January 2010

Three Ways to Prevent USB Insecurity in Your Enterprise

With great advantages come great responsibilities. As the advances in USB devices have made them invaluable to most business users' workday processes, they have also exposed their organizations to three enormous risks: data loss, data theft and malware propagation. Learn how removable device policy enforcement can mitigate these risks while enabling managed use of these necessary productivity tools

Overview

When engineers first started working on the Universal Serial Bus (USB) format in 1994, their goal was to develop a single, power-efficient standard that could replace the growing number of peripheral connections that cluttered the back of our PCs. Security was the farthest thing from their mind — back then it was hardly on the minds of any IT professionals. From the establishment of the USB 1.0 standard to the rollout of iPods and thumb drives, and all the way through the development of USB 3.0-enabled mega-storage devices, portable device innovation has always been about speed, capacity and convenience. This has meant great things for the business world, which leverages these devices for incredible productivity gains. For example, workers can now use ultra-portable flash drives to easily transfer large amounts of data between locations. They can use these same devices to store important presentation information while on the road at conferences and sales meetings. And large organizations can use vast amounts of these devices to quickly disseminate information to customers or employees by uploading to devices and distributing them to the right people. Unfortunately, many of those gains could well be wiped out for enterprises if these devices end up as the enabling mechanism for a catastrophic data breach. Even as USB devices have evolved into useful storage media, they've also turned into a security nightmare for organizations. One only needs to follow the news to see that USB devices are involved time and time again in today's highest-profile data breaches, either through the loading of breach-causing malware onto the corporate network, by facilitating the intentional covert removal of data, or simply by enabling data loss through the misplacement of an unencrypted device. And it's not just USB devices that are a threat, either. In fact, they're just the tip of the iceberg. All of the same threats also extend to all forms of removable media in use today including CD, DVD and Blu-ray drives as well as FireWire- and eSATAconnected devices. Clearly, the real key to successful use of all portable devices is striking the right balance between the productivity they offer and the risks they pose.

Employee-owned mobile data-bearing devices

Understanding USB's Importance

Once a mere novelty peripheral, USB storage devices are about as common now as the mouse and keyboard. According to analysts with In-Stat, more than 3 billion USB devices shipped in 2008 alone, and those numbers will only keep ticking upward. In-Stat estimates a 6.6 percent compound annual growth rate for these devices through 2013. Portable devices have increasingly become a staple of the corporate environment, whether an organization provides them for workers or not. According to the Ponemon Institute's 2009 State of the Endpoint survey, only 26 percent of organizations have a policy that permits employees to connect their own devices to the network, and yet, a full 40 percent of respondents say their organizations allow employees to do so anyway. This suggests that many

appropriate steps are not being taken to secure mobile devices owned by employees. A recent survey conducted by Applied Research- West on behalf of SanDisk found that 77 percent of corporate users say they've used a personal flash memory device for work purposes. And that's not counting the use of other devices such as iPods, cameras and smartphones that workers commonly plug into their workstations for personal use as well. And what's more, most users don't understand the risks they take when they use these devices on the corporate infrastructure. For example, one in 10 workers surveyed by Applied Research reported having found flash drives in public places. Of those, more than half admitted that one of the first things they would do would be to plug in the foreign device to find out what was on it—a risky proposition given the amount of malware that can be downloaded upon connection with an endpoint. While many IT managers do recognize what kind of problems such end user ignorance can promote, the typical knee-jerk reaction to enact an outright ban of USB devices and other portable media is hardly the right path to follow. "This may indeed be necessary and provides immediate protection of data loss. However, it's a blunt, coarse control that really doesn't solve the underlying problem," wrote Gartner analyst Neil MacDonald about the blanket bans he's seen lately. "Such drastic policies get in the way of legitimate users trying to do their job." Instead of enacting ineffective and productivitysquashing bans that address the medium itself, MacDonald suggests organizations think about how to protect the valuable information contained on the USB and the corporate assets it connects to. "Better, how about a control that enforces a policy like 'don't allow sensitive data to be copied to a USB drive unless the data (or the drive itself) is encrypted,'" MacDonald wrote.

Surveying the Risks

Simply put, the ease of use, the prevalence of the format and the inherent insecurity of USB make it a dream for most crooks and mischief makers. Not only that, but the small size and portability that make these devices so useful also make them as easy to lose as a kid's coat on a schoolyard. To figure out a way to take advantage of portable devices without risking too much in the process, it is important to first thoroughly understand the threats that will need to be addressed. Let's examine three of the top risks:

1. **Data Loss**

By far the most common way a typical employee will expose his or her organization to risk through USB use is simply by misplacing a device containing sensitive data. It is all-too-easy to accidentally leave behind a portable device on public, unsecured computers, be they at hotels, libraries or airport business centers. It happens all of the time. In fact, the Ponemon Institute estimates that 800,000 data-sensitive devices—including USB drives, hard drives, laptops and mobile devices—are lost or stolen each year. Unless these drives are encrypted, important data could be at risk. Not only could this pose a danger to missioncritical intellectual property, but if the lost information is classified as regulated data such as customer information, the organization will also be burdened with engaging in the disclosure process. And make no mistake, employees are using these devices to store very important data. In June 2009, the Ponemon Institute released statistics that said that 69 percent of surveyed employees copy confidential or sensitive business information onto USB devices. Of those surveyed, only 13 percent said their companies have a policy allowing the practice, meaning that even blanket bans don't mean much without proper controls.

Of data losses attributed to insiders, 65.8 percent of them are due to nonmalicious insider activity - including the loss of USB devices. Source: CSI Computer Crime and Security Survey, December 2009

2 **Data Theft** The unchecked use of portable devices within an organization can also open it up to the risk of massive data theft through storage that only keeps growing in capacity. That voluminous capacity alone can make these devices a prime virtual burglar's bag to run away with the company jewels. Take, for instance, the case of an IT worker at the Federal Reserve Bank of New York who was apprehended by the FBI in April 2009 for taking out loans using false identities. The feds found a USB flash drive plugged into his personal computer that contained loan applications with the names of those identities he stole. The practice of theft via portable devices may be more rampant than most think. In fact, recent

industry surveys have shown that as many as four in 10 employees have already stolen some sort of corporate information using a USB flash drive. And when paired with certain sinister software tools, these devices can be used to even more devastating effects. One of the first programs to really highlight the threats posed by USB usage, Pod-Slurp is a great example of such a tool. Simply plugging a USB device loaded with Slurp into a victim's computer would automatically start the scripts copying each and every document from the host PC's My Documents directory onto the USB stick. One could modify the script to target spreadsheets, PowerPoint files or any specific file type of one's choice. Further, it could easily be modified to send files via e-mail or FTP instead of copying them to the USB device. What types of sensitive or proprietary information are insiders taking with them when they leave the organization? Well, according to the Ponemon Institute, 60 percent of employees reported that they would take confidential information when they left their organization. This includes e-mail lists, customer information contained within contact lists, financial information and even employee records.

3. **Malware Propagation and Hacking** It is not only corporate users who enjoy the benefits of today's USB devices. Cybercriminals are increasingly using removable media and taking advantage of end-user naivety to introduce malware onto computers. Security companies are reporting an increase in malware that propagates via USB devices and other removable media. Malware, such as the SillyFDC worm that plagued the Army in 2008, the many variants of viruses that cropped up to exploit Microsoft Autorun vulnerabilities in 2009 and several variants of Conficker, copy themselves to all drives connected to infected machines. Any USB device connected to an infected machine would then become infected, and later when it is connected to yet another machine, that machine too also begins infecting other USB devices plugged into it. This "worm-like" malware propagation method copies itself to all available drives, shares, removable media and peer-topeer software application file folders. Non-financial business information Customer information including contact lists Source: Ponemon Institute, 2009

This can greatly increase the exposure of an organization that may otherwise have its network security bases covered. One infected endpoint can easily spread malware to a shared USB stick, which then can further infect any other endpoint to which it connects. In addition to propagating malware, USB drives can also prove to be an exceptional hacking platform for those attackers with physical contact to corporate machines. One of the many legitimate, useful features of USB drives is their ability to act as a "PC on a stick" through the use of certain platform and virtualization utilities such as BartPE/ PeToUSB, UBCD4, UNetBootin and MojoPac. But again, this legitimate use can also be used for dark purposes. It also makes it possible for malicious users to replicate their entire Windows hacking lab with a USB device and run it on virtually any PC with an available USB port. When the malicious user is done, she simply removes the USB device and leaves without a trace. On the other end of the spectrum, hackers can install software on unsecured public computers to collect data off any devices plugged into these systems, so unsuspecting workers don't even have to leave behind devices to lose data. Unsecured computers infected with utilities such as USBDumper could easily and silently copy any and all information from devices that plug into these machines.

Reaping Productivity Gains without the Risks

The traditional definition of a corporate "endpoint" is clearly evolving. For millions of employees, portable media represents the next generation of endpoints, shifting from simply PCs and laptops. Because of this evolution, enterprise endpoint security must also grow to address the increasing concerns. Ultimately, this shifting corporate endpoint exposes a new threat vector that IT professionals must confront and secure. So what can you do to reap the productivity gains without the risk? enable organizations to develop and enforce granular use policies for removable devices (such as USB flash drives) and other removable media (such as CDs and DVDs) to control the flow of inbound and outbound data from your endpoints. The products that comprise Lumension Data Protection include: enforce organization-wide usage policies for removable devices, removable media and data (such as read/write encryption). seamlessly integrate the capabilities of Lumension Device Control into an already-established SCCM-managed environment to reduce implementation costs and quickly enhance security policy enforcement.

1. **Encrypt Devices to Prevent Improper Data Disclosure:** By encrypting removable media, you can ensure that it can be safely used and transported without the fear of exposing confidential data to unauthorized users. Users can access their encrypted data on any computer on the network or, optionally, even on computers that do not have client software installed. Centralized and decentralized encryption schemas provide the administrator with the flexibility to centrally encrypt removable media or enable users to encrypt removable media on their own and, more importantly, enforce the use of that encrypted media.

2. **Enforce Device Usage Policies to Prevent Misuse:** By enforcing usage policies for removable devices (such as USB flash drives) and other removable media (such as CDs and DVDs), you can control the flow of data to and from your endpoints. Devices that are not authorized are simply not allowed to execute. Through a central console, device control policies are quickly established and enforced through two simple steps: identification and assignment. Policies are managed per user or user group as well as per computer, and user groups are immediately associated with devices on the fly—dramatically simplifying the management of endpoint device resources. Auditing and reporting functions enable administrators to precisely track when devices are used, by whom and how—and even retain a copy of any data being written to a removable storage device. They can also see attempts to use unauthorized devices and track that as well.

3. **Prevent Introduction of Malware via Removable Devices:** By validating removable devices as they are used within the enterprise, you can prevent malware from being introduced onto the network. This includes assigning permissions for authorized removable devices (such as USB sticks) and media (such as DVDs and CDs) to individual users or user groups and controlling the downloading of unknown or unwanted files from removable devices.

Evolving from USB Chaos to Containment

As Gartner's MacDonald points out, using epoxy to block USB ports is not the answer. Clearly, the productivity gains brought by the many USB devices available today outweigh the safety of a total ban. In fact, given the state of today's economy, the use of USB devices should be encouraged and embraced to help reduce operating costs and improve productivity. However to win the war against mobile malware and information theft, organizations must develop and be able to enforce clear, in-depth policies regarding the use of removable devices and media within the organization. They must also deploy proactive solutions, such as support these policies. While the enterprise security war will continue to be long and trying, enterprises can gain a decisive advantage by taking a proactive approach to protecting their organizational endpoints, no matter how much they evolve. After all, the notion of a "PC on a stick" should benefit business processes, not impede them.