Symantec. Website Security.
We go beyond

WHITE PAPER

Argumentos para convencer al responsable de seguridad de la información de la necesidad de invertir en una solución de protección de sitios web completa

UN NUEVO CONCEPTO DE CONFIANZA

Argumentos para convencer al responsable de seguridad de la información de la necesidad de invertir en una solución de protección de sitios web completa

¿Pasa demasiado tiempo gestionando los certificados SSL/TLS? ¿Carece de un sistema que le permita analizar y elaborar informes sobre todos los certificados del entorno? ¿Alguna vez se ha interrumpido algún servicio por culpa de un certificado caducado? ¿Tiene que actualizar manualmente los certificados?

Si ha respondido afirmativamente a alguna de estas preguntas, ha llegado el momento de invertir en una solución de gestión de certificados automatizada.

Dar este paso sería muy beneficioso para su empresa, ya que dejaría de perder tiempo y dinero en tareas manuales poco precisas y contaría con las herramientas adecuadas para proteger mejor el sitio web, disfrutar de una mayor visibilidad y prevenir posibles problemas de seguridad. Este artículo analiza las ventajas de adoptar una protección de sitios web completa y explica cómo justificar la inversión ante el director de seguridad informática. Así podrá empezar a mejorar su modelo de protección y dedicar más tiempo al análisis, la elaboración de informes y otras tareas de seguridad de carácter estratégico.

El valor de un sitio web bien protegido

Un sitio web seguro debe ser fiable, tener una disponibilidad elevada y estar protegido frente a accesos no autorizados, robos de datos y ataques con malware.

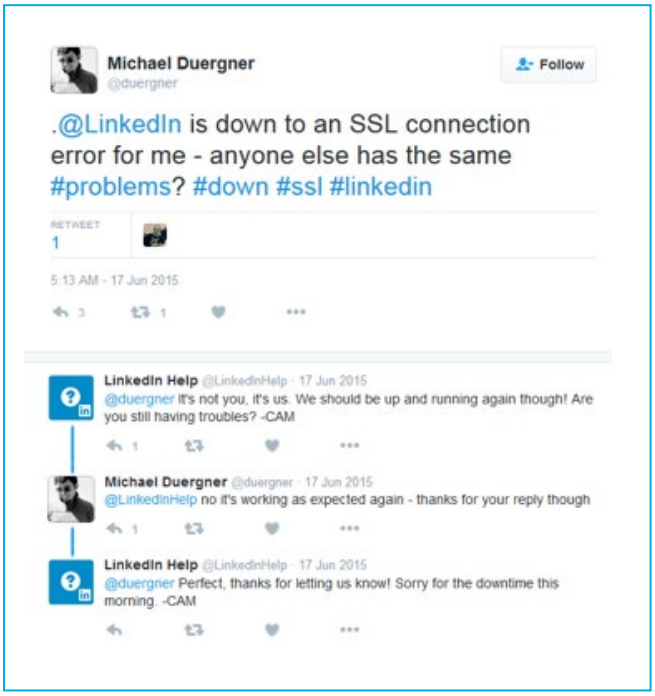
Los certificados SSL/TLS son una arma importante en su arsenal de seguridad. Además de servir para la autenticación y el cifrado de páginas web (sus funciones tradicionales), ahora se consideran piezas clave de un entorno de protección del sitio web más amplio, con funciones como el análisis contra software malicioso, las evaluaciones de vulnerabilidad y la aplicación de revisiones.

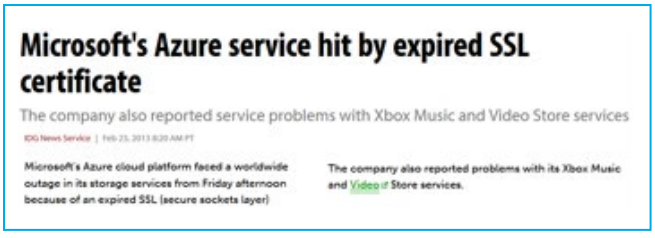
En los últimos años, ha habido casos muy sonados en los que el acceso a sitios web se ha visto interrumpido por problemas relacionados con los certificados, algo que pone de manifiesto la importancia de no descuidar este aspecto.

Cuando un sitio web es seguro, apenas se nota. Pero una protección inadecuada —o, peor aún, inexistente— puede tener consecuencias como estas:

- La inutilización de sitios web de importancia vital para la empresa debido a problemas relacionados con los certificados SSL/TLS.
- La enorme pérdida de visitas durante largos periodos a consecuencia de ataques de denegación de servicio distribuida.
- El robo masivo de información de los clientes a manos de hackers, ya sea para filtrarla en Internet o para venderla a delincuentes que quieran aprovecharla.
- El uso de sitios web en apariencia fiables para infectar con malware los sistemas de quienes los visitan y, seguidamente, obtener y eliminar todos los datos.
- La desfiguración o el sabotaje de sitios web con fines propagandísticos o para dañar la imagen de sus propietarios.

Todo esto subraya la importancia de utilizar las mejores soluciones y contar con el apoyo de un líder global en seguridad que ofrezca un servicio de atención ininterrumpida.





El costo operativo de la falta de seguridad de un sitio web

La mayoría de las empresas se preocupan por proteger sus sitios web de distintas maneras (por ejemplo, manteniendo actualizados los certificados SSL/TLS e instalando firewalls o programas contra software malicioso en los servidores web). Pero las mejores intenciones no siempre van acompañadas de prácticas irreprochables.

Las siguientes seis preguntas le ayudarán a evaluar las actividades relacionadas con la protección de sitios web y la gestión de certificados en su empresa:

- ¿Tiene en su infraestructura certificados SSL/TLS de distintos proveedores y, si es el caso, sabría decir cuántos, quién los emitió y dónde están exactamente?
- ¿Sabe cuándo caducan todos y cada uno de los certificados que gestiona?
- ¿Sabe cuánto tiempo dedica a renovar e instalar certificados manualmente?
- ¿Sabe qué gasto supone para su empresa la administración de certificados SSL/TLS?
- ¿Sabe qué presupuesto anual exige la gestión de certificados SSL/TLS?
- ¿Sabe exactamente quién compra certificados en su empresa y cómo los gestiona?

Los profesionales de la seguridad rara vez responden afirmativamente a todas estas preguntas.

Lo habitual es que usen un sistema de protección de sitios web poco automatizado, que se sientan desbordados por sus tareas cotidianas y que les resulte difícil gestionar diferentes soluciones desvinculadas entre sí y relacionarse con los distintos proveedores.

Una mala gestión de la seguridad no solo supone una pérdida de tiempo, dinero y recursos, sino que también dificulta la detección y resolución de problemas.

Muchas empresas invierten demasiado tiempo en gestionar manualmente los certificados y, además, carecen de un sistema que permita ver fácilmente todos los certificados del entorno. Esta falta de visibilidad dificulta, a su vez, la toma de medidas destinadas a reducir los riesgos y asegurar el cumplimiento de la normativa.

A menudo, los procesos de compra, renovación e instalación de certificados son demasiado engorrosos, sobre todo si hay que emitir un pedido distinto para cada operación. Si nada de esto está automatizado, será más fácil que se cometan errores.

Las cifras son elocuentes. Según cálculos de Cisco, cuando los certificados SSL/TLS se gestionan manualmente, cada uno de ellos requiere de cuatro horas y representa un costo de 288 USD.[1]

En empresas con miles de certificados, el costo de la gestión manual es enorme. Si la suya tiene centenares y usa hojas de cálculo de Excel u otros procedimientos manuales para tenerlos bajo control, debería plantearse seriamente adoptar una solución automatizada. Solo con el tiempo que ahorraría la amortizaría muy pronto.

Según cálculos de Cisco, cuando los certificados SSL/TLS se gestionan manualmente, cada uno de ellos requiere de cuatro horas y representa un costo de 288 USD.[1]

[1]«Case Study: Scalable Key and Certificate Lifecycle Management with Cisco Systems», Session ID: SPO1-303, RSA Conference 2011, Cisco Systems Inc.

El costo de un sitio web mal protegido

El costo de una seguridad deficiente del sitio web y de una mala gestión de los certificados SSL/TLS no se limita a los gastos de administración cotidianos. Cuando se produce un problema, las consecuencias económicas pueden ser considerables:

- **Interrupciones del servicio.** Cada interrupción puede resultar muy costosa. Hay informes que estiman que un ataque de denegación de servicio puede costar hasta 20 000 USD[2] por hora. Es probable que el costo sea el mismo si el servicio se interrumpe debido a un algún problema con los certificados u otra vulnerabilidad.
- **Resolución de problemas.** Las empresas de la lista Global 5000 gastan un promedio de 15 millones de dólares en recuperarse de una interrupción de servicio causada por una mala gestión de los certificados, y otros 25 millones en asegurar el cumplimiento de la normativa. Además, las filtraciones de datos se castigan con sanciones cada vez más severas.
- **Pérdida de reputación.** Su empresa no solo se arriesga a acabar en la lista negra de Google y a pagar primas de seguros más altas, sino también a ver profundamente dañada su imagen. Por lo general, la cotización en bolsa solo cae temporalmente[3] después de un incidente de seguridad grave, pero recuperar la reputación perdida lleva mucho más tiempo.

Si no distingue o comprende los riesgos reales, si carece de funciones de automatización, o si no está seguro de cumplir o no la normativa, le será prácticamente imposible saber cómo y dónde convendría invertir sus recursos informáticos y de seguridad.

> El costo de una seguridad deficiente del sitio web y de una mala gestión de los certificados SSL/TLS no se limita a los gastos de administración cotidianos.

[2]https://www.theatlantic.com/technology/archive/2016/10/a-lot/505025/
[3]https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices

Conclusión

A la hora de convencer al director de seguridad de la necesidad de invertir en un sistema de protección de sitios web, hay varios aspectos en los que conviene insistir:

Automatización

Según un informe reciente de NopSec [4], las empresas de servicios financieros tardan un promedio de 176 días en corregir una deficiencia de seguridad porque utilizan procesos manuales laboriosos. A menudo, la falta de automatización dificulta el cumplimiento de la normativa y genera problemas de rendimiento o seguridad.

Al dejar las tareas de protección del sitio web en manos de los empleados, no solo se malgastan recursos. Tanto si se trata de operaciones rutinarias como de otras más complejas, siempre podrá haber errores que pongan en peligro el sitio web, empeoren su rendimiento o contravengan la normativa. Un simple error involuntario puede poner a una empresa en la cuerda floja, sea grande o pequeña. Además, los procedimientos manuales no bastan para protegerse de ataques de gran magnitud. Si su empresa es víctima de un ataque «exprés», la intervención humana nunca llegará a tiempo. En caso de que sus sistemas se vean afectados, tardará más tiempo en solucionar el problema y recuperarse, y los daños podrían ser mayores.

Visibilidad

Gestionar la seguridad y el cumplimiento de la normativa sin los recursos y la visibilidad suficientes es una batalla perdida. Protegerse no es nada fácil porque la seguridad tiene muchas facetas y, además, hay que cumplir la legislación y las normas del sector.

Muchas grandes empresas se debaten constantemente entre dos alternativas: invertir tiempo y recursos en progresar o en protegerse. Si, además, no hay un método estandarizado para proteger los servidores web, las aplicaciones y los datos que componen el entorno del sitio web, la falta de visibilidad empeorará las cosas.

Si no ve ni comprende el riesgo real o desconoce si cumple o no la normativa, le será prácticamente imposible saber cómo y dónde convendría invertir sus recursos informáticos y de seguridad.

Agilidad

Los procedimientos manuales no bastan para protegerse de ataques de gran magnitud. Si su empresa es víctima de un ataque «exprés», la intervención humana nunca llegará a tiempo. En caso de que el ataque logre su cometido, tardará más tiempo en solucionar el problema y recuperarse, y los daños podrían ser mayores.

Ahora más que nunca, invertir en un sistema de protección de sitios web multipunto, multinivel y con la mayor automatización posible es vital para combatir la continua aparición de ataques cada vez más complejos.

[4] http://info.nopsec.com/rs/736-UGK-525/images/NopSec_StateofVulnRisk_WhitePaper_2015.pdf

Symantec™ Complete Website Security

Symantec Complete Website Security ofrece a su empresa, a su marca y a sus clientes protección exhaustiva y en profundidad, así como una visibilidad y agilidad mayores. Sus soluciones completas, las mejores en su categoría[6], le ayudarán armonizar y reforzar los mecanismos de defensa de su sitio web.

Con la protección multipunto y multinivel, el entorno del sitio web estará protegido frente a la aparición de amenazas complejas. Además, disfrutará de una visibilidad en tiempo real que le permitirá bloquear ataques, cumplir la normativa y detectar y resolver problemas con rapidez. Symantec Complete Website Security incorpora las herramientas y servicios necesarios para preservar la integridad y el rendimiento de los servidores del sitio web, los certificados y las aplicaciones.

Gracias a su modelo de seguridad ágil, tendrá todo bajo control y podrá alcanzar sus objetivos de protección y crecimiento en menos tiempo. Al estar respaldada por uno de los líderes mundiales en ciberseguridad, con el distintivo de confianza más reconocido en Internet[7] y una de las mayores redes de ciberinteligencia del mundo, su empresa podrá velar por la seguridad del entorno de su sitio web, de sus clientes y de la empresa con las garantías de asistencia y protección adecuadas.

Más información

Visite nuestro sitio web : http://www.symantec.com/complete-website-security/

[6]http://ww2.frost.com/news/press-releases/frost-sullivan-applauds-breadth-symantecs-security-solutions-well-collaborations-customers-and-peers-provide-customized-tools
[7]Investigación de IpSOS sobre consumo internacional en Internet: (EE.UU., Alemania, Reino Unido, Francia, Australia y Singapur; octubre de 2015) y análisis de comScore sobre las principales empresas de comercio electrónico. Estados Unidos: 90 %. Reino Unido: 89 %. Australia: 88 %. Singapur: 92 %.

Symantec. Website Security.
We go beyond

Symantec™ Complete Website Security

Armonice y refuerce la seguridad de los sitios web

Symantec™ Complete Website Security puede ayudar a reforzar la seguridad de los sitios web; a evitar o minimizar los daños provocados por las amenazas avanzadas, que aumentan constantemente; a liberar recursos para destinarlos a tareas más estratégicas; a simplificar la protección de los sitios web; y a administrar la empresa e impulsar su expansión sin temer por su seguridad.

Para abrir una cuenta o solicitar más información sobre lo que puede hacer Symantec™ Complete Website Security por su empresa, póngase en contacto con nosotros.

Llame al:
América Latina: +1 520 477 3111
Correo electrónico: ssl_info@symantec.com
Si desea los números de teléfono de algún país en particular, consulte nuestro sitio web.

Para recibir información sobre productos, llame al:
América Latina: +1 520 477 3111

Symantec World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com/complete-website-security

Symantec Mexico
Ciudad de México,
Paseo de Tamarindos #400A P-16, Col.
Bosque de las Lomas,
Cuajimalpa, CP 05120,
Mexico DF, México
www.symantec.com/es/mx/complete-website-security

Vaya siempre un paso por delante con Symantec