La necesidad de controlar los dispositivos en los ordenadores empresariales

La situación

Los ordenadores empresariales con Microsoft Windows no solamente no ofrece posibilidad de controlar de forma consistente (económico, fiable, flexible, alta granularidad, centralizado) los dispositivos que están conectados o se pueden conectar al ordenador, sino que con la tecnología Plug&Play se aumentan las posibilidades de proliferación de cualquier tipo de dispositivo descontrolado.

Los usuarios, en su mayoría, no son conscientes que cualquier herramienta o dispositivo de tratamiento de información digitalizada conlleva, aparte de la productividad, también una posible inseguridad y en algunos casos el riesgo de pérdidas económicas e intangibles (pérdida de confianza) es tan alto que puede superar en un múltiplo la productividad conseguida.

Existe tal cantidad de dispositivos y tecnologías que el propio usuario pierde el control. Muchas veces el usuario ni se percata que algo en su ordenador se ha puesto en marcha para comunicarse con algún dispositivo (WiFi, Bluetooth, Infrarojos ...).

Las amenazas

Las distintas tecnologías de intercomunicación, con las que muchos ordenadores están equipados de fabrica, pueden ser una puerta no controlada a nuestra red corporativa. Un ordenador portátil con un ratón Bluetooth deja completamente al descubierto la red empresarial, que tanto nos ha costado proteger con Firewall y otras protecciones perimetrales.

La posibilidad de copia concreta y/o masiva a dispositivos conectados a cualquier PC (discos de memoria USB, grabadores CD/DVD, discos duros externos SCSI o firewire, unidades ZIP/JAZZ/REV, cámaras digitales, reproductores MP3, ...) permite la proliferación de información empresarial de forma descontrolada. De la misma forma, vía éstos mismos dispositivos, también se pueden introducir virus y otro malware en la red empresarial.

Los módems analógicos y digitales, muchas veces quedan instalados y también olvidados, y así constituyen un riesgo de intrusión considerable, y/o una vía alternativa de comunicación a las establecidas por la empresa para usuarios no autorizados.

La solución

Con DeviceWatch® se puede controlar **todo** tipo de interfaces y dispositivos con una granularidad muy fina de forma centralizada. Las corporaciones de cualquier tamaño, pueden controlar todos los PCs con Windows 2000 o Windows XP Profesional de forma consistente y muy efectiva en costes, ya que DeviceWatch® se integra en la estructura actual (Directorio Activo) de la empresa. Adicionalmente, desde un punto de vista hardware, los administradores saben en cada momento qué dispositivos están conectados a qué ordenador, cómo se aplica la política de seguridad empresarial al ordenador, y qué hardware nuevo se está intentando conectar o usar.
En general, los permisos se asignan por usuario, y son los administradores actuales, los que asignan el derecho de uso de un dispositivo conectado a un PC, igual que dan ya derecho de uso de un directorio en la red a un usuario o grupo.
Mediante éste método, en un cliente de DeviceWatch®, un grupo asegurador alemán, un único administrador DeviceWatch® define la política de 80.000 puestos de trabajo, ya sean fijos o portátiles. Las herramientas adicionales como el escáner de hardware, la consola multipolítica y la posibilidad de logs centralizados, y la infraestructura ligera de DeviceWatch® sin puntos de fallo únicos, definen un marco novedoso para el control de hardware descentralizado con la facilidad y economía de control sobre recursos centralizados.

