¡Todo más fácil!

Edición especial de Symantec Website Security Solutions

Protección de sitios web

PARA

DUMMIES®

Aprende a:

- **Justificar la importancia de proteger un sitio web con argumentos empresariales sólidos**
- **Explicar por qué la tecnología SSL es la base de la protección de un sitio web**
- **Elegir e instalar los certificados SSL más adecuados en tu caso**
- **Adoptar las prácticas necesarias para que tu sitio web sea seguro e inspire confianza**

Protección de sitios web

PARA

DUMMIES®

WILEY

Protección de sitios web

PARA

DUMMIES®

Edición especial de
Symantec Website Security Solutions

WILEY

Protección de sitios web para Dummies®

Publicado por
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-08818-9 (pbk); 978-1-118-94831-6 (ebk)

Impreso y encuadernado en el Reino Unido por Page Bros Ltd., Norwich

10 9 8 7 6 5 4 3 2 1

Índice

Introducción

Protección de sitios web para dummies pretende aclarar qué riesgos supone un sitio web desprotegido, por qué es tan importante usar certificados SSL y en qué se diferencian unos certificados SSL de otros. En definitiva: queremos que aprendas a proteger mejor tu empresa y tus sitios web.

Información sobre este libro

Toda empresa que tenga un sitio web debe hacer lo posible por protegerlo, pero las medidas que debe adoptar dependen de sus exigencias y de las normativas que esté obligada a cumplir.

Para encontrar la información más útil en tu caso, no te hará falta leer el libro entero. Cada capítulo es independiente y puedes ir buscando información aquí y allá según te parezca.

A primera vista, la protección de sitios web puede parecer un tema complejo y hasta impenetrable, con un vocabulario técnico difícil de desentrañar. A lo largo de estas páginas, usaremos un lenguaje lo más claro posible para demostrar que no es así. Inevitablemente, tendremos que echar mano de algún tecnicismo, pero siempre te lo explicaremos, así que relájate y prepárate para convertirte en el experto de tu empresa en la materia.

A quién nos dirigimos

Tal vez nos equivoquemos, pero hemos escrito este libro pensando en un perfil de lector que:

- **Se ocupa de gestionar el sitio web de una empresa.**
- **No tiene por qué ser informático.** Quizá te dediques al marketing o dirijas una *startup*.
- **Tiene nociones básicas de informática.** Por ejemplo, seguro que sabes qué es un servidor y conoces bien los entresijos del comercio electrónico y otras transacciones web.

Cómo se organiza este libro

Protección de sitios web para dummies es un libro de referencia. No tienes por qué leerlo en un orden concreto, pero está estructurado de la manera más práctica posible.

En los dos primeros capítulos, se explica por qué toda empresa debería contar con un sitio web seguro. Si no tienes del todo claras las razones o necesitas hacérselas ver a tu jefe, empieza por aquí.

Los capítulos 3, 4, 5 y 6 se centran en los certificados SSL, que son la base de la seguridad de los sitios web. Veremos cómo funcionan, qué tipos existen, para qué sirve cada uno y cómo gestionarlos.

Los capítulos 7 y 8 describen otras prácticas recomendadas para conseguir que un sitio web sea seguro e inspire confianza a quienes lo visiten. Por decirlo de otro modo, estas serían las claves para tener un sitio web impoluto y cuidado con esmero.

En el último capítulo, te indicamos dónde obtener más información sobre temas específicos y qué organizaciones se ocupan de fomentar la protección de los sitios web.

Iconos utilizados

La información más útil del libro aparece indicada con estos iconos, para que te sea más fácil identificarla:

Los métodos de protección de sitios web y otra información práctica se señalan con este icono.

Así destacaremos lo que es importante que retengas (aspectos que no son opcionales, sino necesarios).

Si ves este icono, toma buena nota. Pasar por alto esta información podría tener consecuencias graves para tu sitio web o para tu empresa.

Este icono indica que la página va a llenarse de tecnicismos de un momento a otro y quizá prefieras apartar la vista o hacerte un café antes de seguir leyendo.

¿Y ahora qué?

Si quieres ir profundizando poco a poco en las distintas facetas de la protección de sitios web, empieza por el primer capítulo y ve leyendo los demás por orden. Si prefieres ir directamente a lo práctico, empieza por el tercer capítulo —en el que se explican los fundamentos básicos de la tecnología SSL— y continúa con el cuarto y el quinto, que te ayudarán a averiguar qué tipo de certificado SSL necesitas.

Por supuesto, también puedes hojear el libro para encontrar la información que te interesa o leértelo de cabo a rabo para no perder detalle.

Capítulo 1

Argumentos empresariales que justifican la importancia de proteger un sitio web

En este capítulo, aprenderás...

- Qué coste tiene la ignorancia
- Cuáles son los aspectos básicos de la protección de sitios web
- Por qué la seguridad resulta rentable

Cuando tienes que buscar un producto o servicio, ¿qué es lo primero que haces? Si has contestado «buscarlo en Google», se ve que estás muy en sintonía con los tiempos. Los clientes son personas informadas que no solo visitan tu sitio web para averiguar a qué te dedicas, sino también para saber quién eres y si eres de fiar, sobre todo si tienen pensado comprarte algo.

Tanto si tienes una tienda en Internet como si alquilas apartamentos de vacaciones o vendes productos financieros, tu sitio web es uno de los activos más importantes de tu empresa: un escaparate permanente que debe ser seguro y funcionar a la perfección.

¿Acaso dejarías el portátil desatendido en una cafetería o la puerta del almacén abierta de par en par? Pues proteger tu sitio web es igual de necesario.

En este capítulo, veremos los riesgos que entraña un sitio web desprotegido y hasta qué punto podrían afectar a tu empresa. También explicaremos por qué es tan necesario contar con un sitio web seguro, analizando las ventajas comerciales y económicas, y proporcionando argumentos de peso que te ayuden a justificar la inversión ante quien corresponda.

El coste de la ignorancia

Tal y como demuestran un sinfín de estudios y encuestas, los clientes insatisfechos se expresan en público mucho más a menudo que los satisfechos. Un cliente que vea una advertencia de seguridad al visitar tu sitio web —o que, aún peor, acabe con el ordenador infectado— se lo dirá a todos sus amigos y compañeros de trabajo. Si, además, opta por usar las redes sociales, sus quejas llegarán a oídos de mucha más gente y el daño podrá ser mucho mayor.

Tu reputación no es lo único que está en juego. Si tienes un sitio web de comercio electrónico mal protegido en el que se muestren avisos de seguridad, se abandonarán muchas cestas de la compra y perderás clientes.

Según un estudio de consumo en Internet realizado por Symantec y publicado en marzo de 2011, el 56 % de los encuestados acabarían comprando en el sitio web de un competidor si les apareciera una advertencia de seguridad, y solo el 11 % volvería después al sitio web original.

Qué tienes que perder

Un robo de datos o una infección con código dañino (*malware*) no solo dañaría tu imagen y disminuiría el volumen de ventas. En realidad, las repercusiones son mucho mayores.

Consecuencias económicas

La mayoría de los clientes necesitan algún tipo de indicador visual que les permita verificar que tu sitio web es seguro. De lo contrario, no confiarán en ti ni te comprarán nada. Si aparece un aviso de seguridad en el navegador, ni siquiera los menos precavidos te concederán el beneficio de la duda (en el capítulo 3, *Aspectos básicos de los certificados SSL*, se profundiza en este tipo de advertencias). Su interés desaparecerá de un plumazo y, con él, la posibilidad de que tus ingresos aumenten con sus compras.

Si, para más inri, tu sitio web acaba en las listas negras de los motores de búsqueda, será prácticamente como si no existiera. Según la página `http://www.google.com/intl/es-419/goodtoknow/protection/internet`, Google detecta a diario 10 000 sitios que no son seguros y los identifica como tales. Si corres esa suerte, nadie podrá encontrarte, y ni siquiera te repondrás del todo cuando te quiten de la lista negra porque tu posicionamiento en los motores de búsqueda habrá empeorado. Perder visitas significa perder dinero.

Si eres víctima de un robo de datos, es posible que te impongan sanciones o que tengas que ofrecer a tus clientes algún tipo de resarcimiento. Si sufres una infección grave, probablemente tengas que contratar a especialistas para solucionarlo. Todos estos contratiempos tienen un coste muy elevado, por no hablar del tiempo que pierden los empleados tratando de localizar el *malware*, buscando vulnerabilidades, renovando o comprando certificados SSL, investigando las pérdidas de datos y actualizando los sistemas y las contraseñas.

Según el documento *2012 Cost of Cyber Crime Study* del Ponemon Institute, patrocinado por Hewlett Packard y resumido aquí: `www.symantec.com/connect/blogs/cost-cybercrime-2012`, en 2012, el tiempo medio de recuperación tras un ciberataque fue de 24 días, lo que equivalía a una pérdida de 591 780 dólares. De no sufrir estos reveses, las empresas afectadas podrían haber dedicado el tiempo y el dinero perdidos a iniciativas de ventas o desarrollo mucho más provechosas.

Pérdida de fiabilidad y reputación

Alguien que vea una advertencia de seguridad en un navegador o escuche en las noticias que has sufrido un robo de datos o una infección con *malware* dejará de confiar en tu empresa de inmediato. Los consumidores están al tanto de los peligros de Internet y, ante la más leve sospecha de que no proteges sus datos como es debido, dejarán de hacer compras en tu sitio web.

Por ejemplo, si al conectarse ven una advertencia que indica que el certificado SSL ha caducado, pensarán que no te preocupas por la seguridad o que la empresa ha cerrado. En el mejor de los casos, sabrán que la organización no es tu punto fuerte. Si ni siquiera tienes al día los certificados SSL, es lógico que piensen que tu atención al cliente es igual de desastrosa.

Inclusión en las listas negras de los motores de búsqueda

Cuando un motor de búsqueda bloquea un sitio web, el problema puede tardar hasta seis semanas en resolverse. Hasta entonces, nadie podrá encontrar tus productos o servicios, por mucho empeño que hayas puesto en mejorar tu posicionamiento.

Aunque te libres de las listas negras, ten en cuenta que las advertencias de seguridad que aparecen en el navegador afectan al posicionamiento. Alguien que sospeche que el sitio web no es seguro lo abandonará de inmediato, y cuanta más gente haga lo mismo, peor posicionado estarás.

Incumplimiento de las normativas

Proteger un sitio web no siempre es opcional. Hay leyes y normativas que regulan el procesamiento de pagos, la recopilación de datos, su almacenamiento y otros procesos, e incumplirlas puede salirte muy caro.

En España, el incumplimiento de la ley orgánica de protección de datos (LOPD) puede suponer sanciones de hasta 600 000 euros en caso de infracciones graves, y el nuevo reglamento europeo que está ahora en trámite contempla sanciones millonarias.

Aunque la protección de datos es un tema muy amplio que excede el ámbito de este libro, hay ciertos aspectos relacionados con la seguridad de los sitios web que debes tener en cuenta. Conocer las normativas y tomar las medidas necesarias para cumplirlas es fundamental, ya que actuar a posteriori es mucho más complicado.

Directiva europea sobre protección de datos

La directiva europea sobre protección de datos abarca todo el ciclo de vida de los datos, desde que decides recopilarlos hasta que te deshaces de ellos. Por supuesto, esto afecta muy directamente a los propietarios de sitios web, que están obligados a adoptar las medidas técnicas y de organización adecuadas para evitar el tratamiento ilícito o no autorizado de los datos personales, su destrucción o su pérdida accidental y otros daños.

La definición de «adecuadas» depende del tipo de sitio web que tengas.

- **¿Tienes un blog sencillo o un sitio web con información básica?** Estos sitios web solo utilizan *cookies* sencillas para obtener datos anónimos a través de sistemas como Google Analytics. Son de acceso público y recopilan muy pocos datos personales (o no lo hacen en absoluto), por lo que sus propietarios tienen menos obligaciones que si recopilaran datos más detallados.
- **¿Tienes un sitio web dedicado a promocionar los productos de tu empresa?** Entonces seguro que usas técnicas de personalización avanzadas para crear perfiles de visitante que te permitan dirigir tus campañas de marketing a públicos concretos. Para recopilar estos datos, necesitas el consentimiento de sus propietarios. Cuanto más detallada sea la información que obtienes, mayores serán tus obligaciones y el riesgo de incumplirlas.

- **¿Tienes un sitio web financiado mediante anuncios?** Si es así, además de recopilar información sobre el perfil de quienes lo visitan, es posible que se la envíes a una red publicitaria externa para que optimice con ella las campañas. Recuerda que, dado que eres tú quien controla los datos, también eres responsable de cómo se almacena la información y del uso que se le da en la red publicitaria. Si el sitio web comparte información con redes sociales como Facebook, tus obligaciones serán similares.
- **¿Tienes un sitio web de comercio electrónico?** En ese caso, tendrás que almacenar direcciones, números de teléfono, datos de tarjeta de crédito y otra información financiera para procesar las transacciones de tus clientes. Aunque utilices un sistema de pago externo, tendrás que recopilar ciertos datos y hacer que los clientes inicien una sesión segura en el sitio web con su nombre de usuario y su contraseña. Las transacciones comerciales tienen un gran atractivo para los ciberdelincuentes, así que deberás extremar las medidas de seguridad.
- **¿Tienes un foro u otro sitio web en el que se publique información confidencial?** La directiva europea tiene una categoría especial («datos personales confidenciales») para los historiales médicos, los antecedentes penales, las afiliaciones religiosas y otra información que exige una protección especial. Si tu sitio web registra datos de este tipo, deberás tomar las medidas oportunas.

Obligación de cumplir la normativa de pagos con tarjeta en sitios web en los que se acepte este método de pago

Si aceptas pagos con tarjeta de crédito en tu sitio web, seguramente estás obligado a cumplir la normativa aplicable al sector de pagos con tarjeta. El *PCI Security Standards Council* es un foro abierto que establece los estándares de procesamiento de pagos con tarjeta de crédito en todo el mundo. Entre sus miembros se encuentran las cinco principales marcas de procesamiento de pagos: American Express, Discover Financial Services, JCB International, MasterCard y Visa Inc.

Según la normativa aplicable al sector de pagos con tarjeta (PCI-DSS, por sus siglas en inglés), quienes aceptan pagos de este tipo están obligados a evaluar si cumplen los estándares, a resolver las deficiencias detectadas y a informar de ello.

El procedimiento de evaluación consiste en identificar posibles deficiencias de seguridad en los procesos y tecnologías utilizados para transmitir, procesar o almacenar los datos de los titulares de las tarjetas. Por ejemplo, un sitio web de comercio electrónico tendría que

comprobar si presenta vulnerabilidades y si los datos que se transmiten al sistema de procesamiento de pagos se cifran debidamente. De hecho, la normativa sobre pagos con tarjeta en el marco del comercio electrónico exige el uso de certificados SSL durante la transmisión de datos de titulares de tarjetas, e incluso recomienda que todo el personal técnico esté capacitado para gestionar los productos de seguridad utilizados, entre los que se incluyen los certificados SSL. El texto de las recomendaciones (disponible solamente en inglés) puede consultarse aquí: www.pcisecuritystandards.org/security_standards/documents.php?document=dss_ecommerce_guidelines_v2.

También deben evaluarse los procesos utilizados (por ejemplo, los mecanismos de protección de las claves de cifrado, de los que hablaremos en el capítulo 6, *Gestión de los certificados SSL*).

Las fases de resolución y rendición de cuentas tienen por objeto demostrar que se han tomado las medidas de seguridad oportunas. Para garantizar el cumplimiento de las normativas a largo plazo, habrá que repetir continuamente este proceso y estar siempre alerta a las vulnerabilidades que puedan surgir.

Fundamentos de seguridad web

Para justificar lo necesario que es proteger el sitio web de una empresa no hace falta apabullar a nadie con tecnicismos; basta con argumentar bien las ventajas. En esta sección, veremos las dos razones fundamentales por las que los certificados SSL son una buena inversión. Así, te resultará muy fácil convencer a tu jefe o a quien se ocupe de tomar las decisiones en tu empresa.

Autenticación

Cuando una empresa adquiere un certificado SSL, debe validar su identidad mediante procedimientos más o menos rigurosos según el tipo de certificado (aspectos en los que profundizaremos en los próximos capítulos).

Cuanto más exhaustivo sea el método de validación, mayor será el número de indicadores visuales que se añaden al sitio web para garantizar que es seguro (por ejemplo, la barra de direcciones verde o el símbolo del candado).

La validación corre a cargo de la autoridad de certificación (la entidad externa que emite el certificado). Las mejores autoridades de certificación cuentan con una reputación excelente que hará que tus

clientes confíen en tu sitio web y piensen que es seguro. La confianza que transmite un certificado SSL es consecuencia de los procesos de comprobación y validación a los que se ha sometido.

Cifrado

Los certificados SSL cifran la información confidencial que se transmite a través de tu sitio web o entre servidores internos para que solo tú puedas acceder a ella. Así, los *hackers* no podrán interceptarla y les será imposible robar datos de tarjetas de crédito, nombres y direcciones de correo electrónico u otros datos, como la propiedad intelectual de tu empresa. Además, dado que los datos que circulan entre los servidores y los equipos se transmiten sin modificarse, tampoco se puede insertar código dañino en los mensajes ni en los propios datos.

Los certificados SSL protegen los datos, facilitan el cumplimiento de las normativas, mejoran tu reputación y aumentan las conversiones en el sitio web.

La seguridad es rentable

Bien utilizados, los certificados SSL te ayudarán a atraer más gente a tu sitio web, a potenciar el uso de las herramientas alojadas en él, a aumentar el número de conversiones y a vender más por Internet.

Cada certificado SSL ofrece diferentes indicativos a los clientes sobre cómo proteges sus datos e intentas ganarte su confianza. En el capítulo 3, *Aspectos básicos de los certificados SSL*, se explican las diferencias técnicas entre los distintos tipos, algunos de los cuales incluyen funciones y niveles de seguridad adicionales.

Dado que este capítulo se centra en los aspectos empresariales, veremos qué indicadores visuales de seguridad existen, qué pueden aportar a tu sitio web y por qué sirven para infundir confianza.

La confidencialidad tranquiliza

Los consumidores cada vez son más conscientes del valor que tienen sus datos para las empresas que los recopilan. No solo les preocupa el tratamiento que se da a sus números de tarjeta de crédito o direcciones de correo electrónico, sino también cómo se analizan sus hábitos (por ejemplo, qué términos buscan o en qué hacen clic).

Las noticias sobre espionaje y casos de *hacking* masivo han hecho que la confidencialidad se valore más que nunca.

Si tu sitio web utiliza la tecnología Always-On SSL (objeto del capítulo 5, titulado *El salto a la tecnología Always-On SSL*), quienes lo visiten verán siempre la indicación «https» en la barra de direcciones y sabrán que, desde que llegan hasta que se van, todas las interacciones con el sitio están cifradas. Esta información resulta muy tranquilizadora.

Además, los signos de seguridad SSL avanzada, como la barra de direcciones verde que se activa cuando un sitio web utiliza certificados SSL con Extended Validation, dejan claro que se ha comprobado la legitimidad de una empresa mediante procesos rigurosos. Si los utilizas, el cliente sabrá que tu empresa lo valora lo suficiente como para protegerlo.

Instrumentos para infundir confianza

La gente es desconfiada por naturaleza. Posiblemente la prudencia ayudara a nuestros ancestros a no morir devorados por leones. Hoy en día, nos lleva a investigar por Internet, a buscar información sobre productos y a dar por supuesto que un sitio que no conocemos podría ser peligroso.

Para combatir esta tendencia, los principales proveedores de software de seguridad han creado marcas de confianza que aparecen directamente en los resultados de las búsquedas.

Por ejemplo, si alguien que tenga instalado uno de estos programas de seguridad busca la palabra «bisutería» en un motor de búsqueda, verá una lista de resultados. Junto al nombre de los validados por una determinada autoridad de certificación se mostrará un símbolo que demuestra que son auténticos y, además, seguros (por ejemplo, una marca de validación como la que se muestra en la figura 1-1.).

Figura 1-1: Symantec Seal-in-Search

Si los internautas pueden verificar que un sitio web es seguro antes de hacer clic en él, sin correr riesgos, será más probable que lo visiten. Esto tiene varias ventajas, ya que además de aumentar el tráfico procedente de los resultados orgánicos de las búsquedas, mejora también el posicionamiento en los buscadores.

Marcas de confianza

Si has comprado un certificado SSL y has seguido las instrucciones de instalación, tu sitio web contará con una marca de confianza (un símbolo o logotipo que indica que una determinada autoridad de certificación le ha dado su aprobación y lo considera fiable).

Estos distintivos son un voto de confianza a favor de tu empresa y de tu sitio web, lo que incrementa el número de conversiones. En el caso de los sitios web de comercio electrónico, aumentan también los ingresos por cliente, según pruebas realizadas por ConversionIQ.

Otro aspecto importante es que no vale con colocar las marcas de confianza en cualquier parte. Si no se ven es como si no estuvieran, así que es conveniente que aparezcan en un lugar destacado y en el momento adecuado (por ejemplo, en las páginas de pago). También puede ser buena idea hacer pruebas comparativas, situándolas en distintos lugares para ver dónde obtienen los mejores resultados.

Indicadores de seguridad de Symantec

Symantec es un proveedor destacado de soluciones de seguridad en Internet y una autoridad de certificación de confianza. Entre los consumidores, suele conocerse con el nombre de Norton, pero los productos para empresas pertenecen a la marca Symantec.

Symantec protege más de un millón de servidores web en todo el mundo y, en 2013, el 91 % de las empresas de la lista Fortune 500 utilizaban sus certificados SSL (más información aquí: www.cpcstrategy.com/blog/2013/01/case-study-symantecs-norton-ssl-and-mcafee-secure-trust-marks-increase-new-visitor-conversion-rates/).

La compra de un certificado SSL de Symantec incluye también:

- el sello Norton Secured, el distintivo de confianza más conocido en Internet según un estudio internacional sobre consumo en Internet realizada por Symantec en noviembre de 2013 (datos internos de clientes de Symantec);
- la función Symantec Seal-in-Search, que muestra el sello Norton Secured junto a los resultados de las búsquedas en los navegadores compatibles y en los sitios web de los socios de Symantec.

Capítulo 2

Cómo reconocer las amenazas que podrían poner en peligro tu sitio web

En este capítulo, aprenderás...

- Quiénes corren más riesgo de sufrir un ciberataque
- A qué amenazas se enfrentan las empresas
- Por qué la autenticación es tan importante como el cifrado

Los ciberdelincuentes se aprovechan de la desinformación de sus víctimas, y lo cierto es que muy pocas empresas saben exactamente a qué riesgos se expone su sitio web. Si no conoces las vías ni los métodos de ataque, difícilmente podrás detectar una vulnerabilidad, por no hablar de resolverla.

Debido a este desconocimiento, un gran número de empresas corren un grave peligro. Según la edición de 2014 del informe de Symantec sobre las amenazas para la seguridad de los sitios web, en 2013 el 77 % de los sitios web legítimos presentaba vulnerabilidades peligrosas, y uno de cada ocho tenía una vulnerabilidad de carácter crítico, lo que pone de manifiesto la dejadez de sus propietarios.

En este capítulo, analizaremos las razones que pueden poner a tu empresa en el punto de mira de los ciberdelincuentes y los tipos de ataque más frecuentes. También veremos qué son los ataques *watering hole* o de abrevadero, cuya peligrosidad hace que autenticar tu empresa sea más importante que nunca.

Cómo evaluar el riesgo

Para determinar qué medidas de seguridad necesitas, empieza por pararte a pensar qué aspectos de tu empresa podrían interesar a los ciberdelincuentes.

En general, el riesgo depende de factores como los siguientes:

- **El tamaño de la empresa.** Ninguna empresa está a salvo, sea del tamaño que sea. Las grandes tienen una facturación elevada y enormes cantidades de datos de valor, pero suelen estar mejor protegidas. Las pequeñas, por su parte, también tienen datos valiosos, atraen a clientes con voluntad de gastar y se relacionan con proveedores o compradores más grandes y expuestos a ataques. Además, los sitios web de las pymes suelen estar más desprotegidos y son fáciles de atacar porque, con frecuencia, los usuarios acceden a ellos con una contraseña idéntica a la que utilizan en otros sitios web.
- **El tipo de información recopilado.** El botín favorito de los ciberdelincuentes son los datos de tarjetas de crédito, las direcciones postales y de correo electrónico y las pistas para el restablecimiento de contraseñas. Quienes se dedican al robo de identidades lo hacen para lucrarse. Cuanto más roban, más quieren, y lo que más les interesa son las tres cosas que suelen bastar para suplantar a otra persona: los datos que aparecen en su documento de identidad, la fecha de nacimiento y la dirección.
- **Lo conocido que es el sitio web.** Cuanto más tráfico tenga un sitio web, más interesará a los ciberdelincuentes para distribuir *malware* e instalarlo en el mayor número posible de equipos de un modo más fácil y rápido.
- **El tipo de visitantes.** Por ejemplo, es posible que un sitio web de B2B reciba visitas de clientes más grandes o más lucrativos. Si esta información llega a oídos de un ciberdelincuente, este tratará de aprovechar la situación.

Amenazas más frecuentes

Dado que cada amenaza debe combatirse de un modo distinto, un sitio web solo será totalmente seguro si incorpora varios niveles de protección.

Si tuvieras que proteger una casa, seguramente pondrías dos cerraduras en la puerta, pestillos en las ventanas y una alarma antirrobo. Con un sitio web ocurre lo mismo: hay que determinar qué puntos corren un mayor peligro y qué ataques tendrían peores consecuencias, para así diseñar un sistema de protección por niveles eficaz.

En la tabla 2-1, se enumeran algunas de las vulnerabilidades que los ciberdelincuentes aprovechan con más frecuencia para registrar pulsaciones de teclas, robar datos, distribuir *malware* o robar información y chantajear a la víctima.

Tabla 2-1 Factores que facilitan el ataque de sitios web desprotegidos

Vulnerabilidad	*En qué consiste*
Servidores sin actualizar con las últimas revisiones	Según el informe de Symantec sobre las amenazas para la seguridad en Internet (volumen 18), el número de ataques procedentes de sitios web infectados aumentó en un 30 % en 2012. Por lo general, las infecciones afectan a sitios web cuyos servidores presentan vulnerabilidades conocidas, pero casi todas tienen solución si se aplican las revisiones y actualizaciones pertinentes.
Accesos de personas no autorizadas	Si se utilizan contraseñas poco seguras, se revelan los nombres de usuario de los administradores o no se modifica la configuración predeterminada del hardware de red y de los programas de uso habitual, será fácil que alguien se haga pasar por un usuario legítimo para atacar los sistemas.
Ataques de secuencias de comandos entre sitios	Estos ataques (también conocidos como *cross-site scripting* y *XSS*) consisten en inyectar código procedente del sitio web del atacante en otro (el de la víctima). Esto permite a los *hackers* ejecutar su propio código en tu sitio web para atacar o infectar a los visitantes, o para engañarlos y lograr que revelen información valiosa (por ejemplo, contraseñas).
Ataques de fuerza bruta	Como su nombre indica, estos ataques consisten simplemente en probar todas las contraseñas y opciones de cifrado posibles hasta descubrir el código que permite acceder a tu sitio web.
Vulnerabilidades de día cero	Estas vulnerabilidades pasan inadvertidas hasta que alguien las aprovecha y lanza un ataque. Ese momento en que se descubre el riesgo se denomina «día cero». Según el informe de Symantec sobre las amenazas para la seguridad en Internet de 2014, en 2013 aumentó la frecuencia de este tipo de ataque y se descubrieron 23 nuevas vulnerabilidades de día cero.

Inspirar confianza resulta esencial

Hoy en día, demostrar que eres quien dices ser es más importante que nunca, ya que los ciberdelincuentes cada vez actúan con más frecuencia y ha aumentado la incidencia del *spear phishing* y de los ataques *watering hole*.

No todos los ataques *watering hole* son iguales, pero el principio en el que se basan es siempre el mismo. Tras elegir a las víctimas (por ejemplo, los empleados de una empresa), los *hackers* averiguan qué sitios web visitan y los infectan. Esto les permite propagar la infección cuando estas personas acceden al sitio. Protegerte del *hacking* es indispensable para que tus clientes no caigan en esta trampa.

Una de las técnicas diseñadas para atraer a las víctimas a los sitios web infectados —que a menudo son falsos— es el llamado *spear phishing*. Los atacantes recopilan información sobre su presa y la utilizan para invitarla a visitar un sitio web. Para ello, se sirven de diversos medios: mensajes de correo electrónico, contenidos publicados en las redes sociales y, en algunos casos, hasta llamadas telefónicas. A veces, los sitios web fraudulentos son falsificaciones muy logradas de otros legítimos. Por eso es fundamental que un sitio web esté debidamente autenticado para que quien lo visita sepa a quién pertenece.

Poder verificar la autenticidad de un sitio web es algo cada vez más importante tanto para las empresas como para los consumidores. Los certificados SSL (sobre todo los que incorporan la función Extended Validation, de los que hablaremos en el capítulo 4) indican a los internautas que tu sitio web no es una falsificación y que, además, se ha sometido a un proceso de autenticación externo.

Capítulo 3

Aspectos básicos de los certificados SSL

En este capítulo, aprenderás...

- Para qué sirven los certificados SSL y en qué se basa su funcionamiento
- Qué nivel de validación necesitas
- Qué autoridad de certificación te conviene elegir

Los certificados SSL (siglas de «Secure Sockets Layer») son la base de la protección de un sitio web, ya que se ocupan de cifrar los datos y demuestran que una entidad externa ha verificado la identidad de tu empresa.

En este capítulo, veremos cómo funcionan y qué uso deberías darles en tu sitio web. Esta información te ayudará a saber hasta qué punto necesitas esta tecnología y qué tipo de certificados se adaptan mejor a tus necesidades.

También te explicaremos cómo solicitar un certificado SSL básico y qué aspectos deberías tener en cuenta para elegir el que mejor te conviene.

¿Cómo protege tu sitio web la tecnología SSL?

Los certificados SSL no solo sirven para proteger sitios web de comercio electrónico. Lo cierto es que en cualquier sitio web, sea del tipo que sea, se intercambian datos y se interactúa de algún modo con las personas que lo visitan. Cada vez que alguien rellena un formulario de contacto, comenta una entrada de un blog, interactúa con una red social desde el sitio web o inicia sesión para conectarse a determinadas páginas o a una aplicación web, está dándose una interacción de este tipo.

Es lógico, por tanto, que todos los sitios web —y más aún los pertenecientes a una empresa— deban estar protegidos con un certificado SSL o con los que hagan falta.

El cifrado, paso a paso

Para entender cómo funciona la tecnología SSL, hay que tener claros los siguientes términos:

- **Navegador:** la aplicación con la que se accede a Internet (por ejemplo, Google Chrome, Microsoft Internet Explorer y Mozilla Firefox, aunque la lista es mucho más larga).
- **Servidor:** el motor gracias al cual funciona tu sitio web. Como posiblemente ya sepas, también hay otro tipo de servidores, pero en este contexto el término hace referencia al equipo o los equipos conectados a Internet en los que está alojado el sitio web.
- **Nombre de dominio:** el nombre que distingue a tu sitio web, tal y como está registrado. Por ejemplo, «google.com» es un dominio, y «google.es», otro distinto. La parte que sigue al punto (p. ej., «.org» o «.com») se denomina «dominio de nivel superior», mientras que el nombre que lo precede se denomina «dominio de segundo nivel» (p. ej., «Google» o «Facebook»).
- **Subdominio:** las empresas que ofrecen varios servicios pertenecientes a una misma marca suelen utilizar subdominios. Por ejemplo, «Maps.google.com» es un subdominio de «google.com». Los *hackers* suelen aprovechar esta circunstancia para engañar a sus víctimas. Por eso es habitual encontrarse con direcciones URL tipo «google.hackahz.com», que no guardan relación con «Google.com».
- **Claves criptográficas:** el cifrado SSL se basa en un par de claves criptográficas que cifran y descifran la información. Estas claves son indispensables en los sistemas de seguridad que utilizan una infraestructura de clave pública (PKI, por sus siglas en inglés).

Cuando alguien visita un sitio web protegido con un certificado SSL actualizado y de confianza, en cuestión de milésimas de segundo ocurre más o menos lo siguiente:

1. **El navegador del visitante intenta conectarse al sitio web protegido con el certificado.**
2. **El navegador solicita al servidor web que se identifique.**
3. **El servidor envía al navegador una copia del certificado SSL.**

4. **El navegador comprueba si el certificado SSL es fiable (para lo cual tiene en cuenta la fiabilidad de la autoridad de certificación que lo emitió).** Los navegadores más comunes saben automáticamente en quién confiar porque traen preinstalado un almacén raíz con raíces públicas de confianza vinculadas a autoridades de certificación aprobadas de antemano. Si el navegador confía en la autoridad de certificación, confiará también en el sitio web y enviará un mensaje de confirmación al servidor.

5. **El navegador también comprueba el estado del certificado para asegurarse de que no haya sido revocado.** Por lo general, lo hace mediante uno de estos dos recursos:

   - La lista de revocación de certificados (CRL), en la que figuran los números de serie de todos los certificados emitidos por una autoridad de certificación determinada que han sido revocados. La autoridad de certificación firma la lista para garantizar su autenticidad y evitar que sea manipulada.

   - El protocolo de estado de certificados en línea (OCSP), que consiste en enviar una petición de un certificado SSL determinado y recibir una respuesta que indica si el certificado es válido o ha sido revocado. La autoridad de certificación firma la respuesta OCSP para garantizar su autenticidad y evitar que sea manipulada. La mayoría de los navegadores utilizan este recurso.

   Un certificado puede revocarse por diversas razones, como que no se haya emitido conforme al procedimiento estándar, que el propietario haya publicado documentos falsos o que se hayan dejado expuestas claves privadas a consecuencia de un robo de datos.

6. **El servidor comunica la clave pública al navegador. Juntos, la utilizan para establecer otra clave, la clave de sesión, que servirá para crear un canal seguro y cifrado para el intercambio de información.**

7. **Una vez que se establece una conexión cifrada y segura, la dirección URL del sitio web aparece precedida del prefijo «https», en vez de «http» a secas.**

Este proceso, denominado *handshake SSL* o protocolo de enlace, se utiliza para que nadie robe ni intercepte la información que el sitio web transmite a los internautas (o viceversa).

Aparición de advertencias en el navegador

Para que el *handshake SSL* se realice correctamente, hace falta que el sitio tenga un certificado SSL actualizado que haya emitido una autoridad de certificación de confianza. Si no es así, el navegador interrumpirá el proceso y mostrará una advertencia.

Según el estudio *Alice in Warningland* realizado por Google y la Universidad de Berkeley (California), estas advertencias son motivo suficiente para que dos tercios de quienes las ven no visiten un sitio web, así que es importante evitarlas. El estudio (en inglés) puede consultarse aquí: `www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/akhawe`.

Cada navegador presenta las advertencias de distinta manera, pero todos suelen indicar por qué aparecen y preguntar al internauta si quiere ignorarlas y continuar. En la figura 3-1 se muestran algunos ejemplos.

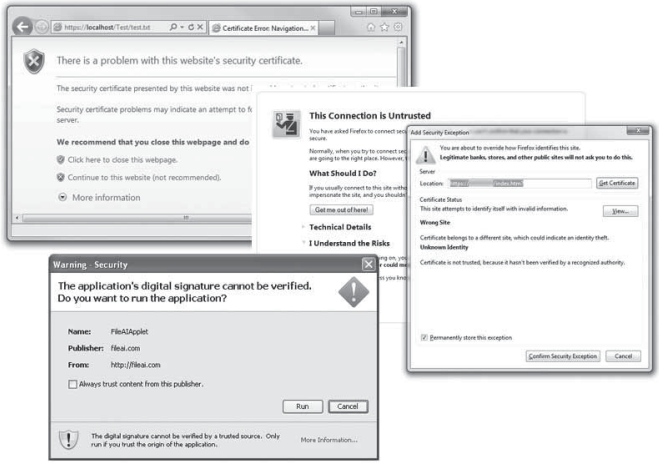

Figura 3-1: Advertencias que aparecen en distintos navegadores si un certificado SSL no es de confianza, no está actualizado o tiene un nombre de dominio que no coincide con el del sitio web al que se intenta acceder.

La verdad es que son bastante inquietantes. Por eso es importante hacer lo posible para que los que visiten tu sitio web no los vean nunca.

¿Cuántos certificados necesitas?

Depende. Es posible proteger varios nombres de dominio con un mismo certificado, pero en algunas circunstancias es necesario obtener un certificado para cada dominio. Los certificados SSL se basan en el llamado *nombre común* del sitio web, que es el nombre de *host* y de dominio. Si tu sitio web es accesible de varias maneras (p. ej., a través de las direcciones «www.ejemplo.com» y «ejemplo.com»), necesitarás un certificado SSL para cada vía de acceso. Si, además, tienes más de un servidor, posiblemente también necesites varios certificados.

Algunas autoridades de certificación ofrecen la posibilidad de adquirir certificados SSL que abarcan distintos subdominios. Se trata de los certificados Wildcard o comodín, que protegen todos los sitios web alojados en un mismo servidor (p. ej., «es.ejemplo.com» y «us.ejemplo.com», que tienen distintos subdominios pero el mismo dominio de nivel superior).

Cómo determinar el nivel de validación adecuado

Existen numerosos tipos de certificados SSL para distintos usos. Incluso dentro de los diseñados para proteger sitios web, hay también bastante variedad.

En el capítulo 4 hablaremos del más avanzado (el certificado con Extended Validation), pero esta sección está dedicada a los más sencillos: los certificados SSL con validación de dominio y con validación de la empresa.

Por qué los certificados con validación de dominio no son suficientes

Hay autoridades de certificación que emiten certificados con validación de dominio a quienquiera que figure como contacto administrativo del dominio en el registro WHOIS. Su procedimiento de verificación no es precisamente exhaustivo: se limita a enviar un mensaje de correo electrónico a la dirección de la persona de contacto.

La validación de dominio es el nivel de autenticación más bajo utilizado para la emisión de certificados.

Como te imaginarás, esto no es ningún obstáculo para un ciberdelincuente, que solo tendrá que conseguir una dirección de correo electrónico y comprar un nombre de dominio para salirse con la

suya. Alguien que tenga a BancoUno.com en el punto de mira podría registrar «banco1.com» y, a continuación, usar una dirección de una cuenta de correo electrónico web para obtener un certificado SSL con validación de dominio para el sitio web.

Muchos internautas son conscientes de estos peligros y, cuando visitan un sitio web, se fijan en si utiliza métodos de autenticación más avanzados, como los certificados con Extended Validation, que demuestran que el propietario ha superado un proceso de validación riguroso (en el capítulo 4 hablaremos de ellos en profundidad).

Requisitos para la obtención de certificados con validación de la empresa

La protección SSL con validación de la empresa (OV) ofrece bastantes más garantías que la validación de dominio. Además de comprobar a quién pertenece el nombre de dominio, la autoridad de certificación verifica la identidad de la empresa y la de la persona que solicita el certificado SSL.

Por ejemplo, el procedimiento podría incluir la validación del domicilio social de la empresa y del nombre de una determinada persona de contacto. Esta información se extrae del certificado y se muestra en la interfaz de usuario del navegador. La figura 3-2 muestra cómo aparece la información de un certificado SSL con validación de empresa.

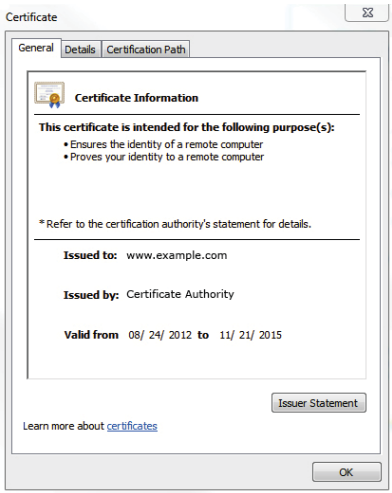

Figura 3-2: Información sobre un certificado SSL con validación de empresa (OV), tal y como se muestra en un navegador

Aspectos importantes a la hora de elegir una autoridad de certificación

No todas las autoridades de certificación que venden certificados SSL son iguales. Algunas tienen mejor reputación por tener procedimientos de autenticación más exhaustivos, gracias a los cuales los internautas confían más en sus certificados.

Antes de decantarte por una autoridad de certificación, hazte las siguientes preguntas:

- **¿Ha sufrido algún incidente de seguridad?** Un sitio web solo está a salvo si la autoridad de certificación que lo protege también lo está. Si, por ejemplo, se emiten certificados falsos a nombre de una autoridad de certificación que haya sufrido un ataque, la validez del certificado que usas en tu sitio web podría quedar en entredicho. Consulta el sitio web de la autoridad de certificación que tengas pensado elegir y trata de averiguar si ha sufrido algún incidente de seguridad grave u otro tipo de ataque.
- **¿Forma parte del CA/Browser Forum?** Se trata de un consorcio de autoridades de certificación y proveedores de navegadores de Internet. La afiliación es voluntaria, y sus miembros se ocupan de establecer los requisitos mínimos exigibles a distintos métodos de validación y cifrado. Hablaremos de él en el capítulo 9. Para ahorrarte preocupaciones, procura elegir una autoridad de certificación afiliada.
- **¿Quién más la utiliza?** Averigua cuántas empresas (y de qué tipo) usan sus certificados, y busca documentos en los que se analicen sus experiencias. Si entre sus clientes se encuentran grandes marcas, entidades bancarias o sectores sujetos a normativas muy estrictas, será más probable que sea fiable y te ofrezca más garantías de seguridad.
- **¿Cuánta información debes facilitar?** Cuanta más información te pida una autoridad de certificación, mejor. Si pone un gran empeño en validar tu identidad, sabrás que se toma en serio la seguridad en Internet, algo que sin duda valorarán tus clientes. También es recomendable comprobar si se somete a auditorías externas que evalúen sus procedimientos cada cierto tiempo y, en caso de detectar deficiencias, la obliguen a resolverlas. Por ejemplo, las prácticas de autenticación de Symantec se someten a auditorías anuales realizadas por KPMG.
- **¿Con cuántos navegadores son compatibles sus certificados?** Cuantos más navegadores reconozcan el certificado y lo consideren de confianza, más clientes potenciales verán que tu sitio web es seguro.

Algoritmos de cifrado

Un sitio web autenticado con un certificado SSL cifra los datos que transmite al servidor quien lo visita para que nadie intercepte la información confidencial.

El tipo de cifrado se basa en el algoritmo utilizado —que, a su vez depende del navegador, del servidor del sitio web y del propio certificado—. Cada certificado usa un algoritmo distinto, y no todos son igual de rápidos y eficaces.

El algoritmo de criptografía de curva elíptica (ECC), que utilizan algunos certificados SSL premium de un número reducido de autoridades de certificación, es uno de los más avanzados. Utiliza claves de cifrado más cortas que el algoritmo RSA, que se está quedando anticuado pese a que aún es el más habitual en el sector. Gracias a esta ventaja, el servidor puede ocuparse de un mayor número de conexiones cifradas a la vez sin agotar la capacidad de procesamiento, lo que también disminuye el gasto en refrigeración.

El algoritmo ECC también es más seguro. Por ejemplo, una clave ECC de 256 bits es 10 000 veces más difícil de descifrar que una clave RSA de 2048 bits. Quizá esto no te diga mucho, pero el matemático holandés Arjen Lenstra lo explica de un modo más gráfico: compara la capacidad de procesamiento utilizada para descifrar una clave criptográfica con la energía necesaria para hervir distintas cantidades de agua. Para descifrar una clave RSA de 228 bits, necesitaríamos una capacidad de procesamiento equivalente a la energía con la que herviríamos una cucharilla de agua. Para descifrar una clave EEC de 228 bits, tendríamos que poder hervir toda el agua del planeta.

Lenstra utiliza el término *seguridad global* para referirse a este fenómeno (consulta aquí el documento completo: http://eprint.iacr.org/2013/635.pdf o bien la explicación de este blog: `blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography`; en ambos casos, la información está en inglés).

Capítulo 4

Certificados SSL con Extended Validation

En este capítulo, aprenderás...

- En qué se diferencian los certificados SSL con Extended Validation de otros certificados
- Qué ventajas tienen los indicadores visuales y por qué son importantes para infundir confianza
- Qué información necesitas para solicitar un certificado con Extended Validation

Para los internautas, es muy importante poder reconocer que el sitio web en el que están no es un clon, sino el que de verdad pretenden visitar. El *phishing* es un fenómeno frecuente y hay gran cantidad de sitios web falsos que se hacen pasar por los auténticos para que el visitante facilite sus datos de inicio de sesión o información bancaria. Si la víctima cae en la trampa, los ciberdelincuentes le roban los datos.

Es lógico, por tanto, que los consumidores quieran cerciorarse de que están donde creen que están y de que están facilitando sus datos a quien corresponde. Los certificados con validación de la empresa (de los que ya hablamos en el capítulo 3) confirman una serie de datos básicos sobre el propietario de un sitio web, pero los certificados con Extended Validation (EV) exigen un proceso de autenticación de identidad mucho más riguroso.

En este capítulo, veremos por qué son una inversión rentable y qué hay que hacer para obtenerlos.

Por qué vale la pena usar certificados SSL con EV

Los sitios web autenticados mediante un certificado SSL con EV se distinguen a simple vista. Lo más habitual es que la barra de

direcciones del navegador aparezca de color verde, lo que indica que el propietario del sitio web ha facilitado información detallada sobre su empresa a una autoridad de certificación que ha comprobado su autenticidad.

Es un mecanismo sencillo, pero muy eficaz. Los sitios web protegidos con EV suelen obtener más clics y tasas de conversión más altas, así como un menor índice de abandono.

Marcas tan reconocidas como Twitter, HSBC y la herramienta de gestión de proyectos Basecamp utilizan este tipo de protección en sus sitios web.

Cuando más conocido sea tu sitio web y más confidencial sea la información que solicitas a quienes lo visitan, más podrá beneficiarse tu empresa de la tecnología SSL con EV.

Requisitos para obtener un certificado SSL con EV

El organismo que establece los requisitos para la emisión de certificados con EV es el CA/Browser Forum, un grupo de autoridades de certificación y proveedores de navegadores fundado para aprovechar al máximo las posibilidades de los certificados SSL y ofrecer más garantías de seguridad a los internautas.

En el capítulo 3 encontrarás más información sobre la labor que desempeña, pero si consultas su sitio web verás que los certificados con EV solo se conceden a empresas, organizaciones privadas y entidades gubernamentales. Básicamente, el solicitante tiene que estar reconocido oficialmente y haberse registrado con el procedimiento estándar en su país o en su zona.

Por ejemplo, una empresa legalmente constituida que figure en el Registro Mercantil no tendrá problema para obtener un certificado SSL con EV.

Es necesario aportar una gran cantidad de información, ya que a las exigencias del CA/Browser Forum suelen sumarse también las de la autoridad de certificación, que posiblemente tenga requisitos de autenticación adicionales. Tendrás que facilitar un nombre de contacto y un teléfono de empresa que coincidan con los del registro, ya que si la autoridad de certificación encuentra alguna discrepancia, se pondrá en contacto contigo para que corrijas el error (si es que es un error) o se negará a emitir el certificado si los datos no son idénticos.

Los pasos necesarios para obtener un certificado con EV pueden parecer engorrosos, pero son necesarios para que las autoridades de certificación demuestren que cumplen sus propios requisitos y los establecidos por el CA/Browser Forum. Por ejemplo, Symantec cuenta con un equipo dedicado enteramente a la autenticación EV que es independiente de los de ventas y asistencia. Además, utiliza métodos de registro y seguimiento detallados que permiten reconstruir cómo se respondió a una determinada investigación incluso años después.

El CA/Browser Forum

En 2005, un grupo de autoridades de certificación y proveedores de navegadores fundaron el CA/Browser Forum con la intención de aprovechar mejor las ventajas de los certificados SSL y ofrecer más garantías de seguridad a los internautas.

En junio de 2007, el CA/Browser Forum adoptó la versión 1.0 de las directrices para la emisión de certificados SSL con Extended Validation (EV). Los certificados con EV someten al propietario del dominio a un proceso de autenticación de identidad mucho más riguroso. Además, los sitios web protegidos con certificados de este tipo muestran información adicional sobre la identidad del propietario mediante colores, iconos u otros elementos.

El consorcio también ha adoptado los llamados «Requisitos de seguridad del sistema para redes y certificados», cuyo cumplimiento es obligatorio para todos los miembros y se comprueba mediante auditorías, además de exigirse a todas las autoridades de certificación que emitan certificados públicos de confianza.

Capítulo 5

El salto a la tecnología Always-On SSL

En este capítulo, aprenderás...

- Qué aspectos diferencian a la tecnología Always-On SSL
- Por qué puede beneficiarte adoptarla
- Qué pasos son necesarios para pasarse a la tecnología Always-On SSL sin empeorar el posicionamiento del sitio web en los motores de búsqueda

La mayoría de los sitios web utilizan el cifrado SSL en las páginas de inicio de sesión y de compra, en las que es más probable que se intercambien datos. Con otro tipo de interacciones no se utiliza el cifrado, lo que pone al visitante y al sitio web en peligro porque el nivel de seguridad no siempre es el mismo.

La tecnología Always-On SSL elimina este riesgo porque la comunicación estará cifrada desde que alguien llega al sitio web hasta que se va. Se trata de un método rentable que permite hacer búsquedas, compartir contenidos o comprar por Internet de forma más segura. Mientras naveguen por tu sitio web, los clientes verán siempre el símbolo del candado en el navegador, que indica que está utilizándose el cifrado SSL y que te preocupas por su seguridad y la de tu empresa.

En este capítulo, analizaremos los riesgos que supone utilizar un cifrado SSL intermitente y te explicaremos cómo adoptar la tecnología Always-On SSL del modo adecuado.

Aspectos que diferencian a la tecnología Always-On SSL

Los ciberdelincuentes pueden interceptar cualquier dato que se transmita entre el servidor web y el navegador. No solo roban contraseñas o números de tarjeta de crédito, sino que a veces también se hacen pasar por visitantes legítimos o tratan de obtener información con la que tal vez puedan adivinar contraseñas. Si adoptas la tecnología Always-On SSL, todas las comunicaciones estarán cifradas y será imposible interceptarlas.

Imagínate un caso como este: Alguien se conecta con sus datos de cliente a una tienda en Internet. La contraseña se cifra porque la página de inicio de sesión está protegida con un certificado SSL, pero la página que se abre a continuación no está protegida. En ese mismo momento, el servidor del sitio web envía una cookie al navegador (el código que usa el servidor para reconocer al cliente mientras navega de una página a otra). La cookie se envía sin cifrar, así que un *hacker* podría copiarla y usarla para hacerse pasar por el visitante.

Si lograra suplantar a un cliente que ya ha iniciado sesión, podría acceder a los datos de su cuenta y, si la víctima tiene una tarjeta de crédito asociada a la cuenta, quizá incluso pueda hacer compras con ella.

Además, cuando el usuario navega entre distintas páginas y algunas tienen una conexión segura y otras no, es posible que le aparezcan advertencias en el navegador similares a las mencionadas en el capítulo 3, lo que quizá le haga abandonar el sitio y dejar a medias las transacciones pendientes.

Con la tecnología Always-On SSL, los internautas siempre ven el prefijo «*https*» en la barra de direcciones mientras están en un sitio web y se sienten más seguros.

Consejos para una transición sin problemas

Si usas varios servidores para distintas secciones del sitio web, es posible que tengas que comprar más de un certificado. Además, es importante seguir el procedimiento de adopción estándar y no dejar ni una sola página sin cifrar, ya que hacerlo podría empeorar el funcionamiento del sitio web y su posicionamiento en los motores de búsqueda.

Normalmente, la autoridad de certificación a la que compres un producto con tecnología Always-On SSL te dirá qué tienes que hacer, pero a continuación resumimos los aspectos básicos que hay que tener en cuenta.

Redireccionamiento

Si decides utilizar la tecnología Always-On SSL, todo tu sitio web pasará a utilizar el protocolo *https*, un proceso similar a cambiar de dominio. Tendrás que redireccionar todas las páginas a su equivalente «https», además de registrar por separado la versión https del sitio web en las herramientas para *webmasters* de Google (de las que hablaremos en el capítulo 8).

Velocidad de carga

Usar el cifrado en todas las páginas exige una potencia de procesamiento algo mayor, así que es conveniente evaluar la infraestructura del servidor web. Lo más probable es que el efecto sea mínimo, y sería muy raro que una pequeña disminución en la velocidad de carga afectara al posicionamiento del sitio web en los buscadores, pero es mejor asegurarse de que todo está en orden.

Conexiones desprotegidas

Todos los enlaces e interconexiones de tu sitio web tienen que estar conectados entre sí de forma segura. Asegúrate de que no hay ninguna conexión desprotegida al servidor web y, si la hubiera, desactívala. Es fundamental que, cuando alguien navega por tu sitio web, la sesión esté siempre cifrada, independientemente de las páginas que abra o de dónde haga clic.

Lo último en seguridad

Tanto las autoridades de certificación como los matemáticos buscan constantemente maneras de mejorar el cifrado SSL para poner más trabas a los *hackers* y reducir los riesgos si alguien se infiltra en una sesión cifrada. Un certificado SSL establece una conexión segura y cifrada (recuerda el capítulo 3), pero ya están surgiendo otras tecnologías muy prometedoras.

La novedad más interesante, que ya utilizan empresas tan conocidas como Twitter y Google, se conoce con el nombre de *Perfect Forward Secrecy* (PFS). Con este sistema, el par de claves criptográficas que se crea al instalar un certificado SSL no se usa para cifrar los datos, sino para crear otras claves de forma segura. Estas nuevas claves, que son específicas de cada sesión, no se transmiten nunca del navegador al servidor o viceversa, lo que impide interceptarlas mediante un ataque de interposición *man-in-the-middle* (la técnica utilizada para espiar este tipo de comunicaciones).

Cada vez que alguien inicia una sesión nueva en un sitio web, esta se cifra con distintas claves. De este modo, si un *hacker* logra infiltrarse en una sesión, no podrá acceder a ninguna otra, y si roba las claves privadas del certificado, tampoco podrá descifrar los datos que haya podido registrar y almacenar.

Capítulo 6

Cómo gestionar los certificados SSL

En este capítulo, aprenderás...

- Quién debe ocuparse de la protección de sitios web y qué procedimientos conviene establecer
- Qué programas y herramientas de automatización podrían facilitarte el trabajo
- Lo importante que es proteger las claves de cifrado

Todos los certificados SSL, sean del tipo se sean, tienen que renovarse de forma periódica. La frecuencia depende de la autoridad de certificación y del paquete adquirido, pero el periodo de validez de los certificados suele oscilar entre uno y tres años.

El problema es que, a medida que una empresa crece, va adquiriendo certificados poco a poco y es difícil saber quién compró cada uno, cuándo y a quién. Si, además, alguien se olvida de renovar un certificado, las consecuencias serán aún más graves porque el navegador mostrará una advertencia de seguridad en las páginas que debería proteger (tal y como se muestra en la figura 3-1).

Estas advertencias hacen mella en la confianza de los consumidores y, por consiguiente, en las ventas. De hecho, según un estudio de consumo en Internet realizado por Symantec y publicado en marzo de 2011, el 91 % de los encuestados abandonarían una transacción si el navegador mostrara una advertencia que indique que la conexión no es segura.

En una empresa que no sistematice la gestión de certificados reinará el descontrol. Los empleados solicitarán certificados para sus proyectos y no tendrán en cuenta la reputación de la autoridad de certificación ni el tipo de certificado más adecuado para toda la empresa, con lo cual es probable que acaben utilizándose *certificados de origen dudoso*.

Los certificados SSL de origen dudoso no han sido emitidos por ninguna autoridad de certificación de confianza. Esta definición engloba los certificados autofirmados y aquellos emitidos por autoridades de certificación que no cumplen los requisitos del CA/Browser Forum u otros requisitos necesarios para satisfacer la normativa de protección de datos o la aplicable a los pagos con tarjeta (analizados en el capítulo 1, *Argumentos empresariales que justifican la importancia de proteger un sitio web*).

Cuando alguien visita un sitio web protegido con este tipo de certificado, aparece una advertencia en el navegador similar a la que se vería si el certificado estuviera caducado, ya que el nivel de autenticación y protección no es el mismo que el de un certificado emitido por una autoridad de certificación de confianza.

En este capítulo, te ayudaremos a conseguir que todos los certificados SSL que utilice tu empresa estén al día, hayan sido emitidos por una autoridad de certificación aprobada de antemano y se gestionen de forma segura.

Procedimientos de control

Una empresa que quiera gestionar bien sus certificados SSL tendrá que establecer los procedimientos oportunos. Cuanta más gente intervenga en las tareas relacionadas con la protección de un sitio web, mayor será el riesgo de que alguien olvide algo, se pierda información o se produzca un incidente de seguridad.

Designación de responsables

Centraliza la gestión de los certificados SSL y designa a alguien que se ocupe de ella. En empresas grandes, es posible que no baste con una persona, pero es importante que el equipo de gestión sea lo más reducido posible y que siempre haya alguien que supervise a los demás.

De este modo, sabrás quiénes tienen autorización para comprar y renovar certificados, y podrás controlar si conocen y respetan los procedimientos estándar. Sin embargo, que solo haya una persona responsable de controlar todos los certificados SSL es un riesgo, basta con que la persona se vaya de vacaciones para que un certificado no se renueve a tiempo.

Traspaso de responsabilidades

Una de las razones más frecuentes por las que caducan los certificados SSL es que la persona encargada de renovarlos se ha ido de la empresa o ha cambiado de departamento. Aunque el riesgo es menor si se adopta una gestión centralizada, aun así hace falta definir un protocolo de cesión de responsabilidades que se siga cada vez que haya cambios dentro del equipo que se ocupa de las tareas de administración.

Toda la información sobre los certificados (las fechas de renovación, los tipos de certificado, las autoridades de certificación emisoras, etc.) debe reunirse y guardarse en una carpeta segura de la empresa. No es buena idea que el administrador de los certificados SSL guarde los datos en su equipo o en una carpeta privada; no solo es peligroso, sino que si se va de la empresa, no podrás acceder a los datos necesarios para administrar los certificados.

Si alguien responsable de la gestión de certificados cambia de puesto o abandona la empresa, tendrás que cambiar todas las contraseñas relacionadas con los certificados (por ejemplo, las que dan acceso a la carpeta de la empresa, al servidor y a las claves de cifrado). Lee el apartado «Protección de claves privadas» de este capítulo para obtener más información al respecto.

Herramientas que facilitan la gestión de certificados

Gestionar los certificados SSL resulta más sencillo, rápido y barato si se utilizan herramientas que almacenen toda la información en un lugar seguro y automaticen parte del proceso de renovación. Symantec, por ejemplo, tiene varias para negocios de distintos tamaños.

Hoy en día, existen herramientas para pequeñas y grandes empresas. Por lo general, constan de un almacén que guarda en la nube toda la información relativa a los certificados SSL y un panel que permite consultar cuándo caducan los certificados. Con tan solo iniciar sesión en tu cuenta desde un navegador web, tendrás a tu disposición la información sobre todos los certificados SSL de la empresa, aun cuando tengan autoridades de certificación distintas.

Usar estas herramientas también te ahorrará tiempo y dinero a la hora de gestionar los certificados SSL. Disfrutarás de las siguientes ventajas:

- **Un proceso de compra más eficaz.** Comprar certificados SSL en pequeñas cantidades lleva mucho tiempo. Hay que rellenar formularios, hacer pedidos, obtener los datos de pago y ocuparse de otros trámites. Con un sistema de gestión centralizado, podrás hacer todas estas gestiones a la vez.
- **Un inventario mejor controlado.** Tener un inventario completo y preciso es fundamental para evitar problemas graves y no caer en la desorganización. Hay que saber, por ejemplo, qué certificados caducarán durante el mes en curso o a qué certificados podría afectar la virtualización de determinados servidores. Con una herramienta de gestión que se actualice automáticamente, toda esta información es muy fácil de obtener.
- **No más sustos de última hora.** Si descubres que un certificado está a punto de caducar, es posible que te cueste renovarlo a tiempo. Renovar certificados por lotes es mucho mejor que acabar siempre enterándose de que urge renovar un certificado o dos. Estas herramientas te avisan con antelación para que no se te pasen las fechas ni tengas que hacer renovaciones contra reloj.
- **La ventaja de poder hacer compras de mayor volumen.** Al centralizar la gestión, es más fácil comprar todos los certificados a una autoridad de certificación. Así, siempre reunirán los requisitos que hayas establecido y podrás beneficiarte de descuentos por volumen.

Las herramientas con funciones más avanzadas también permiten definir procedimientos de gestión y aplicarlos en toda la empresa. El sistema estará bajo tu supervisión, pero podrás delegar tareas o asignar privilegios a distintas unidades de negocio.

Protección de las claves privadas

En el capítulo 3 ya vimos que las claves privadas se usan para permitir el cifrado de los datos que intercambian los internautas con tu sitio web. Se podría decir que son las que establecen tu identidad en Internet. Es fundamental mantenerlas en secreto porque quien tenga acceso a ellas podrá suplantar tu sitio web y robar los datos de quienes lo utilicen.

De hecho, para los ciberdelincuentes suele ser más fácil infiltrarse en la red de una empresa y robar las claves de cifrado que romper el cifrado en sí.

En los sitios web de comercio electrónico, proteger las claves privadas es aún más importante porque se utilizan para cifrar los datos de las tarjetas de crédito. Este proceso está sujeto a la normativa de pagos con tarjeta (de la que ya hablamos en el capítulo 1), así que una mala gestión de las claves privadas podría constituir una infracción.

Si alguien se adueña de las claves privadas, podrá utilizarlas para crear otros sitios web en nombre de tu empresa. Estos sitios web falsos, que tal vez contengan *malware*, parecerán legítimos porque estarán autenticados con el certificado SSL de una autoridad de certificación de confianza. Si alguien se infecta al visitarlos, te echará la culpa a ti.

Para que nadie se apodere de tus claves privadas, sigue estos consejos:

- **Separa los servidores de la red de la empresa.** Asegúrate de que los servidores en los que se guardan las claves no estén dentro de la red de la empresa. Así, si un *phisher* logra infiltrarse en tu red con datos obtenidos a través del correo electrónico o las redes sociales, los daños serán menores. Asimismo, procura que solo unas cuantas personas tengan acceso a las claves y que solo haya un número reducido de equipos con copias de estas. Los duplicados deben estar tan controlados como las claves originales, lo que resulta más fácil si no hay muchos.
- **Adopta prácticas administrativas de eficacia demostrada.** No hagas copias innecesarias de las claves.
- **Automatiza la gestión de claves.** Usa un sistema de gestión de claves y certificados automatizados que genere y guarde las claves privadas sin que apenas se necesite intervención humana.
- **Sé cuidadoso con las contraseñas.** Cámbialas con regularidad y usa contraseñas distintas para cada almacén de claves.
- **Guarda un registro detallado de los cambios administrativos.** Cada vez que haya cambios en el personal administrativo, cambia las contraseñas del almacén de claves.

Symantec puede ayudarte

Symantec es una de las autoridades de certificación que cuenta con sus propias herramientas de gestión y mantenimiento de certificados SSL.

El Symantec Trust Center, pensado para negocios no muy grandes, permite gestionar todos los certificados SSL de Symantec y otros productos SSL desde un mismo lugar. Desde este portal web, una empresa puede consultar qué certificados tiene, renovarlos, comprar otros nuevos y actualizar sus datos de contacto.

Las empresas medianas o grandes, por su parte, pueden beneficiarse de las ventajas del Symantec Certificate Intelligence Center, que automatiza algunas de las fases de la gestión de certificados y ayuda a tenerlo todo controlado. Además de facilitar la gestión de los certificados SSL de Symantec, localiza y supervisa los de otras autoridades de certificación, incluidas las internas.

Una tercera herramienta de este tipo, Managed PKI for SSL, está dirigida a grandes empresas que tienen un gran número de certificados SSL gestionados por distintos administradores de diversas unidades de negocio. Con ella, es posible crear flujos de trabajo personalizados para la compra de certificados SSL, delegar tareas a distintos administradores y emitir certificados al instante en una serie de dominios aprobados de antemano.

Capítulo 7

Prácticas recomendadas para la protección de servidores web

En este capítulo, aprenderás...

- La importancia de instalar actualizaciones y revisiones
- Lo peligroso que es no estar alerta a las vulnerabilidades
- Qué prácticas reducen el riesgo que representan tus empleados

Para garantizar la seguridad de tu sitio web y de las personas que lo visitan, tienes que asegurarte de que ni el propio sitio web ni los servidores contienen código dañino (malware). De lo contrario, alguien podría:

- controlar el tráfico entrante y saliente;
- robar los datos que se transmiten del sitio web al ordenador de los internautas (o viceversa);
- instalar *malware* en los dispositivos de los clientes;
- infiltrarse en tu servidor (o, peor aún, en la red de la empresa) y acceder a tus datos y equipos.

Si no tomas medidas, alguien que quiera atacarte o explorar las vulnerabilidades de tu sitio web lo tendrá muy fácil. Ni siquiera hace falta que sea un experto en programación, ya que incluso hay a la venta *kits de herramientas* que los ciberdelincuentes pueden adquirir como si fueran paquetes de software corrientes.

En este capítulo, te diremos qué tienes que hacer para proteger los servidores web y cómo reconocer qué aspectos podrían ponerte en peligro.

La importancia de actualizar los sistemas

Los servidores de tu sitio web son como cualquier otro dispositivo conectado a Internet o a la red de la empresa. Al igual que los equipos de sobremesa, los portátiles y los programas que tienen instalados, exigen un mantenimiento y hay que actualizarlos y gestionarlos.

Por un lado, los servidores tienen su propio sistema operativo. Por otro lado, están las aplicaciones que muestran las páginas web a los internautas. Además, un gran número de sitios web también utilizan sistemas de gestión de contenidos que permiten a los usuarios sin grandes conocimientos técnicos crear y editar páginas web.

Todas estas capas de software pueden presentar vulnerabilidades que aumenten el riesgo de infección con *malware*. En muchos casos, los ciberdelincuentes aprovechan vulnerabilidades conocidas y que podrían resolverse fácilmente. El problema es que, con frecuencia, las víctimas no se preocupan por actualizar el hardware ni el software.

Preocúpate por tener siempre al día el software y el hardware, e instala las actualizaciones y revisiones en cuanto estén disponibles. Los proveedores sacan revisiones cuando los ciberdelincuentes o su propio personal encuentran una vulnerabilidad. Si no instalas las actualizaciones, estarás desprotegido frente a un ataque.

Servicios de detección de malware y evaluaciones de vulnerabilidad

Por mucho empeño que pongas en no dejar ninguna vulnerabilidad sin resolver, es posible que se te pase alguna. Las herramientas de análisis de terceros te ayudarán a sistematizar el proceso. Un gran número de proveedores y autoridades de certificación cuentan con servicios de evaluación de vulnerabilidades y detección de *malware*. Por ejemplo, los certificados SSL de Symantec incluyen análisis gratuitos que buscan vulnerabilidades sin resolver y comprueban si hay *malware* oculto (en el capítulo 8 encontrarás más información al respecto). Gracias a ellos, podrás tomar las medidas oportunas cada vez que se detecte un problema.

Este tipo de análisis no puede faltar en ninguna estrategia de seguridad multinivel. En 2013, el servicio de evaluación de vulnerabilidades de Symantec se utilizó para analizar miles de sitios web. En más de

tres cuartos de ellos, se encontraron vulnerabilidades sin resolver que alguien podría aprovechar para llevar a cabo un ataque. De todas las vulnerabilidades detectadas, un 16 % se consideró de carácter crítico porque, en caso de ser descubiertas, «habrían permitido a un atacante acceder a datos confidenciales, alterar el contenido del sitio web o infectar los equipos de quienes visitaran sus páginas» (Informe de Symantec sobre las amenazas para la seguridad).

Control de accesos

Por último, es conveniente que te preocupes por la seguridad de los servidores desde el punto de vista físico. Un empleado descuidado o que tenga algo en contra de la empresa podría ayudar a otras personas a infiltrarse o dejar el sitio web desprotegido y expuesto al *malware*.

Las siguientes medidas ayudan a reducir al mínimo estos riesgos:

- **Utilizar un sistema de autenticación de dos factores.** Exige dos formas de identificación en lugar de una para acceder a los servidores. Por ejemplo, podrías hacer que tus empleados inicien sesión con una contraseña y un lector de tarjetas (un sistema similar al que usan los cajeros automáticos, donde se necesita la tarjeta y el PIN).
- **Adoptar un procedimiento de acceso de doble clave.** Este método solo permite iniciar sesión si en el momento de hacerlo están presentes dos personas distintas.
- **Dar acceso limitado a la red.** Con este sistema, si alguien se infiltra en el sitio web, no tendrá acceso a toda la red de la empresa (y, a la inversa, si se infiltra en la red, el sitio web estará protegido).
- **Restringir el acceso.** Si solo permites que un número reducido de personas accedan a los servidores del sitio web, te será más fácil detectar a los intrusos.

Evita el uso de navegadores en los sistemas en los que esté instalado un servidor web. Muchos sistemas se infectan por *malware* que se descarga al acceder a páginas web dañinas. Lo mejor para mantener un servidor a salvo es asegurarse de que nadie utiliza un navegador desde el sistema en el que está instalado.

Capítulo 8

Claves para mantener protegido tu sitio web

En este capítulo, aprenderás...

- La importancia de inculcar al personal ciertos hábitos de seguridad básicos
- Por qué hay que estar siempre alerta y a la última
- Qué herramientas para administradores web permiten consultar si tu sitio web está en una lista negra

Los ciberdelincuentes siempre están buscando nuevas maneras de infiltrarse en sitios web y atacarlos para lucrarse. Su ingenio no conoce límites y la tecnología informática evoluciona constantemente, así que los métodos de protección de sitios web no pueden quedarse atrás.

Usar certificados SSL y proteger el servidor es fundamental, pero no suficiente. Para que un sitio web corra el menor riesgo posible, todo el personal de la empresa deberá adoptar una serie de precauciones y permanecer alerta en todo momento. Las personas son el eslabón más débil de la cadena de seguridad.

Para garantizar la seguridad de tu sitio web, es vital que tus empleados sepan qué peligros acechan en Internet. En este capítulo, veremos qué deben saber y, por otro lado, qué puedes hacer tú para protegerte aún más. Analizar tu sitio web, organizarte y usar herramientas de supervisión para administradores de sitios web te ayudará a evitar incidentes (o, si sufres alguno, a reducir al mínimo sus consecuencias).

Para evitar los peligros hay que conocerlos

Aunque este libro se centra principalmente en la protección de sitios web, tanto las empresas como los consumidores se enfrentan en Internet a muchos otros peligros que, en ciertos casos, podrían dar al traste con todos tus esfuerzos en materia de seguridad.

Por ejemplo, si un empleado abre un archivo adjunto de un desconocido y este contiene *malware*, podría acabar infectando la red de la empresa. Si los servidores web están conectados a la red o si en ella se guardan claves criptográficas o contraseñas de servidor, alguien podría acceder a estos datos y usarlos para atacar tu sitio web.

Conciencia a los empleados de los riesgos a los que se enfrentan al usar los dispositivos con los que trabajan. Por ejemplo:

- **El *phishing* en las redes sociales.** Hoy en día, se publica tanta información personal en las redes sociales que los delincuentes están empezando a frecuentar estas plataformas para publicar enlaces dañinos o tratar de obtener datos confidenciales. Un *phisher*, por ejemplo, podría tentar a sus víctimas con un vale-regalo falso o hacerles creer que la persona que ha publicado un enlace es amiga suya.
- **La posibilidad de que los ciberdelincuentes utilicen unidades USB como señuelo.** Ha habido casos en los que se han dejado unidades USB con *malware* en la zona de aparcamiento de una empresa. Los empleados, movidos por la curiosidad, las han cogido y, al conectarlas al ordenador del trabajo, han infectado toda la red. Pídeles a todos que, si encuentran unidades USB o discos de origen desconocido, se los entreguen al departamento informático.
- **El envío de mensajes de correo electrónico que son intentos de *phishing*.** En los últimos años, los ataques dirigidos se han vuelto más complejos y convincentes. En ciertos casos, los atacantes incluso llaman por teléfono a la víctima para avisarla de que van a enviarle un mensaje de correo electrónico. Hace poco, en Francia se produjo un incidente de este tipo. Alguien llamó a un departamento financiero quejándose de un retraso en un pago y diciendo que reenviaría la factura para que la empresa la abonara de inmediato. La supuesta factura era en realidad un archivo adjunto con *malware* que, al abrirse, acabó provocando una infección.

- Los peligros de visitar sitios web desprotegidos. En los cinco primeros capítulos de este libro, hemos ido analizando las distintas ventajas de los certificados SSL, que autentican al propietario de un sitio web y cifran los datos que se envían a través de él. Es importante que los empleados tengan en cuenta estos aspectos cuando visitan otros sitios web mientras trabajan. Por ejemplo, si la barra de direcciones aparece de color verde o comienza por «*https*», sabrán que el sitio web en el que están no es un clon, sino el que de verdad pretenden visitar.

Formas eficaces de limitar los daños

Por precavido que seas, quizá en alguna ocasión no puedas impedir que tu sitio web sufra un ataque. En ese caso, lo fundamental es darse cuenta lo antes posible y tomar las medidas necesarias para que la repercusión sea mínima.

Análisis periódicos de los sitios web

Algunos tipos de *malware* provocan innumerables trastornos e inhabilitan los servidores, mientras que otros se ejecutan en el servidor web sin levantar sospechas, lo que permite a los delincuentes robar toda la información posible y buscar otras vulnerabilidades que también puedan aprovechar.

Nunca se puede bajar la guardia porque cada vez que se encuentran nuevas vulnerabilidades en el software —lo cual sucede a menudo— surgen nuevos tipos de *malware* para explotarlas. Cuanto antes se detecte un problema, menor será el daño. Por eso es tan importante comprobar a diario o semanalmente si el sitio web contiene *malware*. Los servicios de análisis que existen para este fin no solo detectan el código dañino, sino que indican exactamente cuál es, lo que permite eliminarlo.

Por las mismas razones, también es necesario hacer análisis periódicos que comprueben si el sitio web presenta vulnerabilidades. Por lo general, con este servicio recibirás un práctico informe donde se detallan las vulnerabilidades críticas que se deben investigar de inmediato y otros riesgos de menor importancia. Esta información te ayudará a saber en qué aspectos de la protección del sitio web deberías centrarte o invertir más.

Herramientas para administradores de sitios web

Tanto Google como Bing cuentan con herramientas para administradores web. Si te registras y tu sitio web acaba en las listas negras del motor de búsqueda en cuestión, recibirás un aviso al instante.

La peor forma de enterarte de que estás en una lista negra es notar un descenso en el tráfico del sitio web. Con los avisos de estas herramientas, sabrás antes que tienes un problema y podrás tomar medidas para resolverlo.

Planes de recuperación en caso de desastre

Espera lo mejor y prepárate para lo peor. Si sufres un robo de datos o una infección de *malware*, siempre será mejor que hayas establecido un protocolo para recuperarte lo antes posible.

Los pasos concretos dependen del sector en el que trabajes, de los datos que recopile tu sitio web y de las jurisdicciones en las que operes, pero conviene que te plantees las siguientes preguntas.

- ¿A **quién** tienes que avisar? ¿A tus clientes? ¿A una entidad reguladora externa? ¿Quién se ocupará de dar la noticia?
- ¿**Qué** datos corren peligro? ¿Sabes qué redes se han visto afectadas y qué archivos deberías mirar para ver si han resultado atacados?
- ¿**Por qué** se ha producido el incidente? ¿Quién tendría que haber detectado y resuelto la vulnerabilidad que ha causado el problema?
- ¿**Cuándo** se produjo el incidente? ¿A cuántos datos afecta?
- ¿A **cuánto** ascienden los costes derivados del incidente si se tienen en cuenta la pérdida de ingresos, las horas de trabajo invertidas y las multas o indemnizaciones que haya que asumir?

Designa a alguien que se encargue de la elaboración de un plan, de supervisar su cumplimiento en caso de que haga falta llevarlo a cabo y de evaluar su utilidad y relevancia cada cierto tiempo.

La vulnerabilidad Heartbleed

Tanto este capítulo como el séptimo insisten en la importancia de tener siempre actualizados los servidores. La vulnerabilidad Heartbleed, un incidente de seguridad relacionado con la tecnología SSL que fue noticia en 2014, ilustra lo que puede ocurrir si se descuidan estas prácticas.

Los pormenores técnicos son algo complicados, pero vale la pena esforzarse un poco por entenderlos. Además, así verás cuánto has aprendido hasta ahora.

Cuando un navegador y un servidor web usan un certificado SSL para establecer una conexión segura, es útil que permanezcan conectados un tiempo aunque no se transmitan datos continuamente. De lo contrario, habría que estar conectándose al mismo sitio web una y otra vez, lo cual sería un engorro.

En muchos servidores web, la tecnología SSL se implementa mediante OpenSSL, una biblioteca de software criptográfico abierto que se sirve de un «latido» para mantener abiertas las conexiones seguras. Básicamente, la biblioteca envía un mensaje al servidor, que verifica la conexión y devuelve el mensaje al emisor.

El mensaje consta de dos elementos: un paquete de datos de hasta 64 KB denominado «carga útil» e información sobre el tamaño de este.

La vulnerabilidad Heartbleed permite que el atacante «engañe» a la biblioteca SSL, de forma que el tamaño del paquete de datos parezca mayor de lo que es en realidad.

Lo que hace tan peligrosa la vulnerabilidad Heartbleed es que, al recibir este mensaje, OpenSSL no comprueba si la carga útil real coincide con la declarada. En cambio, da por supuesto que el tamaño es el correcto y trata de enviar la carga útil al equipo desde el que se envió. Como no tiene 64 KB de datos, accede a la memoria de la aplicación y «rellena» la carga útil con los datos almacenados junto a ella, que podrían ser de cualquier tipo (p. ej., datos de inicio de sesión de un usuario, datos personales o, en algunos casos, claves de sesión o claves de cifrado privadas).

Si un servidor se ve afectado por esta vulnerabilidad, la única solución es pasarse a la nueva versión de OpenSSL. Las actualizaciones siempre son importantes, pero en este caso son absolutamente esenciales. Es importante recalcar que Heartbleed no fue consecuencia de un defecto intrínseco de la tecnología SSL, sino del programa de código abierto OpenSSL, cuyo uso está muy extendido.

Capítulo 9

Las diez fuentes de información más útiles sobre protección de sitios web

En este capítulo, aprenderás...

- A qué fuentes puedes recurrir para informarte
- Quién hay detrás de cada una de ellas
- Qué información proporcionan

Este libro contiene información sobre los aspectos básicos de la protección de sitios web, pero es posible que quieras profundizar en otros. Por ejemplo, si trabajas en un sector sujeto a normativas muy estrictas, quizá necesites más información sobre cómo garantizar su cumplimiento.

O tal vez estés buscando materiales que tus empleados puedan consultar para informarse sobre los peligros de Internet.

La lista de entidades, organizaciones y recursos de este capítulo te dará acceso a material muy útil.

CA Security Council

`https://casecurity.org/`

El CA Security Council (CASC) está formado por las principales autoridades de certificación y tiene como objetivo desarrollar y promoción de prácticas recomendadas para mejorar la implantación segura de certificados SSL y las operaciones de las autoridades de certificación, así como la seguridad en Internet en general. El CASC no establece normativas, pero es un referente muy importante para comprender mejor las políticas principales de seguridad y su potencial impacto en la infraestructura de Internet.

Su sitio web cuenta con gran cantidad de blogs y libros blancos con información sobre amenazas de seguridad, ataques y noticias sobre las autoridades de certificación.

Certification Authority Browser Forum

cabforum.org

El Certification Authority/Browser Forum, también llamado CA/Browser Forum, es un consorcio de autoridades de certificación y proveedores de navegadores de Internet. Se fundó en 2005 con el propósito de fomentar el uso de métodos de seguridad que demuestren a los internautas que los sitios web que visitan son seguros y auténticos.

Su objetivo es lograr que el mayor número posible de empresas utilicen certificados SSL para autenticar sus sitios web e infundir confianza.

El sitio web contiene información dirigida a particulares, empresas, programadores y auditores. Consúltalo para afianzar tus conocimientos sobre los aspectos más generales de los certificados SSL o bien para informarte sobre cómo instalarlos. Además, como ya mencionamos en el capítulo 4, el CA/Browser Forum establece los requisitos para la emisión de certificados con EV, así que también encontrarás una gran cantidad de material sobre ese tema.

Symantec Website Security Solutions

www.symantec.com/es/es/ssl-certificates/

Symantec, una de las principales autoridades de certificación y miembro fundador del CA/Browser Forum, cuenta con un gran número de recursos informativos sobre la protección de sitios web.

www.symantec-wss.com

En esta página, encontrarás libros blancos sobre distintos temas, como los peligros a los que se enfrenta tu sitio web y el funcionamiento del *malware*. Si la visitas, también podrás descargar el informe de Symantec sobre las amenazas para la seguridad de los sitios web, que analiza con todo lujo de detalles las tendencias actuales en materia de protección de sitios web.

Online Trust Alliance

otalliance.org

La Online Trust Alliance (OTA), fundada en 2005, es una organización global sin ánimo de lucro con sede en Bellevue (Washington, EE. UU.). Según su propia descripción, se trata de «un grupo de trabajo informal cuyo objetivo es conseguir que los internautas estén más informados, hacer de Internet un lugar más fiable y promover la innovación y la vitalidad de la Red».

El sitio web contiene información práctica sobre multitud de temas, como el uso de la tecnología Always-On SSL, la normativa de protección de datos, la protección de aplicaciones para dispositivos móviles y las autoridades de certificación. La organización también tiene en marcha diversas iniciativas, como la dedicada a ayudar a las empresas a proteger su reputación.

Electronic Frontier Foundation

www.eff.org

La Electronic Frontier Foundation estudia los efectos de la tecnología y la seguridad web en los consumidores. Desde su fundación en 1990, ha tratado de defender la privacidad de los usuarios, la libertad de expresión y la innovación mediante una serie de actividades, como la participación en acciones legales, la práctica del activismo, el análisis de políticas y otras iniciativas destinadas a impulsar los avances tecnológicos.

Si lo que quieres es infundir confianza a quienes visitan tu sitio web, probablemente te interesen sus puntos de vista. Vale la pena leer sus libros blancos sobre la intersección entre la ley y la tecnología, sobre todo si trabajas en un sector con normativas muy estrictas.

PCI Security Standards Council

www.pcisecuritystandards.org

Si tus clientes hacen compras en tu sitio web, la página del PCI Security Standards Council (del que hablamos en el capítulo 1) es de visita obligada. Este foro mundial fundado en 2006 pone a tu disposición un caudal de información sobre el uso de las tarjetas de crédito en transacciones de comercio electrónico. Quizá también te interesen las recomendaciones sobre otros métodos de pago, como los realizados desde dispositivos móviles o con lectores de tarjetas.

Agencia Española de Protección de Datos

www.esagpd.es

La Agencia Española de Protección de Datos es un «ente público independiente cuya finalidad principal es velar por el cumplimiento de la legislación sobre protección de datos personales».

Aunque se centra principalmente en los derechos de los ciudadanos, el sitio web contiene información sobre los métodos de recopilación, almacenamiento y destrucción de información confidencial que deben seguir las empresas. Visítalo para informarte sobre qué tipo de datos personales debes proteger y para estar al tanto de otras obligaciones.

Herramientas para webmasters de Google

www.google.com/webmasters

Las herramientas para *webmasters* de Google no solo te avisan de si tu sitio web está en una lista negra, sino que también cuentan con funciones de análisis que te harán más visible en las búsquedas y te ayudarán a mejorar tu posicionamiento en Google. Te recomendamos que te registres para aprovechar estas ventajas.

INTECO

www.inteco.es

En España, el Instituto Nacional de Tecnologías de la Comunicación (INTECO) «pone a tu disposición todos los recursos relacionados con la ciberseguridad, para que te protejas ante los peligros de la red».

El apartado «Protege tu empresa» es una mina de recursos que te será especialmente útil. Encontrarás información sobre cómo crear un plan de seguridad o cómo conseguir que el uso de dispositivos móviles en el trabajo no suponga un riesgo para tu negocio.

Symantec Connect

http://www.symantec.com/connect/blogs/website-security-solutions

Como ya hemos dicho, Symantec es una de las principales autoridades de certificación. Su eficaz infraestructura de clave pública (PKI) incluye sitios de recuperación en caso de desastre y centros de datos que garantizan una seguridad comparable a la que se exige para usos militares. De este modo, los clientes disfrutan de una solución excelente en cuanto a la disponibilidad y la protección de los datos, con lo que no tienen que preocuparse por nada. Según una encuesta de Netcraft SSL, en septiembre de 2013, la mitad de los sitios web con tecnología SSL con Extended Validation (incluidos los de algunas de las principales empresas de comercio electrónico y servicios bancarios) usaban marcas de Symantec.

Los clientes, socios y empleados de Symantec acuden al sitio web de Symantec Connect para buscar soluciones, compartir conocimientos técnicos y aportar ideas para posibles productos. Te invitamos a leer los blogs y a participar en interesantes debates sobre la seguridad en Internet y la protección de sitios web.

Symantec. | Website Security Solutions

Proteja su sitio web y expanda su negocio

Symantec ofrece una amplia gama de soluciones de seguridad para sitios web, como el mejor cifrado SSL del sector, la gestión de los certificados, la evaluación de vulnerabilidad y el análisis contra software malicioso. Además, el sello Norton™ Secured y la función Seal in Search de Symantec demuestran a sus clientes que en su sitio web pueden realizar búsquedas, navegar y comprar sin ningún peligro.

Norton SECURED
powered by Symantec

Sello Norton Secured

A diario, el sello se muestra más de mil millones de veces en 170 países.[1]
El 90 % de los encuestados declaran que es más probable que continúen con un proceso de compra electrónica si lo ven.[2]

Evaluación de vulnerabilidad

En 2013, se hicieron públicas 6787 vulnerabilidades.[3]
Los análisis semanales ayudan a detectar y solucionar las deficiencias de seguridad que pueda presentar su sitio web.

Análisis contra software malicioso

El 67 % de los sitios web maliciosos son sitios legítimos que han sido atacados.[3] La función de escaneado diario detecta el código dañino (malware) e informa al propietario del sitio web.

Asistencia ininterrumpida

Atención a todas horas, todos los días del año. Un gestor personal de cuentas para satisfacer sus necesidades concretas.

01001
00101
00111

Un cifrado aún más seguro

Criptografía de curva elíptica (ECC).[4]

Póngase en contacto con su asesor de seguridad de Symantec para obtener más información.

Llame al 900 93 1298 o visite www.symantec.es/ssl

1 Datos de clientes internos de Symantec.
2 Estudio sobre consumo internacional en Internet: Estados Unidos, Alemania y Reino Unido. Julio de 2013.
3 Informe de Symantec sobre las amenazas para la seguridad de los sitios web (2013).
4 Symantec ofrece la tecnología ECC sin ningún coste adicional para todos sus certificados SSL Premium.

Contar con un sitio web seguro es clave para el éxito de una empresa

Los consumidores son conscientes de los peligros que acechan en Internet y solo te confiarán sus datos si saben que los protegerás como es debido. En esta guía, te explicaremos cómo vencer este recelo y ganarte su confianza gracias a los certificados SSL y a una serie de hábitos de mantenimiento. Te ayudaremos a encontrar la opción más adecuada para tu empresa.

- ***Infunde confianza.*** ***Compra tus certificados SSL a una autoridad de certificación de confianza que cuente con procedimientos rigurosos de autenticación de empresas.***
- ***Protege los datos de tus clientes.*** ***Con el cifrado SSL, los hackers no podrán interceptar los datos que se transmitan en tu sitio web.***
- ***Tranquiliza a los internautas y consigue más conversiones.*** ***Para que quienes visiten tu sitio web hagan compras y faciliten sus datos sin temor, usa marcas de confianza y otros distintivos de seguridad.***

Además, analizaremos:

- **Los riesgos que entraña un sitio web desprotegido**
- **Para qué sirven los certificados SSL y cuál es el procedimiento estándar para adquirirlos**
- **La importancia de elegir una autoridad de certificación de confianza**
- **Las prácticas recomendadas para garantizar la seguridad de un sitio web a largo plazo**

Symantec: Symantec Website Security Solutions ofrece una amplia gama de soluciones de seguridad para sitios web, como el mejor cifrado SSL del sector y servicios de gestión de certificados, evaluación de vulnerabilidad y análisis contra software malicioso. Además, el sello Norton™ Secured y la función Seal in Search de Symantec demuestran a tus clientes que en tu sitio web pueden realizar búsquedas, navegar y comprar sin ningún peligro.

WILEY

ISBN: 9781119088189