SMARTPHONES GET THE HEADLINES...

...But Lax USB Security is Just as Risky

Practical considerations
for the IT Professional

As first published as a Beachhead-contributed article in:

InformationWeek DARK Reading

BEACHHEAD®

They're small, cheap and in the minds of many employees, disposable.

While more expensive (and, OK, exciting) mobile devices like smartphones and tablets receive the lion's share of data security scrutiny, organizations would be wise not to overlook the profound and costly damage a company can suffer due to those simple, unsecured USB flash drives. They are small, they are cheap, and they could be easily forgotten -- if not for the fact they usually contain a ton of sensitive company data.

Employees often place confidential data on USB flash drives while giving little care to the potential risks. In fact, in today's world where issues such as BadUSB and Stuxnet fill the headlines, a 2013 AhnLab survey found that 78% of IT professionals admit to having picked up and plugged in abandoned USB drives they just happened to find. Non-shockingly, 68% of these IT professionals report being involved in a data breach, many USB-related. And while expensive devices like laptops, phones, and tablets are typically managed so that their losses are noticed immediately, many companies have no way of knowing if USB flash drives became lost or stolen.

Researchers in a recent 2014 study have found that secondhand USB drives purchased on sites like eBay often contain easily recoverable corporate or personal confidential information, with data never having been deleted in 29% of cases. If most organizations make great efforts to protectively house their sensitive data in a bunker of security software and device access policies, the lack of a spotlight on USB flash drive security makes these devices a frighteningly open door. Data is data, no matter how fancy the home that it lives in.

In our age of über-mobility and workers taking large data files with them across the work/home divide, USB flash drive use is so common it has become almost an afterthought, with tens of millions of the inexpensive devices in use and going overlooked each year. Many organizations leave USB flash drives unsecured because of not wanting to hamper worker productivity, and most use no software to detect or secure sensitive data when being moved to a USB flash drive, or to check USB drives for viruses or malware. Those same businesses, though, certainly would not extend that risk to other mobile devices like smartphones, tablets, or laptops.

USB Devices are vulnerable and carry tremendous compliance risk.

These numbers are concerning, and organizations that ignore USB flash drive security do so at their peril. In July of this year, the Duke University Health System experienced a patient data breach resulting from the theft of an unencrypted thumb drive. A similar incident in June saw the data of 33,000 Santa Rosa Memorial Hospital patients stolen in a burglary from a staff member's locker. Incidents like these prove the importance of treating USB flash drives as a critical front when an organization sets policies and strategies around device security.

Prevention techniques aren't all that different from those for employee phones and tablets. For smaller businesses without dedicated IT security personnel (but whose data is no less important), USB flash drive data security can be handled through MSPs and software resellers. Another option is services that offer

hardened and secured USB devices as a solution, but these take away the versatility of carrying a personal data device that can be used to move any file (which, of course, is the reason users like them).

Corporate data breaches are not the only security concerns; people who use their own devices for work might have personal files on them, too -- files they don't want anyone, including their company, to see. One way around this is to create a secure division within the drive, where there are two segments on the same device: business and personal (not unlike a digital mullet, if you will). In this setup, companies can control their halves of devices, securing and encrypting files, and retaining the capability to remotely wipe their data if necessary. At the same time, the personal files a user keeps on her device is separate and not mixed up with company data.

This system has several advantages as far as security and user convenience. Workers can use their own devices and keep them if they leave the company (which, let's face it, they probably would do anyway). If a device is lost or stolen, or if the worker is no longer authorized to have certain data, the company can quarantine or remotely wipe the files belonging to them. Such solutions are cloud-based; the user inputs her username and password, and the device "phones home" to the server and authenticates. If the admin hasn't blocked that device from accessing the files in its drive, then those files are available. If the admin does block them, the user can't get to them, and the admin can also simply remove the data.

That second authentication factor is key to USB device security, because with these devices the username and password credentials are often compromised. USB flash drives are designed for sharing, and the credentials are usually shared as well. Former employees will still know the passwords to devices in their possession. (In fact, we've often seen USB drives with the passwords written in Sharpie right on the device.)

Device security, be it phones, tablets, laptops, or other items, is often a balance between simplicity for the user and the strictness of control by organizations. This is certainly the case with USB flash drives. When looking at how to protect their mobile devices, companies should value the versatility employees enjoy when allowed to use their personal drives for work purposes, while putting in place measures to protect sensitive company data without encumbering their workers with difficult hoops to jump through.

The ultimate goal for companies should be to keep data readily available for those who need it to do their jobs, while keeping it safe from those who mean harm. Easier said than done, of course, but it's better than making the news for an errant USB drive with hundreds of thousands of Social Security numbers on it.

BeachheadSecure™ Mobile Device Security

The BeachheadSecure™ Management System is an entirely cloud-based management platform that enforces encryption, security and control over employee and company-owned PCs and Macs, Phones and Tablets ***and*** USB Storage. BeachheadSecure is a cost-effective solution that squarely addresses the key objectives of a business facing the challenges of a mobile workforce accessing and manipulating company sensitive data.

The USB Storage module (licenses) are seamlessly added to the BeachheadSecure administration console and enforce both encryption and authentication policy on USB devices that carry sensitive business data. Most organizations select a two-factor authentication on USB devices accessed outside its walls. The first is a (local) user name/password requirement and the second - an automatic (and silent) authentication to the server which gives administrators the ability to revoke access to a device(s) at any time.

The BeachheadSecure Platform can either be self-managed or managed on your behalf by highly trained IT service professionals that have earned "Beachhead-authorized MSP" recognition. Qualified IT professionals using this powerful cloud-based tool secure your mobile devices as an affordable monthly service with no impact to your business or employee productivity.

For more information about The BeachheadSecure Management System please contact the Beachhead Reseller Team at:

bhleads@beachheadsolutions.com

408.496.6936 x.1003