack of USB connectivity for the iPad, for example. In a recent ad (below) for Microsoft's Surface tablet, a thumb-drive-wary iPad says, "I'm sorry. I don't have a USB port ..."

So how do systems without USB transfer files? Generally, with new cloud storage systems, where the end user never has to carry a "data load" on a USB drive or any other kind of hardware. These kinds of systems feature a major trade-off; the devices aren't much good for data intake (they can't accept a simple .doc or photo file from outside the network's reach), but they provide a lot of convenience otherwise, and fewer security risks.

Another example is Google Glass, the ultra-new wearable computing interface. Since these types of devices aren't USB-connectible, file transfer will have to exist in the cloud. Over time, this may help some companies renovate their IT systems and deal less with all of the dangers of the "dirty USB."■