

6 steps to solving the USB problem

The most urgent security issue on all IT departments' lists is statistically "the USB problem". 20,000,000 unsecure USB drives with valuable data are lost yearly, heavily contributing to making the USB problem to be regarded as the largest challenge for IT departments as listed by Eweek and reported by Cisco.

Introduction

For sharing and transferring large quantities of data both on time and on budget, a secure USB flash drive is essential.

- There is 100% availability of USB ports on modern computers.
- Flash drives are not sensitive to scratches or dust.
- USB drives are robust, making them suitable for transporting data from place to place and solving everyday issues at the office.
- Flash drives use little power and one drive replaces hundreds of CDs or DVDs, providing long lifespan and reusable storage.
- There are no fragile moving parts and drives are small and light.

All in all there are many good reasons for solving the USB problem in a productive way. Simply put, we want to keep the productivity gains and the flexibility and ease of use that we have today. This is not the time for getting the glue gun out and going after the USB ports with epoxy. This is not the time for issuing a "no portable devices" directive. There is a way to remain productive and secure and we are about to explore this route.

Problem

The USB problem is at the top the agenda. As reported by Cisco, 33 percent of IT professionals were most concerned about data being lost or stolen through USB devices.

Over 20,000,000 unsecure USB drives are lost yearly and the USB problem has come to be regarded as the largest challenge for IT departments. When Eweek listed the top ten ways employees pose a risk to organizational security, the proliferation of unmanaged and unprotected USB storage devices took the number one spot.

Preventing disclosure of sensitive information is the issue at hand. Data stored on unsecure, standard USB drives means that data is at risk for unauthorized access. Unsecure USB drives have no way to ensure

the integrity or confidentiality of stored data. The storage capacity is growing, the physical sizes are decreasing, and this means that many people today misplace the same amount of data that a large office file cabinet would store. That this is an accident waiting to happen has been confirmed over and over again. Privacy Rights Clearinghouse maintains a list of data breaches. Since 2005 they have compiled a chronology of breaches mounting to over 250 million lost sensitive records. To add to the list of problems, there are now auto-running viruses proliferating that are designed to infiltrate hosts via unsecure USB drives. As McAfee noted in their "2009 Threat Predictions" report, this is the number one threat next to infections from web sources.

33 percent of IT professionals were most concerned about data being lost or stolen through USB devices.

Losing intellectual property on an open, unsecured USB flash drive could be disastrous for any organisation. There are good reasons to protect trade secrets, aggregated data or other sensitive records, as doing so ensures shareholder value, public confidence, and internal productivity.

The value and sensitivity of the information owned by most organizations increase and valuable information has become a target for hackers and fraudsters. Because portable information is at an increased risk of being stolen and misused, resources must be set aside to solve the USB problem.

Add to this the fact that up to two-thirds of USB drives used by businesses are misplaced at least once in their lifetime and the incentives for solving the USB problem become significant.

Resources

Example policy for USB and remote access
http://www.sans.org/resources/policies/Remote_Access.pdf

Unsecure USB is the greatest security risk, according to Eweek.
Eweek 10 Ways Your Employees Pose a Security Risk for Your Organization

7 major weaknesses with software encryption of USB drives.
<http://www.blockmastersecurity.com>

EU report - directive on USB usage
http://www.enisa.europa.eu/doc/pdf/publications/Secure%20USB%20drives_180608.pdf
33% of IT professionals name unsecure USB drives as the biggest problem in this 2008 report.
http://cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-506224.html

250 million sensitive records exposed since 2005.
<http://www.privacyrights.org/ar/ChronDataBreaches.htm>

Up to 66% of USB drives are lost.
<http://www.centennial-software.com/company/press/?id=136>

Gartner: 155 million USB drives sold in 2008.
<http://www.bizjournals.com/phoenix/stories/2007/11/12/focus21.html>

SC Magazine Trend report 2009
<http://www.scmagazineus.com/McAfee-Malware-will-use-web-and-USB-sticks-to-spread-in-2009/article/126351/>

Tags

Secure USB drive, secure USB, SafeStick, end-point security, port control, file shredder

Notes On The Author

BlockMaster is the innovator of the original secure USB drive, SafeStick. SafeStick was designed from the outset to meet the security, usability and cost demands of the modern organization. SafeStick is deployed worldwide by industry leaders.

Visit GetSafeStick.com for further evaluation and information.