DOI:10.16661/j.cnki.1672-3791.2013.27.094

移动存储设备使用过程中的风险及管控

范晓明[1,2]
(1.中国海洋大学信息科学与工程学院 山东青岛 266100; 2.寿光市信息产业管理办公室 山东寿光 262701)

摘 要:U盘和移动硬盘等移动存储设备以其体积小、存储量大、数据保存周期长等优点越来越受到大家的青睐。但对企业而言,随之引入的安全风险却大大增加,移动存储设备滥用给企业的安全管理带来极大隐患。本文将从企业安全管理、风险控制的角度出发,全面、系统地阐述如何管控对移动存储设备的使用。

关键词:移动存储设备 数据安全 数据泄露 病毒木马
中图分类号:TP309 文献标识码:A 文章编号:1672-3791(2013)09(c)-0014-01

随着微电子制造和应用技术的不断发展,移动存储介质作为信息交换的一种便捷介质,不断趋向小型化、便携化,已逐渐成为信息存储交换的首选设备,得到广泛应用。然而从企业安全管理的角度出发,由于缺少有效管理措施,导致移动设备使用中病毒交叉感染、重要信息丢失、信息泄密等安全问题不断发生。因此,在巨大的安全风险之下,而又面对着如此不堪一击的管理现状,如何才能真正做到对移动存储设备的全面管控,就成为企业安全管理员的燃眉之急。本文将从移动存储设备的全生命周期着手,探究移动存储设备的全面管控之道。

1 注册管理

外部移动存储设备想要在企业内部的终端上使用时,需要先进行注册,有管理员许可、登记造册后方可使用。注册时,详细记录注册申请人、申请时间等基础信息的同时,可以根据实际使用的需要,区分普通注册和加密注册,进而将移动存储设备分为以下三个安全等级:

(1)外部移动存储设备:未经注册的移动存储设备;(2)内部普通移动存储设备:普通注册的移动存储设备;(3)内部专用移动存储设备:加密注册的移动存储设备。顾名思义,加密注册的移动存储设备安全级别最高。

2 接入控制

在注册管理的基础之上,就需要系统保证能够自动识别外部、内部普通和内部专用移动存储设备。与此同时,管理员即可通过安全策略,定义是否允许内部终端上使用外部移动存储设备,哪些终端上能够使用外部移动存储设备,以及使用时具体的操作权限(如只读或可读写)。通过对移动存储设备的接入控制,能够完全杜绝未经管理员许可,擅自在内部终端上使用外来移动存储设备的现象发生,实现了移动存储设备规范化使用的第一步。

3 权限管理

在移动存储设备管理的整个过程中,人、计算机、移动存储设备构成了三个关键因素,全面管控的核心就是控制这三者之间的绑定和对应关系。在注册管理的基础之上,需要能够自动、唯一识别每一个已注册的移动存储设备,进而通过安全策略指定哪个移动存储设备、能在哪台终端计算机、由哪个终端用户、按照哪种权限使用,实现移动存储设备规范化使用的第二步——细粒度管控。这一管控过程可以细分为两个环节:移动存储设备与终端计算机的绑定:一旦把移动存储设备插入终端计算机,管理系统就能够自动判断该终端计算机能否使用该移动存储设备。如果能够使用,则会开放相应的使用权限如只读、可写;否则,将完全拒绝使用,并在终端用户试图打开该移动存储设备时,向终端用户发出提示信息;移动存储设备与终端用户的绑定:当且仅当该终端计算机上能够使用该移动存储设备时,系统会进一步对终端用户进行身份验证,以确认该终端用户能否使用该移动存储设备。如果能够使用,则会开放相应的使用权限;否则,将完全拒绝使用,并在终端用户试图打开该移动存储设备时,向终端用户发出提示信息。

4 使用审批

管理员在安全策略中,授予终端用户在终端计算机上使用移动存储设备后,仍然需要通过手机短信等实时手段,对移动存储设备的每一次使用进行审核,确保每一次使用都是确因工作需要而进行的。在确保移动存储设备能够在终端计算机上由终端用户使用时,就需要终端用户输入本次使用原因,并通过手机短信等方式即时发给管理员进行审核,当且仅当审核通过之后,才能最终按照相应的权限使用移动存储设备。

不同的企业处在不同的发展阶段,并不是所有企业都需要如此细粒度的管控,因此,还需要系统能够灵活配置,允许管理员即时关闭使用审核这样的细粒度管控功能。

5 全程审计

从注册管理、到移动存储设备插入、再到移动存储设备的具体使用操作都需要留有详细的审计信息,以方便管理员在需要的时候查看审计记录,追溯安全事故责任人。

6 销毁处理

上面从移动存储设备的注册、接入到使用、审计,均为移动存储设备正常使用周期内的管控功能。当企业不再需要移动存储设备上存储的数据或移动存储设备本身时,如果不做任何特殊处理只是随意将其丢弃在一旁,可能会导致无意的数据泄露,给企业带来不可估量的损失。因此,作为对移动存储设备的全生命周期管理,最后的环节就是对其上存储的数据或者移动存储设备本身进行彻底的销毁,保证敏感数据不外泄,对整个管理过程形成闭环。

7 防止恶意代码传播

移动存储设备是恶意代码传播的主要手段之一,据安全公司McAfee发表的‘2010年第一季度威胁报告’称,一种通过移动存储设备传播的蠕虫病毒是对PC最大的威胁。一种与自动运行有关的感染是第一季度对PC的第三大威胁(参见图1)。因此,禁止自动运行是移动存储设备管理最基本的要求,通过禁止自动运行,有效降低企业内网感染恶意代码的风险。

本文基于移动存储设备使用带来的风险和管理的现状,阐述了对移动存储设备进行全面管控的过程中,需要执行的每一个管控环节,希望对各企业的移动存储设备管理提供借鉴。

报告 迈克菲威胁报告:2010 年第一季度

下面花点时间了解一下最“流行”的恶意软件。下面的列表显示了全世界消费者检测所报告的主要恶意软件。(此列表在世界上不同的地区往往不同,但本季度我们跟踪的所有地理区域都报告了相同的主要威胁。)

全球前 5 大恶意软件

1. Generic!Atr:一般可移动设备恶意软件
2. Generic.dx:一般下载程序和特洛伊木马
3. W32/Conficker.worm!inf:可移动设备 Conficker 蠕虫检测
4. 一般潜在有害程序:通用潜在有害程序
5. GameVance:匿名地收集统计数据的在线游戏软件

此前 5 大恶意软件与前几个季度的结果非常吻合。前 5 大恶意软件中的两种为自动运行恶意软件(甚至有一种使用 Conficker),而其他则为各种密码窃取特洛伊木马。我们往往将虚假安全产品通通检测为潜在有害程序,而 Internet Explorer 一直是网络犯罪分子最喜欢的攻击目标,从而导致我们感染操作 Aurora。

图1 迈克菲威胁报告,2010 年第一季度节选