企业级系统生命周期管理

链接到CSO零天攻击漏洞(Jan 10, 2013)

- 一个零天攻击安全漏洞可能感染到带有木马的PC。
- 目前对于此漏洞的唯一防护措施是禁用Java浏览插件。
- 面对成千上万台电脑，我们如何实现集中化的禁止这个漏洞??

客户遇到的挑战

- 零天攻击是不给客户及时响应立即感染的系统漏洞
- 现有的管理工具占用太多资源同时响应速度很慢
- 由于电脑数量众多，无法立即禁止
- 对他们的资产没有清晰的认识，因此无法管理

解决方案:

1. Patch Management Client Devices (D0HSRLL)
   - 对于数量众多(成千上万台)，跨平台，多操作系统和应用程序的补丁进行自动化管理，同时与被管理终端所处的地理位置和网络带宽连通性无关。
2. Core Protection Module Client Devices (D0JITLL)
   - 防护终端遭到病毒，特洛伊木马，蠕虫，间谍等恶意软件的攻击。
3. Lifecycle Management Starter Kit Client Device (D0PVNLL)
   - 资产发现
   - 软件分发
   - 补丁管理

TEM优势

- 最快的还是花系统管理工具来防止零天攻击(增长生产力!)
- 在业界最低资源占用(小于2%)的单一代理解决方案(减少使用资源!!)
- 单台管理服务器可以处理250K终端节点。(极低的软硬件构架=降低成本!!)
- 持续的合规检查(高安全性!!)
- 无需VPN即可实现对所有终端加密管理，只要终端一上Internet我们就可以管理. (管理便捷，任何时间，任何地点!!)

以下客户已经通过IBM解决方案获益:

Lenovo、Li &Fung、中国石化、四川烟草、湖南移动、交通银行香港分行、玉山银行、CLSA、ZTE, BEA、AIA, Praxair、南洋大学、现代汽车、招商地产，Walmart超市、Mattiott酒店、黄陵矿业、Intel、诺华制药等

如有相关问题可以咨询IBM服务热线: 800-810-1818转2378