

Tomando el camino directo a la seguridad en la Tecnología de la Información

ING DiBa usa SecureWave para control centralmente todos sus puertos USB

Puertos USB y "Conectar y Usar" (P&P): ¡puede ser así de simple! Sólo enchufe un dispositivo y podrá comenzar a usarlo de inmediato. Es precisamente esta funcionalidad que causa frecuentes problemas a las compañías. Entre estos problemas sólo requerimos mencionar virus que se cuelan, pérdida de datos intencional o accidental y un uso personal. Después de todo P&P es sumamente conveniente para los usuarios y les permite instalar periféricos externos en cuestión de segundos. Esto incluye no sólo medios removibles sino también aquellos dispositivos que, por su diseño, contienen grandes cantidades de memoria. Periféricos tales como, por ejemplo, iPods, cámaras digitales y PDA que se usan inocentemente para copiar todo tipo de datos. La migración a Windows XP ha estado vinculada, para muchas compañías, a un cambio de actitud en los temas de seguridad y el uso de estas nuevas oportunidades. El grupo financiero ING DiBa reconoció esta necesidad a principios de 2005. Detlef Ebert del Centro de Tecnología Informática de Nuremberg decidió, después de intensivas pruebas, no prohibir totalmente el uso de estos dispositivos y optó por otorgar autorización específica a usuarios y dispositivos usando el programa Sanctuary[®] Device Control (SDC) de SecureWave. "Esto significa que las políticas de seguridad para cada uno de los departamentos puede implementarse centralmente, así como la ventaja de que se puede integrar rápidamente la última tecnología según se requiera," explicó Detlef Ebert.

La banca en directo ha disfrutado de un auge desde la aparición de las conexiones de Internet de alta velocidad. Ahora pueden lograrse tratos ventajosos aprovechando los consejos de la banca vía Internet, teléfono o correspondencia. ING DiBa tiene más de 40 años de experiencia en la banca directa, aunque sólo ha existido con ese nombre desde 2004. En 1965 BSV – Bank für Sparanlagen und Vermögensbildung AG – fue fundado en Frankfurt am Main. Después de un cambio importante de su línea a productos, tales como la incursión de la banca directa, la compañía cambio de nombre a "Allgemeine Deutsche Direktbank". En 2002 la compañía de finanzas holandesa ING adquirió DiBa y es en parte responsable de la fuerte posición actual del banco, con más de cuatro millones de clientes. Esta cifra incrementa constantemente gracias a una efectiva campaña de publicidad dirigida por Dirk Nowitzki y con el patrocinio de varios equipos de baloncesto. Por ejemplo, desde junio 2005 ING DiBa patrocina un equipo de baloncesto en silla de ruedas a través de la Asociación Alemana de Deportes de Silla de Ruedas.

Cuando menos significa más

Volviendo al tema de la Tecnología de la Informática, aparte de implementar centralmente las políticas de su equipo y programas en su oficina matriz, los administradores pueden también efectuar proyectos individuales según se requiera. Como resultado de una migración total a Windows XP, se requería una solución para gestionar los puertos USB en su mercado alemán. El Centro de Operaciones de TI decidió, después de informarse con la firma de consultoría TRYPTIS, basada en Munich, usar Sanctuary[®] Device Control de SecureWave. "El proceso

de implantación no duró mucho, nuestros colegas de TRYPTIS sólo requirieron unas cuantas horas de trabajo," agregó Detlef Ebert del Centro de Operaciones TI de ING DiBa. "Su estructura de implantación simple no resultó ser sólo una frase publicitaria, como lo pudimos constatar." El principal reto de este proyecto, por lo tanto, no fue el proceso de pasar a la práctica, sino su evaluación previa. En este caso los administradores involucrados deciden qué dispositivos se usarán en el futuro.

Creando una lista blanca

ING DiBa cuenta con un total de 2.600 licencias de Sanctuary® Device Control que cubren todas las estaciones de trabajo instaladas en sus sucursales alemanas de Frankfurt, Hanover y Nuremberg. El programa opera bajo el principio de "Lista Blanca". Esto significa que todos los dispositivos externos quedan bloqueados de forma predefinida y sólo se pueden usar después de realizar una autorización central al cliente involucrado. Esto se aplica a todas las conexiones de discos duros, CD-ROM, DVD y puertos seriales, paralelos y USB. ING DiBa tomó la decisión de sólo permitir el acceso a los puertos USB después de su autorización. Para ello, se crea una Lista de Control de Acceso (ACL) de cada dispositivo. Sólo el administrador puede conectar a los usuarios o grupos de usuarios con los periféricos por medio de una autorización de acceso.

"Nuestra decisión de adoptar la solución de SecureWave se basó en las numerosas opciones de control que ofrece el programa así como la facilidad de una autorización relacionada a los dispositivos para todos los empleados," comentó Detlef Ebert.

"Esto nos permite, por ejemplo, autorizar acceso a dispositivos especiales sólo para un grupo de usuarios." La funcionalidad se basa en una opción de cifrado. "Por el momento tenemos en uso cerca de 20 dispositivos diferentes, tales como periféricos BlackBerry, Palms o iPacks," añadió Detlef Ebert. Roger Wagner, Vicepresidente de Ventas y Mercadeo para la Europa Continental de SecureWave.

También observó: "Nuestra experiencia a lo largo de estos pocos años nos ha mostrado que esta característica es particularmente importante para los negocios, puesto que les permite abordar los requisitos individuales de cada empleado sin problemas."

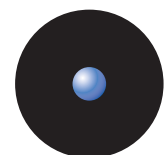
Honor al que honor merece

Windows XP es hoy en día el sistema operativo estándar usado en ING DiBa y el acceso a los dispositivos externos se gestiona centralmente. Desafortunadamente no es posible medir exactamente el nivel de éxito debido al uso de Sanctuary®, puesto que el daño sólo puede identificarse cuando hay un incidente serio. Sin embargo, un posible indicador surge del informe anual de seguridad de ING DiBa, donde el uso del programa está estableciendo un alto estándar, que se mantiene a lo largo de mucho tiempo.

Además de ello, se lleva a cabo una auditoría dos veces al año para verificar que todas las políticas legales relacionadas con la seguridad de la TI se cumplen. Un resultado positivo es que no se han identificado fallos. Por último, pero no por ello menos importante, su éxito se puede medir indirectamente por medio de la actividad del equipo de soporte técnico que, por el momento, ha tenido pocos problemas que resolver.

Se puede dar una respuesta rápida a las peticiones de uso de nuevos dispositivos puesto que una vez que se le otorga la autorización al administrador de sector, su firma digital se introduce en la lista de dispositivos permitidos. Así pues, ¿a dónde vamos en cuestión de seguridad en los puntos de acceso? Basándose en la retroalimentación positiva del uso del principio de "Lista Blanca" de SecureWave, en el futuro se continuará la autorización específica basándose en el usuario. El programa se actualiza continuamente con

la ayuda de TRIPTYS. Esto significa que la compañía puede controlar exactamente quien usa qué y cuándo. El punto importante para un banco que trata con información privada de sus clientes es que la misma, bajo ninguna circunstancia, llegue a las manos equivocadas. Esto puede garantizarse ahora y en el futuro.



SecureWave
Safeguarding Tomorrow

www.securewave.com
info@securewave.com