Securización de equipos informáticos

Pablo García Pérez

Ingeniero de proyecto.
División Seguridad Lógica. Germinus XXI S.A

La securización (o bastionado) es el proceso mediante el cual se implementa una política de seguridad específica sobre una instalación de un sistema operativo. El bastionado de un equipo intenta reducir el nivel de exposición de un equipo y, por tanto, los riesgos y vulnerabilidades asociados a éste.

Como dice la norma ISO/IEC 17799, "la seguridad de la información se logra por la implementación de medidas de control, las cuales pueden ser políticas, prácticas, procedimientos, estructuras organizacionales y procedimientos del software. Estas medidas tienen que ser establecidas para asegurar que se logran objetivos específicos en la seguridad de la organización".

En este artículo vamos a centrarnos en la securización o bastionado de los equipos, es decir en los procedimientos, métodos, prácticas, etc., que nos permiten bastionar nuestros equipos. La securización es parte de la instalación de un equipo o un paso previo a poner un servicio en explotación.

Uno de los errores que se comete cuando se realiza la instalación de una nueva infraestructura informática es realizar las instalaciones de los equipos siguiendo las opciones por defecto de los fabricantes. Esto implica que no se instalarán ciertos componentes que puedan ser importantes para la seguridad, o que se dejarán ciertos componentes que supongan un mayor riesgo de seguridad. Si bien los fabricantes pueden proporcionar una configuración más o menos segura, una configuración así realizada implica un sistema operativo y unos servicios instalados que no tienen en cuenta la política de seguridad de la organización.

Esto constituye un alto riesgo; por un lado la política de seguridad que el fabricante del sistema operativo defina no tiene por qué coincidir con la de la organización (de hecho por regla general nunca lo hará); por otro, la función habitual para el que está definido el sistema informático que va a ser utilizado puede no coincidir con el que la organización quiere darle.

Las configuraciones por omisión de los fabricantes de sistemas suelen buscar el equilibrio entre funcionalidad, facilidad de uso y seguridad. Los fabricantes en raras ocasiones suelen decantarse por el de la seguridad. Asimismo, son precisamente estas configuraciones por omisión las primeras que tratarán de atacar los potenciales intrusos o sus herramientas automáticas. Es por tanto de la máxima importancia realizar configuraciones robustas de los sistemas, en especial cuando su grado de exposición a potenciales intrusos sea elevada (por ejemplo, estarán conectados o se comunicarán con Internet).

La securización de un equipo en un momento determinado, sin embargo, debe hacerse sin olvidar que el nivel de seguridad de un sistema no debe sólo mantenerse en un momento determinado sino que debe preservarse a lo largo de toda la vida útil de estos equipos. Es por tanto necesario realizar una revisión periódica del bastionado de los componentes e integrar esta función dentro de la política de seguridad, de forma que haya garantías de que los equipos están correctamente bastionados durante todo el tiempo en el que vayan a ser utilizados.

El proceso de securización supone un esfuerzo no desdeñable, por ello es importante saber cuando llevarlo a cabo. Ante la pregunta: ¿Cuándo resulta más conveniente realizar el bastionado de los equipos?, se pueden formular varias respuestas.

Generalmente, cuando va a ofrecerse un servicio sobre una determinada infraestructura, el servicio pasa por tres fases distintas: desarrollo, preproducción y producción. Durante la fase de desarrollo, lo habitual es que sea necesario que estén habilitadas muchas funcionalidades, facilidades, herramientas y aplicaciones que necesitan los desarrolladores para completar correctamente su tarea. Es posible que el bastionado de los equipos en esta fase supondría dificultar e incluso impedir la tarea a realizar.

En las dos siguientes fases (preproducción y producción), ya no se requieren todas estas funcionalidades, por lo que podría considerarse realizar la tarea de bastionado. La duda estriba en si realizarlo durante el paso de desarrollo a preproducción, o durante el paso de preproducción a producción. En el caso de realizar el bastionado en preproducción permite asegurar que el funcionamiento del servicio es correcto aún con el bastionado realizado. En cambio, de realizar esta tarea justo antes del paso de producción se puede dar el caso de que se descubra que existen incompatibilidades entre las tareas de bastionado y el servicio.

Sistema operativo	Recomendaciones de fabricantes
Debian GNU/Linux	http://www.debian.org/security/
FreeBSD	http://www.freebsd.org/security/
IRIX	http://www.sgi.com/support/security/advisories.html
Mandrake Linux	http://www.linux-mandrake.com/en/security/
Microsoft	http://www.microsoft.com/security/
	http://msdn.microsoft.com/security/
NetBSD	http://www.netbsd.org/Security/
OpenBSD	http://openbsd.org/errata.html
RedHat Linux	http://www.redhat.com/support/errata/
Slackware Linux	http://www.slackware.com/lists/archive/
Sun	http://sunsolve.sun.com/pub-cgi/secBulletin.pl
	http://www.sun.com/blueprints/browsesubject.html#security
SuSE Linux	http://www.suse.com/us/support/security/index.html
TurboLinux	http://www.turbolinux.com/security/

Tabla 1: Recomendaciones de seguridad proporcionadas por los fabricantes de sistemas operativos.

Pasos básicos de una securización.

Describimos a continuación de forma breve cuáles deben ser los pasos de una adecuada securización de los sistemas operativos de equipos informáticos:

1. Funcionalidad de los equipos y ubicación. Se debe definir claramente las funciones que van a realizar los equipos con el fin de saber qué servicios son necesarios ejecutar en ellos y determinar qué servicios no. La ubicación y el entorno de los equipos pueden hacer necesario incrementar el grado de protección del equipo, lo que a su vez modificará los requisitos de bastionado de dicho equipo.
2. Instalación de parches. Es necesario tener instalados los últimos parches ofrecidos por los fabricantes y distribuidores, tanto para el sistema operativo, como para todos los servicios y herramientas locales que se ejecuten en el equipo.
3. Acceso al sistema, autenticación y autorización. Sólo debe permitirse el acceso al sistema y los servicios que éste ofrece a los usuarios autorizados y además en las condiciones más seguras posibles, es decir utilizando servicios de acceso que usen cifrado (p. ej. instalando SSH en lugar de telnet en sistemas Unix), estableciendo las contraseñas que sean necesarias y controlando el acceso a los ficheros, servicios y aplicaciones, en especial a los más críticos.
4. Entorno y permisos del equipo. La definición del sistema de particiones y el sistema de ficheros en el sistema operativo de equipos informáticos es de gran importancia. Por ejemplo, estableciendo una estructura de particiones correcta y estableciendo la opción sólo lectura en las particiones que mantengan binarios.
5. Política de cortafuegos internos. Para determinados equipos con altos requisitos de seguridad puede ser necesario utilizar o instalar funciones de cortafuegos en el propio sistema operativo, que realice el filtrado de paquetes. Esto puede ser necesario en equipos situados en una red no protegida por un cortafuegos, o en el caso

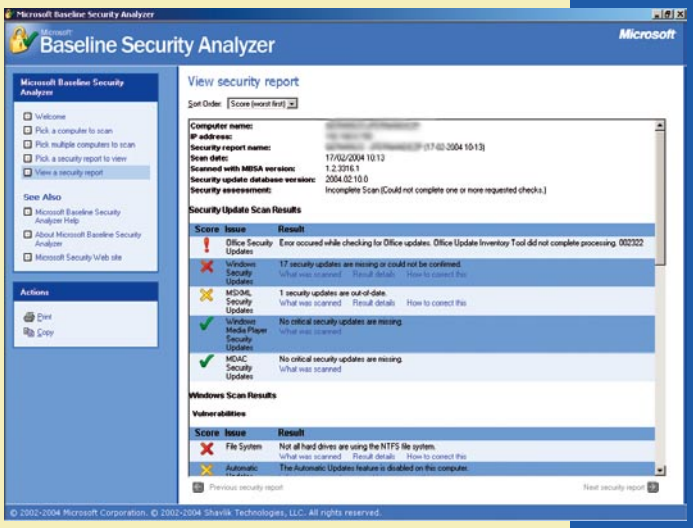

Ilustración 1: Informe generado por el MBSA

de equipos muy críticos en los que se desee añadir una protección adicional.

6. Establecer sistemas de auditoría y automatización de seguridad. Es conveniente seguir una política de seguridad que contemple tener habilitados sistemas automáticos de auditoría y seguridad, que nos permitan chequear nuestros sistemas de forma fácil y eficiente, detectando las posibles vulnerabilidades de los mismos, los ataques de los que hayamos sido objeto, actualizando las configuraciones según se añadan o cambien funcionalidades al equipo, etc.

Recomendaciones de los fabricantes

No hay que olvidar que los fabricantes de los distintos sistemas operativos nos ofrecen recomendaciones para el correcto bastionado de los equipos, recomendaciones que lógicamente conviene conocer y seguir si queremos que nuestros sistemas estén correctamente protegidos.

En la tabla adjunta se indica la localización de dichas recomendaciones, que incluyen gran cantidad de información sobre seguridad para los principales sistemas operativos disponibles.

Herramientas de securización

Existen infinidad de herramientas que pueden ser enormemente útiles para facilitarnos el bastionado de nuestros equipos, automatizando tareas que de otra forma serían extraordinariamente tediosas y que pueden llevar mucho tiempo.

Podemos encontrar herramientas de bastionado proporcionadas por los propios fabricantes de los sistemas operativos, que son de gran utilidad porque proporcionan un método rápido y probado para realizar tareas básicas de securización del sistema operativo y, en algunos casos, independientes de la política de seguridad.

✓**Para sistemas operativos Microsoft cabe destacar**

- MBSA: Microsoft Baseline Security Analyzer, desarrollado por Microsoft como parte del "Programa de estrategia de Protección Tecnológica". Tiene un interfaz de línea de comando y gráfico, con lo que es posible realizar un análisis de los sistemas Windows 2000, Windows XP y Windows Server 2003, determinando revisiones que faltan y vulnerabilidades de la seguridad tanto en el sistema operativo como en los servicios Internet Information Server (IIS), SQL Server, Internet Explorer (IE) y Office. También nos permitirá realizar búsquedas de actualizaciones de seguridad en multitud de productos.
- IIS Lockdown Tool, una herramienta de seguridad que facilita la protección de servidores web IIS4 e IIS5 permitiendo también proteger el sistema ante ataques externos contra el servidor web.

✓**Para sistemas UNIX:**

- Titan, una herramienta multi-plataforma, que bastiona Linux, FreeBSD, así como distintas versiones de Solaris. Está orientada hacia el administrador avanzado y dispone de una serie de perfiles predefinidos.
- Bastille. Una herramienta de bastionado automático para distribuciones de Linux (Debian, Mandrake, Red Hat, SuSE y TurboLinux), Mac OS X y HP-UX. Bastille intenta educar al administrador guiando el proceso de bastionado reali-

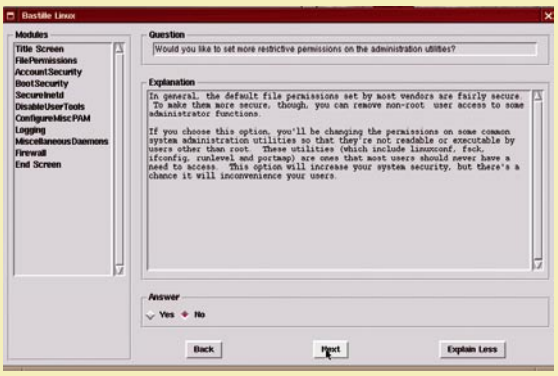

Ilustración 2: Bastionado de un equipo con Bastille

zando preguntas sobre el uso que se le va a dar al sistema e implementando el bastionado en función de las respuestas, aunque también dispone de una serie de perfiles predefinidos que pueden implementarse de forma automática.

- Jass (Solaris Security Toolkit). Una herramienta de bastionado automático para el sistema operativo Solaris que proporciona un mecanismo para facilitar el bastionado de los equipos durante el proceso de instalación.

Hay que añadir que este trabajo se puede complementar con herramientas de auditoría, algunas de las cuales se muestran en la tabla adjunta. Dentro de estas herramientas se encontrarán tanto herramientas de auditoría remota de equipos (a través de la red) como herramientas de auditoría local (ejecutada directamente en el sistema). En ambos casos las herramientas de auditoría revisarán el equipo y ayudarán a confirmar si el bastionado se ha realizado correctamente o no.

Conclusión

La securización es una tarea imprescindible dentro de la puesta en explotación de los sistemas informáticos; para llevarla a cabo los responsables de los equipos deben utilizar la política de seguridad definida por la organización e implementarla siguiendo las recomendaciones de seguridad de los fabricantes de los equipos y las herramientas automáticas que puedan estar disponibles para facilitar su tarea.

> *"El nivel de seguridad de un sistema debe presevarse a lo largo ded toda la vida útil del equipo"*

Conviene no olvidar que existen también versiones (o configuraciones) muy específicas proporcionadas por los fabricantes de los sistemas operativos genéricos que dispondrán de una certificación de seguridad concreta (Common Criteria, ITSEC...). Estas versiones (comúnmente denominadas 'Trusted') serán las que se deban utilizar en entornos en los que se requieran niveles muy elevados de seguridad. No suelen coincidir, ni en configuración ni a veces tampoco en algunos aspectos de diseño, con las versiones genéricas aunque puedan estar basadas en éstas. ❑

Tabla 2: Herramientas de bastionado y auditoría

Aplicación	Nombre	Tipo	URL
S.O. Microsoft Windows	MBSA	Bastionado/Auditoría	http://www.microsoft.com/spain/technet/seguridad/herramientas/mbsa.asp
	IIS Lockdown Tool	Bastionado	http://www.microsoft.com/spain/technet/seguridad/herramientas/iislock.asp
S.O UNIX	Titan(para Linux, Solaris, FreeBSD)	Bastionado/Auditoria	http://www.fish.com/security/titan.html
	Bastille (para Linux, HP-UX)	Bastionado	http://www.bastille-linux.org/
	Jass (para Solaris)	Bastionado	http://wwws.sun.com/software/security/jass/index.html
	Tiger	Auditoria	http://www.tigersecurity.org
Cualquier S.O.	ISS System Scanner	Auditoria local	http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_system.php
	ISS Internet Scanner	Auditoría remota	http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php
	Nessus	Auditoría remota	http:/www.nessus.org