Mayorista de Valor Agregado

Cómo establecer y controlar las políticas de uso de dispositivos personales

Memorias USB, MP3 Players, Agendas personales,
Cámaras fotográficas, Conexiones Wireless

Presentado por:
Juan Francisco Torres

safend
Securing Your Endpoints

Mayorista de Valor Agregado

Contenido de la charla

- Conceptos básicos y terminología
- Problemática
- Impacto en las empresas
- Impacto en el modelo de seguridad
- Tecnologías existentes
- Solución propuesta
- Conclusiones y recomendaciones

Mayorista de Valor Agregado

Conceptos básicos y terminología

Punto Final (End-Point)

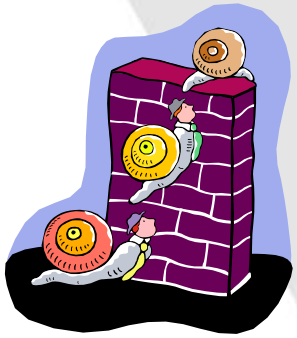
- En comunicaciones, es el último eslabón en la cadena de comunicaciones
- Corresponde a las estaciones de trabajo, portátiles y quioscos de la empresa.
- Tipos de dispositivos externos:
  - Puertos físicos (USB, Firewire, Serial, PCMCIA, etc.)
  - Puertos inalámbricos (WiFi, Bluetooth, IrDA)
  - Dispositivos de almacenamiento físicos y removibles (Ipod, CD/DVD)

Dispositivo externo

- Elemento conectado a un punto final a través de un puerto
- Tipos de dispositivos externos:
  - Reproductores
  - Cámaras
  - Agendas
  - Teléfonos inteligentes (Smart Phones)
  - Impresoras, Scanners, periféricos multifunción (scan/fax/print)
  - Discos portátiles y/o removibles
  - CD/DVD-RWs
  - Otros…..

Seguridad de punto final

- Concepto de Seguridad de Información que establece la responsabilidad de la seguridad directamente sobre el punto final o dispositivo.
- Tradicionalmente, los dispositivos como firewalls, servidores antivirus, IDS/IPS fueron los responsables de la seguridad en el punto final.
- Este concepto desplaza el manejo de la seguridad desde el perímetro hacia el punto final.



Mayorista de Valor Agregado

Problemática

Mayorista de Valor Agregado

Situación actual:

Dispositivos conectados a cada PC – Sin visibilidad, sin control

Equipo IT

Puntos Finales

Mayorista de Valor Agregado

La amenaza de los dispositivos

- Más de 26,000 productos USB diferentes, 700M vendidos en 2004
  - Dispositivos Almacenamiento
  - Adaptadores red
  - Impresoras, scanners, webcams
  - Cafeteras, luces, etc….
- Más de 2000 millones de dispositivos vendidos hoy
  - Más de 14 millones de iPods vendidos en 2005
  - Más de 5 millones de dispositivos Bluetooth vendidos por semana
  - Capacidad de almacenamiento en aumento – 10GB drive por $50 by 2010
  - Virtualmente imposible de seguir



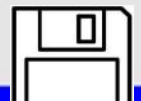

Entendiendo la amenaza

- 39% de los propietarios de discos USB los usan para transferir archivos entre el trabajo y el hogar
- “Robo de datos se estima en $50000M en perdidas [en 2004] en EU únicamente.” - The Economist (6/18/2005)
- “Seguridad de información deficiente expone información personal de mas de 50 millones de personas en 2005” -The Economist (6/18/2005)


Mayorista de Valor Agregado

Entendiendo la amenaza

- "**50%** de los incidentes de seguridad se originan desde dentro de la organización." – 2005 FBI / CSI Computer Crime and Security Survey
- "**70%** de las penetraciones de seguridad con pérdidas por **$100,000** son realizadas desde dentro de la organización." -- Vista Research
- Nuevas regulaciones obligan el control de datos en dispositivos removibles




Memorias Flash

Amenazas

- Fácil ingreso de dispositivos de alta capacidad y de reducido tamaño a las organizaciones
- Conveniente para usuarios no autorizados que copian grandes cantidades de información confidencial.
- Troyanos y otras aplicaciones destructivas pueden superar todas las estrategias de seguridad de las organizaciones
- Conexión de adaptadores alámbricos e inalámbricos entre redes crea puntos de acceso sin control
- PDAs y Teléfonos móviles crean puntos de salida potenciales en cada punto final

2006 - INCIDENTES RECIENTES

"Empleado de firma de auditoría olvida medio removible con información sensible de la compañía en un avión"

"Discos USB usados por el ejercito de EU en Afghanistan, con información confidencial - disponibles para la venta en el mercado de Kabul"

Mayorista de Valor Agregado

Impacto en las empresas

Riesgos asociados con los dispositivos

- **Fuga de datos**: Grandes cantidades de datos sensibles o de propiedad intelectual pueden salir por los puntos finales.
- **Infiltración**: Código malicioso como virus, gusanos y troyanos puede penetrar a través de los puntos finales.
- **Cumplimiento de normas**: Visibilidad, control y auditoría puede ser muy limitada, lo que genera no conformidades dentro de los modelos de gestión.

Por qué es importante la seguridad de punto final?

- **Amenaza interna**: El punto final es el más sensible, dado que en estos residen el 60% de los datos confidenciales (IDC).
- **Acceso de usuario autorizado**: Ni las soluciones centralizadas ni las políticas “en papel” mitigan el riesgo.
- **”Pérdida” u olvido**: Dispositivos removibles con información son fácilmente olvidados o expuestos.
- **Propiedad intelectual**: Pérdida a través de dispositivos común en casi 40% de las empresas.

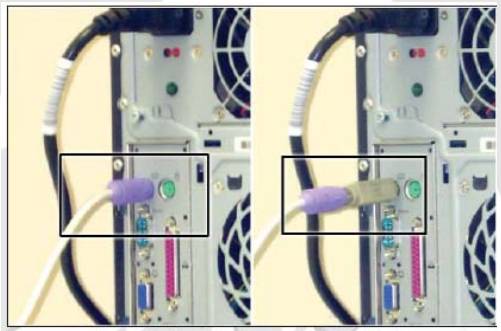


Figure 2: Before and after: a keylogger connected in between the keyboard and computer

Mayorista de Valor Agregado

Impacto en el modelo de seguridad

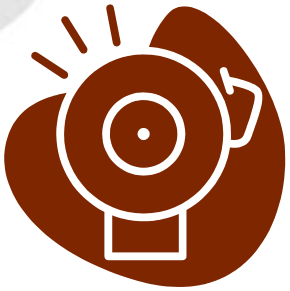
Mayorista de Valor Agregado

Propiedades del modelo de seguridad

- **Confidencialidad**: Los recursos del sistema sólo pueden ser accedidos por los elementos autorizados.
- **Integridad**: Los recursos del sistema sólo pueden ser modificados o alterados por los elementos autorizados.
- **Disponibilidad**: Los recursos del sistema deben permanecer accesibles a los elementos autorizados.

Variables afectadas

- **Confidencialidad**: Elementos no autorizados pueden conectarse al punto final para acceder a la información y extraerla.
- **Integridad**: Código externo puede afectar directamente cualquiera de los recursos del sistema.
- **Disponibilidad**: Cómo controlar el acceso a la información sin exponerla a riesgo, y contando con registros.



Se asume que:

- “En mi empresa no pasa nada”.
- Los usuarios no conocen lo suficiente para que esto sea un riesgo.
- Un control restrictivo limita el acceso a la información.
- La información no esta disponible, por lo que no se puede hacer seguimiento detallado.

Mayorista de Valor Agregado

Tecnología existente

Solución extrema

- Bloqueo del hardware de puertos físicos e inalámbricos
  - Equipos y portátiles actuales cuentan con puertos para facilitar el acceso a la información
  - Se requiere el acceso a ciertos dispositivos de operación normal (impresoras, scanners, cámaras, etc)

Versiones actualizadas de sistemas operativos

- Sistemas operativos como MS Windows XP cuentan con controles muy primitivos y locales (registro)
- No se encuentra integrado al software de control y administración de dominios.
- No permite manejo granular
- No cuenta con seguridad de alteración

Mayorista de Valor Agregado

Soluciones de software existentes

- Interfaz poco amigable con información compleja (ligada al registro del sistema operativo)
- Requieren período de escaneo y monitoreo continuado para presentar resultados
- Control genérico y estático
- Débil control sobre alteración
- Poca integración con herramientas centralizadas como Active Directory
- Complejo mecanismo de identificación de dispositivos y creación de reglas

Mayorista de Valor Agregado

Solución propuesta

Mayorista de Valor Agregado

Acerca de Safend

Seguridad de punto final innovadora - Simple, Productiva

- Permite **Visibilidad** y **Control** de los puntos finales de la empresa
- Protege contra la fuga de datos corporativos a través de:
  - Puertos físicos
  - Puertos inalámbricos
  - Medios removibles
- Alianzas con fabricantes de dispositivos y proveedores de seguridad

Mayorista de Valor Agregado

Con Safend

Visibilidad y Control granular

Equipo IT

Puntos Finales

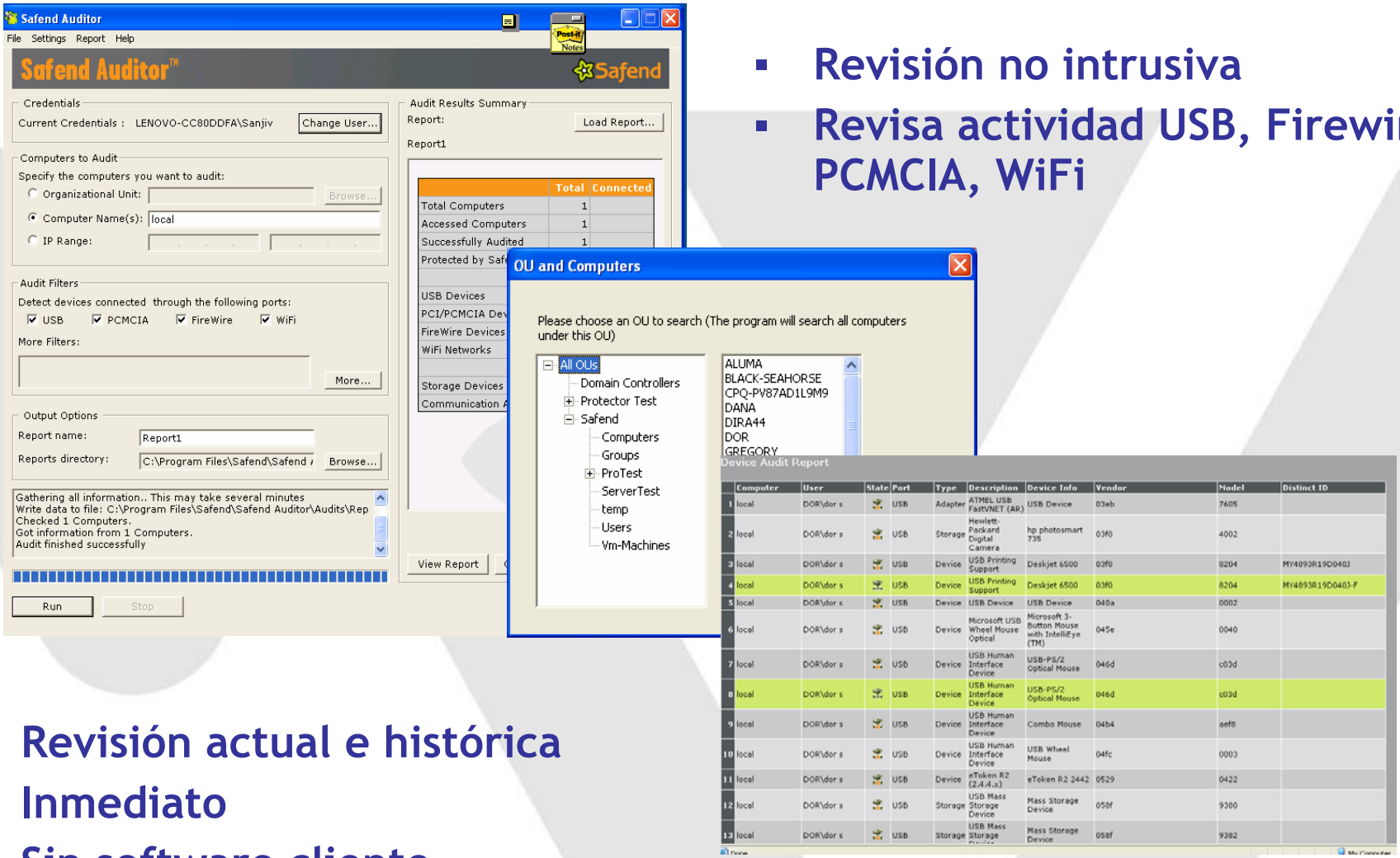
Visibilidad: Safend Auditor

Auditoría de seguridad para todos los puntos finales

- Audite la conexión de dispositivos a los puertos de comunicación
  - USB, Firewire, PCMCIA, Wi-Fi
- Proporciona información actual e históricas
- Sin clientes, uso inmediato, silencioso
- Revise los resultados para detectar los puntos débiles y los niveles de riesgo
- Fácil uso

Safend Auditor

Mayorista de Valor Agregado



- Revisión no intrusiva
- Revisa actividad USB, Firewire, PCMCIA, WiFi

- Revisión actual e histórica
- Inmediato
- Sin software cliente

www.mvaonline.com

Mayorista de Valor Agregado

Control: Safend Protector

Escudo de seguridad para los puntos finales

- Aplica políticas granulares a través de toda la organización
- Seguridad basada en análisis único de protocolos
- Resistente a alteración
- Administración centralizada, integrada con Active Directory
- Registro para análisis forense
- Interoperabilidad completa
- Fácil de usar y desplegar
- Bajo costo de uso

"Safend has done a great job with their anti-tampering counter measures"
- Kevin Mitnick, Renowned former hacker, and author

Mayorista de Valor Agregado

Control: Safend Protector

- Controle el uso de todos los puertos de comunicación física e inalámbrica de su punto final
- Apruebe el uso de dispositivos a través de todos los puertos basado en:
  - Tipo producto, Modelo, Número de Serie
- Controle el uso de todos los dispositivos de almacenamiento
  - Medios removibles;USB, FireWire, PCMCIA, SD, CD/DVD; Floppies; Tape drives
  - Permita conexión en modo Solo Lectura
- Recolecte registros forenses de todos los datos almacenados o leídos de un dispositivo de almacenamiento removible
- Controle el uso de WiFi, Bluetooth y IrDA

Safend Protector
El cliente

- Mínima interacción con los usuarios finales
- Instalación ‘silenciosa’
- Cliente ligero
- Driver de filtrado a nivel de Kernel
- Fuerte control de alteración
- Contraseña de suspensión

▪Un dispositivo permitido conectado al punto final

▪Un dispositivo no permitido conectado al punto final

Mayorista de Valor Agregado

Conclusiones y recomendaciones

Mayorista de Valor Agregado

Para tener en cuenta…

- Realizar un análisis detallado del uso e impacto de los dispositivos externos que son utilizados en los puntos finales de la empresa.
- Contar con una política de uso aceptable que tenga en cuenta el uso de los dispositivos externos para puntos finales, y alineada con la política de la compañía.
- Contar con herramientas que permitan realizar el monitoreo y control de los puertos en los puntos finales, de fácil administración.
- Deshabilitar el acceso a la BIOS de los puntos finales para evitar alteraciones.

Mayorista de Valor Agregado

Bibliografía

- www.yankeegroup.com
- www.vnunet.com
- en.wikipedia.org
- www.keyghost.com
- www.sharp-ideas.net/archives/2005/06/pod_slurping.html
- www.blackhat.com/presentations/bh-usa-05/BH_US_05-Barrall-Dewey.pdf
- www.eweek.com/article2/0,1759,1840131,00.asp
- www.safend.com

Gracias por su atención

Más información en www.mvaonline.com
Email: info@mvaonline.com

Lo esperamos en el área de Exhibición a las 6:00 PM