Recomendaciones básicas de seguridad

acens
the hosting company

acens Technologies S.A.
San Rafael 14 - Pol. Ind. Alcobendas
28108 Madrid
902 90 10 20
www.acens.com

Recomendaciones básicas de seguridad

Introducción

Al igual que se producen avances en la tecnología aplicada a los servicios Internet, las técnicas de ataque orientadas a obtener acceso a los sistemas de información de forma no autorizada evolucionan y se adaptan a las características de este medio tan cambiante.

Debido al carácter internacional de la red y a la popularización del medio, en la gran mayoría de los casos el atacante desconoce a quien pertenecen los servidores, cual es su función o que tipo de información albergan. Esto provoca que los servidores conectados a Internet reciban multitud de intentos de acceso no autorizado provenientes de todas las partes del mundo, con el objetivo de utilizar los recursos de la máquina y realizar actividades ilícitas sin preocuparle quien es el propietario de dicho servidor o la información que éste albergue, provocando mal funcionamiento y/o pérdida de datos en los servidores y ocasionando que el servidor figure como origen de las actividades ilícitas realizadas.

En Internet se producen a diario multitud de intrusiones en sitios web, provocando en muchos casos el cambio de las páginas web (o defacement) y quedando el resultado visible para todos los internautas hasta que se restituyen los datos originales, incluso existen páginas de Internet que conservan el histórico de webs hackeados y el ranking de los hackers más activos, como por ejemplo en el sitio web: http://www.zone-h.org

En la mayoría de estos ataques la víctima no es escogida por su identidad o los contenidos de su web, sino porque se ha detectado que su web posee páginas, formularios o código vulnerable, empleando en muchos casos los buscadores de Internet para detectar que webs son vulnerables (Google Hacking).

Ilustración 1: Ranking de hackers en www.zone-h.org

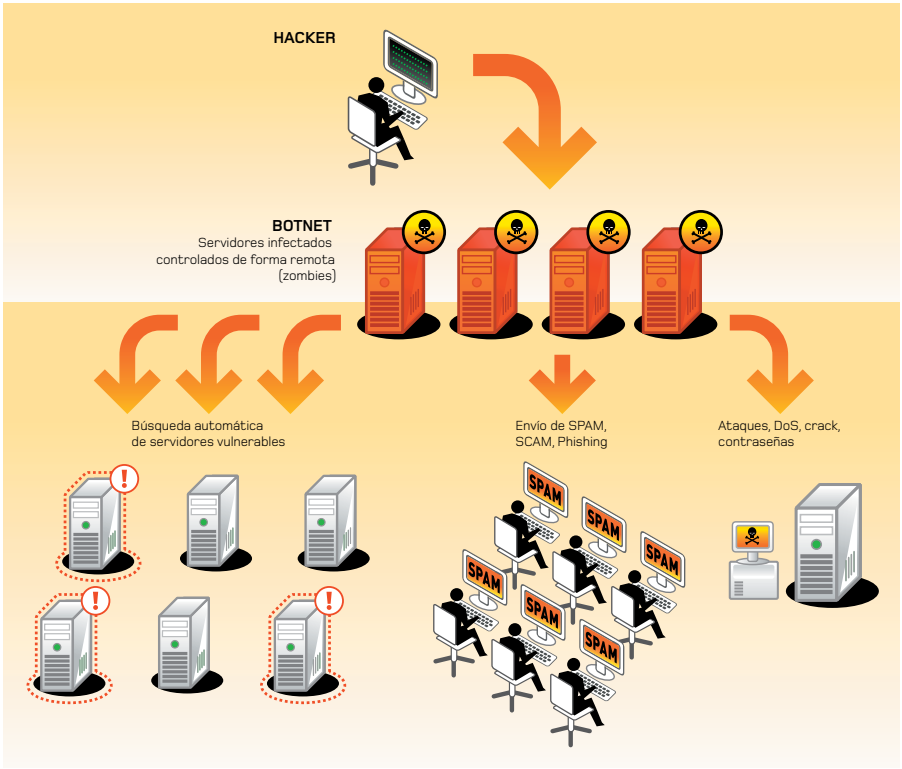

Ilustración 2: Redes de botnets realizan ataques y buscan nuevos servidores vulnerales

El más claro exponente de este tipo de hacking aleatorio son las denominadas botnets, redes de máquinas zombies que han proliferado en Internet sobre todo en los últimos dos años. Una máquina pasa a pertenecer a esas redes de zombies principalmente de dos formas: por tener una vulnerabilidad que es detectada y aprovechada de forma remota, o por la ejecución de un troyano por parte de uno de sus usuarios, formando redes de zombies son controladas normalmente por otro servidor master boot a través de canales IRC (Internet Relay Chat) y que son empleadas e incluso alquiladas con diferentes objetivos: realizar ataques DDoS, enviar SPAM (envío masivo de correo), phising (intentos de obtener credenciales por correo), y realizar barridos de forma automática para detectar nuevos servidores vulnerables a los que añadir a la botnet.

Debido a estos barridos masivos y automáticos el tiempo en que una máquina vulnerable conectada a la red pasa a ser comprometida ha disminuido de forma considerable en los últimos meses, y se hace necesario ajustar al máximo las medidas de seguridad así como reducir el número de servicios visibles a la red a aquellos imprescindibles para la funcionalidad deseada. Obviamente, un atacante se centrará más en los servidores que a priori le ofrecen más vías de entrada y descartará aquellos que parece que han sido configurados de forma expresa para ofrecer lo justo.

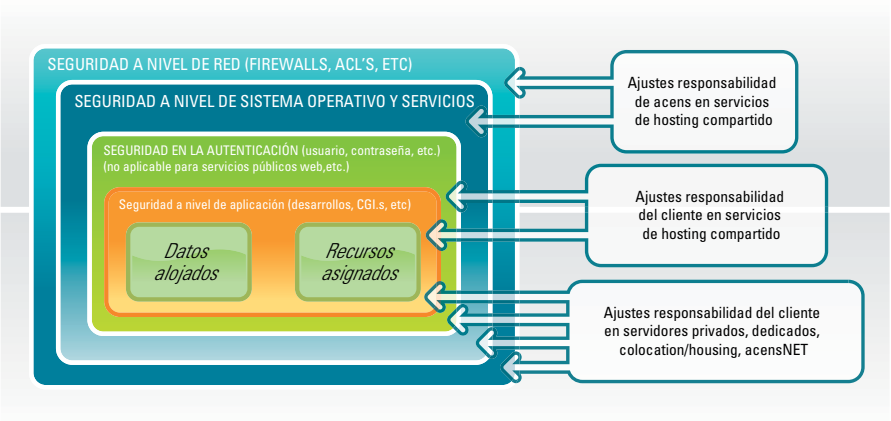

Ilustración 3: Simplificación de las capas de seguridad lógica a tener en cuenta

Su proveedor deberá proporcionarle unas medidas de seguridad que considera adecuadas para la mayoría de los casos y los propósitos generales para los que se emplean cada uno de sus servicios, desde el alojamiento compartido hasta el housing o colocation. No obstante tenga en cuenta que es su responsabilidad realizar una adecuada gestión de la utilización del servicio y de sus aplicaciones o datos, de tal forma que evite accesos no autorizados a su información o que terceros saquen provecho o realicen actividades ilegales desde los recursos que acens le ha asignado.

Los datos alojados o los recursos asociados a un servicio habrán de estar protegidos por diferentes capas de seguridad lógica, y en todas ellas hay que realizar los ajustes oportunos para evitar accesos no autorizados.

Principales causas de incidencias en materia de seguridad lógica detectadas por acens

Servicios de gestión no bloqueados en firewall	
Gestión incorrecta de contraseñas	
Desarrollos de páginas web inseguros	
Aplicaciones no parcheadas	
Windows	Unix
FTP anónimo con permisos de escritura	Cuentas correo o FTP con shell válido
Servicio telnet activado	Acceso directo como root con contraseña (telnet, ssh, webmin)

Tabla 1: Principales causas de las incidencias de seguridad

Seguridad a nivel de red: Bloqueo de servicios en firewall

El firewall o cortafuegos permite establecer un control de acceso basándose principalmente en la dirección IP origen de las peticiones dirigidas a su servidor. De esta forma se puede restringir la visibilidad de los servicios de una máquina conectada a Internet mostrando únicamente aquellos servicios públicamente accesibles y bloqueando los accesos a los servicios privados o de gestión. En Internet, debido al carácter mundial de la red y a los problemas ocasionados por las redes de máquinas infectadas descritas anteriormente, los servidores continuamente reciben intentos de acceso no autorizados de forma remota, en función de la configuración del firewall se pueden rechazar la mayoría, particularmente aquellos que provienen de redes no confiables.

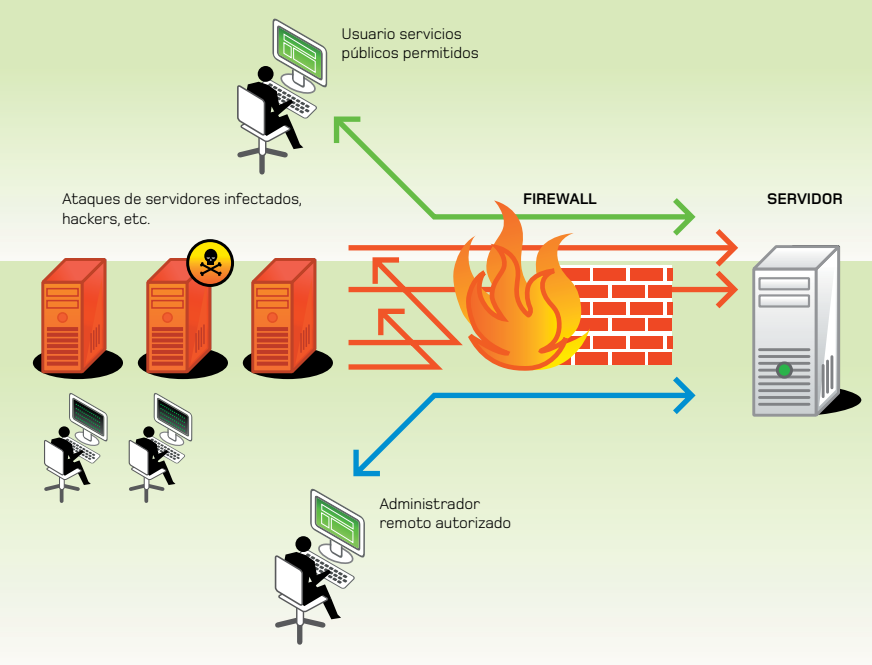

Ilustración 4: Filtrado de acceso mediante el firewall

En el caso de los servicios de alojamiento distintos al alojamiento compartido la recomendación principal consiste en bloquear los protocolos considerados de administración (Remote Desktop o Terminal Service, telnet, ssh, webmin, usermin y si es posible ftp) de tal forma que solo se pueda acceder desde las direcciones IP que normalmente empleen para la gestión, de esta forma conseguiremos que el resto de Internet solo vea los servicios que consideramos públicos (habitualmente Web).

Para determinar las redes desde las que permitir estos accesos de administración tenga en cuenta que:

- Si estos accesos de administración se realizan desde un único puesto de usuario con IP fija (p.e. ADSL con dirección IP fija), puede determinar su dirección IP en la siguiente dirección, teniendo en cuenta que si pasa por un proxy esa será la dirección IP a autorizar en los accesos a herramientas de gestión basadas en web: http://www.acens.com/comprobar_proxy.php

- Si los accesos de administración se realizan desde una red corporativa deberá proporcionar el rango IP completo desde el que quiere que se puedan alcanzar los protocolos de administración.

- Si se accede a esos protocolos de administración desde puestos que no tienen una dirección IP fija el nivel de seguridad se reduce considerablemente, puesto que serían visibles a todas las máquinas de Internet y se dependería en exclusiva de la robustez de las contraseñas tal y como se ha indicado en anteriores apartados. Es una situación no deseable y es muy aconsejable que intente delimitar los puestos o redes desde los que desea que sean visibles estos protocolos de gestión que dan acceso a funciones avanzadas de su servidor. En estas situaciones es al menos recomendable indicar un rango asociado al proveedor, para evitar los intentos de acceso no permitidos que se producen constantemente desde redes remotas.

En el caso de servidores con sistema operativo Windows es necesario el bloqueo de NetBios y protocolos asociados de Microsoft, puesto que son servicios que no deberían ser visibles desde Internet, y en el caso de redes de confianza únicamente si se van a utilizar funciones exclusivas de servidores Microsoft, tales como el acceso a carpetas compartidas por protocolo CIFS.
Aparte de los protocolos de administración hay otros servicios susceptibles de ser atacados y cuya política de bloqueo conviene revisar.

> "Es muy aconsejable que intente delimitar los puestos o redes desde los que desea que sean visibles estos protocolos de gestión que dan acceso a funciones avanzadas de su servidor"

Principalmente estamos hablando del acceso a bases de datos (mysql en unix, MS SQL en entornos Microsoft), de los que si es necesario su acceso externo hay que limitarlo a redes de confianza. Por otro lado, hay que revisar si se va a prestar servicio de DNS y/o correo (SMTP, POP3, IMAP, webmail) y bloquearlo en el firewall si el acceso no debe ser público.

Servicios	Carácter típico	Visibilidad recomendada
Web (http y https)	Acceso público	Bloquear en firewall si no se utiliza
Remote Desktop (Terminal Service) **SSH (Secure Shell)** **Telnet** **Webmin, usermin**	Acceso de administración y gestión	Permitir en firewall acceso EXCLUSIVAMENTE desde redes de confianza
FTP	Acceso de administración y gestión Publicación de contenidos	Si solo se utiliza desde redes fijas: Permitir solo desde estas redes en el firewall
Microsoft-NetBios, **Microsoft-RPC,** **Microsoft-SMB**	Acceso bloqueado	Bloquear totalmente en firewall Únicamente abrir a redes confiables si se emplearán servicios Microsoft como carpetas compartidas
Base de datos (MSSQL y Mysql)	Acceso restringido	Bloquear en firewall si no se utiliza En caso contrario bloquear en firewall accesos desde redes no confiables
Correo (SMTP, POP3, IMAP, webmail)	Acceso restringido	Bloquear en firewall si no se utiliza Si solo se utiliza desde redes fijas: Bloquear el resto en el firewall Si el acceso debe ser universal: gestionar correctamente contraseñas

Tabla 2: Servicios típicos presentes en los servidores y visibilidad recomendada

Seguridad en la autenticación: Gestión de usuarios y contraseñas

La principal recomendación, y la causa de la mayoría de las intrusiones no autorizadas en servidores, sigue siendo la elección de una contraseña débil. Desde la contraseña del panel de control hasta las empleadas en las posibles aplicaciones o CGI's que usted albergue en servidores de acens deben cumplir unas reglas básicas que la hagan difícilmente adivinable, tanto por personas como muy en especial por procesos automáticos que utilizan combinaciones basadas en palabras del diccionario y/o conmutaciones de números y letras.

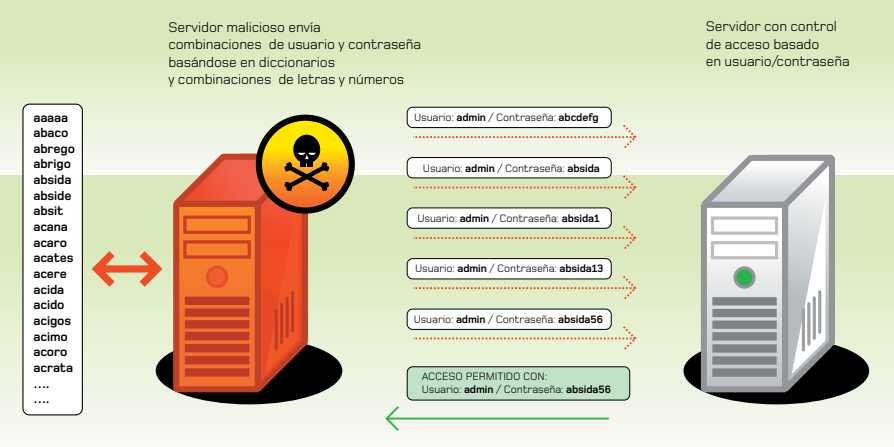

Ilustración 5: Ataques de diccionario y fuerza bruta para averiguar contraseña

Las recomendaciones en la elección de una buena contraseña son las siguientes:

- Nunca establezca una contraseña nula o que sea igual al nombre del usuario (p.e. usuario: prueba, contraseña: prueba), aunque se trate de un acceso temporal tenga en cuenta que continuamente se realizan intentos de acceso a toda máquina conectada a Internet.

- No escoja una palabra que figure en algún diccionario de cualquier idioma, en esos "barridos" realizados contra los servidores se emplean diccionarios para probar la coincidencia de la contraseña con cada una de las palabras.

- No escoja un nombre propio o el nombre de una localidad, suelen ser incluidos en los diccionarios como posibles contraseñas.

- No utilice secuencias de teclado, frases hechas o palabras que aunque no figuran en diccionario pertenecen al argot asociado a cierto ámbito (p.e. qwerty, 12345, noseque, foobar, devnull,homerun).

- No componga una contraseña realizando operaciones de sustitución o cambio de orden en las letras de una palabra de las categorías anteriores (p.e. sustituir la letra "i" por el número "1", la letra "o" por el número "0", invertir el nombre de las letras, añadir un simple número a una palabra, etc.), como puede imaginar las máquinas que están realizando pruebas para dar con la contraseña correcta realizan estas operaciones en cuanto han probado con todas las palabras, realizando todas las permutaciones y combinaciones posibles.

- Combine minúsculas, mayúsculas, números y símbolos en la contraseña, esto evita los ataques de diccionario y dificulta los ataques de "fuerza bruta", los símbolos deben ser "imprimibles" para evitar que se envíen comandos de control que puedan ser no aceptados por la aplicación de login.

- Establezca contraseñas de al menos 8 ó 10 caracteres de longitud, cuanto más longitud tenga la contraseña mayor será la dificultad en averiguarla.

> "Combine minúsculas, mayúsculas, números y símbolos en la contraseña, esto evita los ataques de diccionario y dificulta los ataques de 'fuerza bruta'"

Existen herramientas on-line para chequear la robustez de una contraseña, desde la página http://www.securitystats.com/tools/password.php se puede determinar el nivel de seguridad de una contraseña y se efectúan recomendaciones para mejorarla, aunque obviamente incluso desde la misma página se recomienda no introducir contraseñas que estemos empleando en sistemas en producción.

Conviene que los identificadores de usuario y las contraseñas correspondientes se asignen de forma individual, no siendo compartidas entre varias personas. Esta práctica recomendada es un requerimento para el cumplimiento de algunas normas e incluso a nivel legal si se están manejando ficheros de datos de carácter personal de nivel medio o superior, de forma que se pueda garantizar la identificación inequívoca y personalizada de cada usuario. Es importante que las credenciales individuales no sean proporcionadas a terceros en general, y en particular desconfíe si le solicitan por correo electrónico información sobre su identificador y contraseña.

Como última recomendación básica hay que recalcar la necesidad de que se anulen los accesos cuando ya no sean necesarios y se cambien las contraseñas activas de forma periódica, de tal forma que evitamos problemas con personal que las conozca aunque en la actualidad no deba (antiguos empleados y colaboradores, etc.) y dificultamos la labor de los robots que buscan combinaciones de usuario/password típicas. Si usted maneja ficheros con datos de carácter personal tendrá que modificar las contraseñas con la periodicidad estipulada en el documento de seguridad asociado al fichero declarado ante la Agencia de Protección de Datos.

> “Anule los accesos cuando ya no sean necesarios y cambie las contraseñas activas de forma periódica”

Gestión de usuarios y contraseñas	
Establecer contraseñas robustas	No nulas o igual al nombre de usuario
	No usar palabras que figuren en cualquier diccionario
	No usar nombres propios o ciudades
	No usar secuencias de teclado o argot
	No usar combinaciones o permutaciones de palabras
	Combinar mayúsculas, minúsculas, números y símbolos
	Longitud mayor a 8 ó 10 caracteres
Asignar identificadores y contraseñas de forma individual	
No proporcionar datos de acceso a terceros (especialmente si lo solicitan por email)	
Anular accesos de cuentas no empleadas	
Cambiar contraseñas de forma periódica	

Tabla 3: Resumen de recomendaciones en gestión de usuarios y contraseñas

Seguridad a nivel de aplicación: código web y software

Un error muy común es instalar aplicaciones web, ya sean comerciales o basadas en código abierto, y no realizar un seguimiento de las actualizaciones de seguridad, ni mucho menos la instalación de los parches que se van publicando en el tiempo. La gran mayoría de problemas de este tipo se están produciendo por no haber parcheado convenientemente foros basados en phpbb, y portales web basados en phpnuke y postnuke.

Si usted emplea este tipo de herramientas es conveniente que se suscriba a la lista de correo de anuncios correspondiente, donde se suelen enviar las notificaciones de la existencia de nuevas versiones y si solucionan algún problema de seguridad. Es conveniente que se visiten las páginas relativas a seguridad de cada herramienta, por ejemplo, para foros basados en phpbb: http://www.phpbb.com/security/, o que de forma periódica se revise si existe alguna nueva versión y si soluciona algún problema de seguridad.

Si usted tiene código propio, o desarrollado a medida para su caso, hay que tener en cuenta que se deben seguir una serie de recomendaciones de seguridad a la hora de programar. La mayoría de los problemas se deben a que no se chequea adecuadamente el formato de los parámetros de entrada de la aplicación o CGI, lo que da lugar a diferentes técnicas de ataque (Cross-Site Scripting, SQL Injection, etc.).

Hay que verificar que el dato de entrada se ajusta totalmente al formato y tipo esperado, siendo las recomendaciones generales en este punto las siguientes:

- Establecer los filtros necesarios para ver si cada uno de los parámetros tiene el formato y longitud esperada (p.e. si el parámetro tiene que estar compuesto por letras, por números, por ambos en un orden concreto, ver si supera el límite establecido para el valor esperado, etc.).

> “Un error muy común es **instalar aplicaciones web**, ya sean comerciales o basadas en código abierto, **y no realizar un seguimiento de las actualizaciones de seguridad**, ni mucho menos la instalación de los parches que se van publicando en el tiempo.”

- Eliminar caracteres incorrectos y/o “escaparlos”, prestando especial atención a eliminar si no son necesarios:

  o Espacios, comillas, dobles comillas, punto y coma, barras, etc. Eliminar estos caracteres pueden evitar ataques de SQL Injection si el parámetro se va a emplear para realizar una consulta SQL.

  o Saltos de línea, un error muy común consiste en no eliminar los saltos de línea que incluye uno de los parámetros pasados a la función de envío de correo (p.e. dirección email, asunto)

- Considerar el contexto y lo que vamos a hacer a continuación con esos datos para evitar uso indebido (p.e. No permitir insertar HTML en un campo de texto, no permitir la carga de contenidos de páginas remotas).

- Si se van a abrir ficheros en función de alguno de los parámetros de entrada conviene restringir el nivel de directorios a los que se va a acceder y chequear el parámetro de entrada para eliminar los caracteres que permitan acceder a otros directorios o ficheros.

Estas verificaciones se deben realizar en la aplicación o CGI que recibe los datos, no siendo suficiente realizar comprobaciones mediante Javascript, puesto que un usuario malintencionado puede enviar dichos datos directamente a la aplicación o CGI sin pasar por la página que realiza los chequeos mediante Javascript.

También es importante chequear cualquier código de error retornado por las funciones en las que se empleen de tal forma que se muestre una página »

Seguridad a nivel de aplicación: código web y software (cont.)

de error en lugar de continuar con la ejecución de acciones especificada en el código. Por ejemplo, si no se chequea el error a la hora de conectarse a una base de datos no se podrá detener la ejecución del CGI y los efectos pueden ser negativos.

Si la aplicación web o CGI se conecta a una base de datos es importante emplear un usuario con el mínimo privilegio posible, de solo lectura si se trata de una página que consulte información para mostrarla. En el caso de que sea necesario emplear un usuario de lectura/escritura en páginas concretas (p.e. para realizar inserción de datos) es conveniente no emplear el usuario super-administrador o SA.

En el caso de que la aplicación web, o una sección concreta, requiera autenticación o identificación mediante usuario y contraseña hay que cuidar que en todas las páginas afectadas se realiza la comprobación de identidad, puesto que un error muy común es realizar esa validación simplemente en la página de entrada.

Ya se trate de una aplicación propietaria, de terceros u opensource es necesario que las páginas correspondientes a las operaciones de administración estén protegidas y soliciten autenticación de usuario para permitir su acceso (p.e. gestión de contenidos, gestión de foros, gestión de aplicaciones, etc.).

Un error común en la gestión de los contenidos de la web consiste en dejar ficheros con información sensible bajo el directorio raiz de la web (docroot), estando por tanto disponibles para su descarga pública por web (p.e. ficheros access, ficheros zip o tar con backups, exportaciones de bases de datos, etc.), confiando en que como no están enlazados en el resto de las páginas y no se conoce la URL de acceso es poco posible que alguien los descargue. Lo que procede en estos casos es almacenar dichos ficheros por encima del docroot o en un directorio que requiera autenticación o identificación de acceso como los especificados en el párrafo anterior.

No es recomendable mantener versiones anteriores de las páginas en los directorios visibles por el web, pero si temporalmente hay que realizar una copia de la versión anterior conviene que al fichero no se le cambie la extensión, para evitar que terceros no autorizados puedan visualizar el código correspondiente (p.e. es incorrecto: pagina.asp.old, pagina.php.old; es correcto: pagina.old.asp, pagina,old.php).
Es necesario que el desarrollador conozca los posibles riesgos derivados de una incorrecta programación y sepa como evitarlos, como referencias en la web citaremos:

- Para tecnología Unix - PHP: http://phpsec.org/projects/guide/ y http://www.devshed.com/c/a/PHP/PHP-Security-Mistakes/

- Para tecnología Microsoft - ASP: http://msdn2.microsoft.com/en-us/library/ms998372.aspx

Código web, software y aplicaciones	
Software de terceros	Suscribirse a anuncios de nuevas versiones
	Parchear si aparecen bugs o fallos de seguridad
Software propio	Filtrar y chequear correctamente parámetros de entrada (no solo mediante javascript, en la propia aplicación)
	Comprobar códigos de error de las funciones
	Emplear usuarios con el mínimo privilegio
	Comprobación de identidad en todas las páginas restringidas
	Comprobar códigos de error de las funciones
Activar autenticación de usuario en páginas de administración y gestión	
No dejar ficheros con información sensible accesibles bajo docroot	
Renombrar versiones anteriores de las páginas con la extensión correspondiente	
Cambiar contraseñas de forma periódica	

Tabla 3: Resumen de recomendaciones en gestión de usuarios y contraseñas

Otros errores frecuentes en función del Sistema Operativo

En los servidores con sistema operativo Microsoft-Windows uno de los errores más comunes consiste en activar el servicio FTP anónimo con permisos de escritura, lo que ocasiona que personal no autorizado pueda descargar contenidos ilícitos en el servidor sin realizar ningún tipo de autenticación. Si tiene que prestar el servicio de FTP anónimo revise los permisos de la carpeta Raiz del servidor FTP para evitar que usuarios sin autenticar puedan grabar datos en su servidor. Si todo el acceso a su servidor FTP es mediante combinación de usuario y contraseña desactive la opción que permite conexiones anónimas ("Allow Anonymous Connections") en las propiedades del servidor. Si no es necesario ofrecer el servicio FTP de forma pública intente determinar las redes desde las cuales se podrá acceder para establecer las reglas de cortafuegos necesarias tal y como indicábamos en el párrafo anterior.

En los servidores Windows también es conveniente comprobar que el servicio telnet está desactivado, cuidando de que su "Startup Type" sea diferente a "Automatic" desde la consola de gestión de servicios de Microsoft Windows (Start -> Run… -> "services.mmc"). De esta forma se evitan intentos de acceso a través de este protocolo.

En los servidores con sistema operativo Unix un error muy frecuente consiste en crear cuentas de correo asociadas a cuentas de usuario del sistema operativo con un intérprete de comandos (shell) válido, lo que posibilita el login del usuario no solo por correo sino también por telnet y ssh. Si usted tiene un grupo de usuarios que solo deberían acceder por correo asegúrese de que tienen asignado un intérprete de comandos que no sea válido para acceso telnet, ssh o FTP (p.e. /bin/noshell). Lo anterior es también aplicable al acceso FTP, si usted cuenta con colaboradores que solo deberían acceder por FTP asegúrese de asignarles un shell no válido (p.e. /bin/false). En caso contrario para acceder a su servidor no sería un requisito conocer la contraseña del usuario root, sino que bastaría con averiguar la contraseña de uno de estos usuarios o colaboradores que en principio solo deberían acceder por correo o FTP, llevándonos de nuevo a plantearnos la importancia de la correcta gestión y elección de claves con la que iniciábamos las recomendaciones técnicas de este artículo y la necesidad de que las normas no sean únicamente cumplidas por los administradores del sistema sino por todos los usuarios que tienen acceso al mismo.

Por último, también en los servidores unix, conviene desactivar telnet y utilizar únicamente ssh para las labores de administración. Sobre todo si no se han delimitado en el firewall las redes de confianza a las que les estará permitida la gestión por ssh, conviene que se evite que el usuario root pueda intentar hacer login directo simplemente con una combinación de usuario y contraseña. Esto requiere tener un método alternativo de gestión (webmin, usermin) o un usuario sin privilegios desde el cual se pueda ejecutar "su" y se deberá comprobar que la línea de configuración "PermitRootLogin" del fichero sshd_config (normalmente en /etc/ssh/sshd_config) tiene la opción "without-password".

> "Si tiene que prestar el servicio de FTP anónimo revise los permisos de la carpeta Raiz del servidor FTP para evitar que usuarios sin autenticar puedan grabar datos en su servidor."

> "En los servidores **unix, conviene desactivar telnet y utilizar únicamente ssh** para las labores de administración"