

CONTINUIDAD DE LA ACTIVIDAD EMPRESARIAL Y
PROTECCIÓN CONTRA LAS FILTRACIONES: POR QUÉ
LA GESTIÓN DE CERTIFICADOS SSL ES FUNDAMENTAL
PARA LAS EMPRESAS EN LA ACTUALIDAD

White paper

Continuidad de la actividad empresarial y protección contra las filtraciones: por qué la gestión de certificados SSL es fundamental para las empresas en la actualidad

Continuidad de la actividad empresarial y protección contra las filtraciones: Por qué la gestión de certificados SSL es fundamental para las empresas en la actualidad

Contenido

Introducción	3
Desafíos en la gestión de los certificados SSL	3
Los peligros de los certificados SSL maliciosos y caducados	4
Robo de información del cliente	4
Pérdida de clientes ante competidores	6
Aumento de llamadas a la asistencia técnica	6
Mayor esfuerzo de los departamentos de TI	6
Prácticas recomendadas en la gestión de certificados SSL	7
Conclusión	8
Symantec® Certificate Intelligence Center: Gestión y detección eficaz de SSL.	8

Introducción

Los certificados SSL se han utilizado durante casi 15 años, y continúan desempeñando un papel fundamental en la protección de datos que viajan por Internet y otras redes. Desde transacciones financieras online hasta el comercio electrónico y el desarrollo de producto, los certificados SSL posibilitan a los usuarios de todo el mundo comunicar información confidencial con la confianza de saber que está a salvo de los piratas informáticos maliciosos.

Internet ha evolucionado de innumerables formas en la última década y media. Entonces, ¿por qué los certificados SSL continúan inspirando confianza? En otras palabras, los certificados SSL son muy eficaces para proteger los datos en tránsito. De hecho, según estimaciones, crackear un cifrado de 128 bits en certificados SSL con un ataque de fuerza bruta tardaría aproximadamente casi seis mil billones de años (o casi un millón de veces más que el tiempo de existencia de la tierra).¹ Aun así, el sector de la seguridad permanece siempre alerta, y muchas autoridades de certificación han comenzado a planificar el cifrado de 2048 bits en sus certificados SSL, lo que fortalece aún más la protección de la comunicación de datos online.

Sin embargo, los clientes que realizan transacciones en sitios web y sistemas que están protegidos por seguridad SSL afrontan graves amenazas. Una razón fundamental para este peligro: la gestión deficiente del certificado SSL. Las empresas con cientos de certificados SSL de diferentes proveedores pueden perder el registro de los certificados en su entorno. Cuando esto sucede, los certificados pueden caducar y pasar desapercibidos durante meses, lo que deja a sus visitantes vulnerables a los piratas informáticos.

A veces, el primer indicio de que se ha "perdido" un certificado SSL es una llamada de un cliente que detecta un certificado caducado y pregunta si hacer una compra en el sitio web es realmente seguro. Otras veces puede ser algo más grave, como un incidente de phishing que permite a los cibercriminales robar datos confidenciales de clientes. O un fallo de seguridad que se produce en una autoridad de certificación y repercute en una organización debido a su incapacidad de actuar rápidamente dada la falta de visibilidad de su inventario de certificados SSL.

Independientemente de cuál sea el motivo, perder el registro de los certificados SSL puede provocar pérdidas financieras y daños a la reputación significativos. Afortunadamente, no es necesario que la detección y la gestión de certificados SSL en la empresa sean complejas o consuman mucho tiempo.

En este white paper, se describirán las dificultades relacionadas con una gestión deficiente de certificados SSL, por qué son potencialmente peligrosos para las empresas y de qué manera se puede llevar un registro eficaz de los certificados SSL.

Desafíos para la gestión de los certificados SSL

Las empresas actuales son entornos complejos que, con frecuencia, abarcan varias redes internas y sitios web públicos. Por este motivo, una empresa puede contar con docenas (o cientos) de diferentes certificados SSL implementados en cualquier momento.

1. <http://www.inet2000.com/public/encryption.htm>

Además de una gran cantidad de certificados SSL, muchas empresas utilizan una combinación de diversos certificados de diferentes autoridades de certificación. Como ejemplo, una empresa puede instalar certificados SSL de un proveedor de confianza y conocido en el sitio web público y certificados autofirmados o de marca de valor en su intranet.

Si bien algunas autoridades de certificación ofrecen herramientas online para gestionar sus certificados particulares, con frecuencia, estas herramientas no pueden proporcionar visibilidad de todos los certificados desde varias autoridades de certificación en un entorno. En lugar de facilitar la gestión, la existencia de muchos portales de gestión empeora el problema de registrar varios certificados SSL en un entorno de varias autoridades de certificación. Los administradores necesitan supervisar constantemente su inventario de certificados SSL mediante varios sistemas y elaborar sus propios informes para obtener una percepción más amplia de su inventario de certificados SSL.

Lo que genera más complicaciones es que las políticas de seguridad de las empresas con redes distribuidas pueden diferir de un grupo a otro. En la práctica, esto significa que el Grupo A puede necesitar certificados SSL con Extended Validation para proteger los datos que gestiona, pero el Grupo B utiliza un tipo diferente de certificados SSL de otra autoridad de certificación. O, en un caso que puede ser más común, el Grupo A puede requerir certificados SSL de 2048 bits, mientras que el Grupo B utiliza certificados de 1024 bits. Con políticas diferentes y sin manera de obtener una vista más amplia de los certificados SSL en una empresa, estas incoherencias pueden provocar riesgos para la seguridad y el incumplimiento de políticas normativas y corporativas.

Para añadir otra dimensión al problema, considere qué sucede cuando los empleados que son responsables de gestionar la seguridad de SSL cambian de función o abandonan la empresa. Si no se documenta rigurosamente qué certificados gestionan (y se comunica esta información a otros miembros del equipo), es posible que estos certificados SSL particulares pasen desapercibidos cuando un nuevo miembro del equipo asuma la función. Debido a que los equipos de TI de las empresas están ocupados y, con frecuencia, cuentan con pocos recursos, el registro manual de certificados SSL no solamente representa una carga, sino que hace que sea propenso a errores humanos.

Todos estos factores contribuyen a un entorno donde es posible que los certificados SSL se pierdan o se pasen por alto. Dicho entorno puede provocar interrupciones en la actividad comercial de una empresa y crear riesgos para la seguridad de sus clientes.

Los peligros de los certificados SSL maliciosos y caducados

Un certificado SSL caducado o malicioso en un entorno de red puede tener graves repercusiones. Solamente se necesita un certificado malicioso o desactualizado para exponer a la empresa (y, lo que probablemente sea más importante, a sus clientes) al cibercrimen malicioso. A continuación, se enumeran algunas de las posibles consecuencias de los certificados SSL maliciosos y caducados.

Robo de información del cliente

Gracias a años de noticias sobre filtraciones de información y el trabajo de empresas y grupos de apoyo al consumidor, el público está más preocupado que nunca por el robo de identidad. Un estudio reciente reveló que el 64% de

los ciudadanos estadounidenses están muy preocupados o extremadamente preocupados por el robo de identidad, y el 31% describe su nivel de preocupación como extremo.²

En este contexto, el riesgo de phishing es una importante preocupación. En un ataque de phishing, el pirata informático asume la identidad de una empresa legítima (aprovechando la falta de autenticación de certificados SSL no existentes o caducados de la empresa), y crea un sitio web falso que se parece o que es idéntico al sitio real. Los clientes desprevenidos introducen información confidencial, como el número del DNI o de tarjetas de crédito. El sitio de phishing transmite estos datos directamente al pirata informático que, a su vez, puede venderlos a otros delincuentes.

Incluso si un incidente de phishing o una filtración de datos es relativamente menor, puede agravar estos temores y amenazar seriamente a la empresa.

Además de las pérdidas inmediatas, el phishing y las filtraciones de datos también pueden afectar a la reputación de una empresa y provocar que los clientes y potenciales clientes se cuestionen si una empresa en particular es de confianza. Los expertos del sector afirman que estabilizar las ventas y la confianza en la red de una empresa después de una filtración tarda aproximadamente seis meses³ e, incluso, es posible que la reputación de la empresa no se recupere por completo.

El coste cada vez más alto de la filtración de datos

Si bien el daño a la reputación de una empresa puede ser difícil de medir, entender el impacto económico de una filtración de datos es más sencillo. Según un estudio reciente, realizado en EE. UU., el coste medio de una filtración de datos es de 7,2 millones de dólares por evento, o casi 214 dólares por registro afectado,⁴ cifras que, según estimaciones, continuarán aumentando.



Consecuencias de la caducidad imprevista de SSL y advertencias del navegador

2. "Identifique el temor a los robos en los estadounidenses", por Tim Greene, Network World, 12/04/2010
3. "La filtración de datos de Sony expone a los usuarios a años de riesgos de robo de datos", por Cliff Edwards y Michael Riley, BusinessWeek.com, 03/05/11
4. "El coste de una filtración de datos aumenta", Ponemon Institute, ponemon.org, 08/03/11

Pérdida de clientes ante competidores

Otro factor que preocupa a las empresas son los certificados SSL vencidos. Un certificado SSL vencido puede provocar otro tipo de pérdida empresarial. Entre las principales pérdidas se encuentra la pérdida de tráfico cuando los clientes ven advertencias de la caducidad de un certificado SSL y abandonan su sitio para comprar productos y servicios en sitios que estén protegidos por certificados SSL.

Es posible que los clientes no sepan exactamente cómo funciona el cifrado de clave pública, pero los signos visibles de la seguridad de SSL (como un sello de confianza de SSL o la barra de Extended Validation verde) harán que sea más fácil que realicen transacciones en un sitio en particular.⁵ Si caducan los certificados SSL de sitios de comercio electrónico u otro tipo de sitios públicos, se perderá la confianza de los clientes, lo que provocará la pérdida de negocios.

Aumento de llamadas a la asistencia técnica

En la actualidad, muchas empresas ofrecen herramientas web, menús telefónicos automatizados y otras opciones de autoservicio para facilitar que los clientes que tienen preguntas encuentren la información que necesitan. Sin embargo, si los clientes visitan un sitio web y tienen dudas sobre si sus datos privados están protegidos, abandonarán la transacción (como se mencionó anteriormente) o se comunicarán con la asistencia al cliente.

El coste medio por llamada a asistencia al cliente varía ampliamente entre sectores, pero un dato es seguro: el coste de numerosas llamadas a la asistencia al cliente se incrementa con el transcurso del tiempo. No solo estas llamadas agotan los recursos financieros, sino que además representan una carga adicional para el centro de contacto y evitan que el personal de asistencia atienda otras llamadas de clientes de mayor valor.

El coste adicional y la incomodidad relacionados con las consultas de los clientes pueden evitarse fácilmente manteniendo la seguridad actualizada, incluidos certificados SSL válidos.

Mayor esfuerzo de los departamentos de TI

De igual modo que los clientes llaman a asistencia al cliente cuando tienen dudas acerca de la seguridad de un sitio web, los empleados que ven advertencias provenientes de certificados SSL caducados en intranets u otros sitios internos, suelen contactar con el personal de TI para solucionar el problema. Esto puede añadir una carga significativa a los departamentos de TI que ya están sobrecargados.

En otros casos, es posible que los empleados directamente ignoren estas advertencias de caducidad, lo que deja a los recursos afectados vulnerables ante ataques. Por otra parte, establece un precedente negativo para el cumplimiento de la seguridad, ya que da la impresión de que el personal ignora las medidas internas de seguridad.

Cualquiera de estos escenarios puede evitarse mediante la seguridad de los certificados SSL actualizados en toda la empresa.

5. <http://www.verisign.es/ssl/symantec-certificate-intelligence-center/index.html>

Prácticas recomendadas en la gestión de certificados SSL

Afortunadamente, existen servicios que facilitan la detección y la gestión de certificados SSL en toda la empresa. Algunas soluciones afirman que disminuyen la carga de la gestión de SSL, incluso si no permiten detectar certificados de varias autoridades de certificación. Otras soluciones ofrecen la capacidad de analizar varias autoridades de certificación, pero no cuentan con una interfaz de usuario intuitiva y fácil de navegar.

Para garantizar que encontrará la mejor solución que satisfaga sus necesidades, a continuación le mostramos algunas funciones clave que debe buscar en cualquier solución:

- **Posibilidad de analizar su entorno automáticamente:** si bien es posible auditar redes manualmente, este enfoque tardaría mucho tiempo y requeriría demasiados recursos de personal como para ser posible en un entorno empresarial grande y complejo. Seleccionar un servicio que permita a su equipo realizar análisis automáticos que detecten los certificados SSL de todos los proveedores.
- **Una interfaz fácil de usar:** información difícil de leer o a la que no se pueda acceder no será útil. Por lo tanto, busque una herramienta que ofrezca un panel de información fácil de navegar y que presente datos que se entiendan de un vistazo.
- **Capacidades de delegación:** en el típico entorno empresarial, varios empleados se encargan de gestionar la seguridad. Por este motivo, es fundamental encontrar una solución de detección de certificados que permita a los administradores conceder diferentes niveles de acceso y delegar tareas a varios empleados en la red.
- **Alertas y elaboración de informes:** un certificado SSL caducado pone en peligro los datos. Por lo tanto, es fundamental encontrar un servicio que envíe alertas antes de que un certificado tenga que renovarse. Asimismo, la capacidad de generar informes que sean fáciles de leer y entender es muy importante. Las capacidades avanzadas de elaboración de informes no solamente proporcionarán una percepción más amplia y profunda de los certificados en la red, sino que también permitirán a su equipo comunicar información fundamental a otros empleados (como los ejecutivos) con mayor eficacia.
- **Flexibilidad y escalabilidad:** las redes empresariales son entornos dinámicos y en constante cambio, lo que significa que un servicio de detección de certificados debe contar con parámetros que se puedan configurar, como la duración del análisis y qué direcciones IP analizar, entre otros. Asimismo, el servicio debe ser escalable, para permitir el crecimiento futuro.
- **Puntualidad:** Para ser eficaz, los análisis de la red deben realizarse rápidamente. Si un análisis de toda la red tarda demasiado, es posible que el estado de algunos certificados SSL cambie antes de que finalice el análisis completo. Esto provocará una percepción inexacta del inventario de certificados SSL.

Conclusión

Los certificados SSL son fundamentales para proteger los datos en tránsito. A pesar de su fortaleza y fiabilidad, la seguridad SSL puede ser vulnerable a ataques por una simple razón: la gestión deficiente del certificado SSL.

En un entorno empresarial con varias autoridades de certificación y diferentes certificados, es fundamental obtener una vista más amplia de la seguridad de SSL. Conocer el estado de cada certificado en los sitios y las redes no solamente puede ayudar a controlar los costes del servicio al cliente, sino también a reducir la carga de la gestión de SSL, lo que dará a los ocupados equipos de TI más tiempo para concentrarse en otros proyectos empresariales.

La gestión rigurosa de SSL también puede evitar consecuencias mucho más serias (incluidos incidentes graves de phishing u otro tipo de filtración de datos) que no solamente será costoso remediar, sino que también pueden provocar daños a largo plazo en su reputación.

Symantec® Certificate Intelligence Center: Gestión y detección eficaz de SSL

Symantec Certificate Intelligence Center ayuda a los administradores a detectar y gestionar los certificados SSL con mayor eficacia. Con capacidades de gestión y gran visibilidad, Symantec Certificate Intelligence Center facilita el registro de certificados SSL.

Symantec Certificate Intelligence Center incluye una interfaz intuitiva que permite a los administradores configurar análisis automáticos que detectan los certificados de cualquier autoridad de certificación con rapidez. Los usuarios también pueden configurar alertas que adviertan de forma anticipada a los administradores de SSL sobre la inminente caducidad de los certificados.



El panel de información fácil de navegar que ofrece Symantec Certificate Intelligence Center

Symantec Certificate Intelligence Center, una solución fácilmente escalable, se adapta a los rápidos cambios de la red a medida que las necesidades comerciales se modifican y aumentan. Las capacidades de elaboración de informes también ofrecen a los administradores una percepción más amplia de la seguridad de SSL que es fácil de entender y comunicar en la empresa.

Para obtener más información sobre cómo Symantec Certificate Intelligence Center puede ayudarle a simplificar la detección y la gestión de certificados SSL, visite: <http://www.verisign.es/ssl/symantec-certificate-intelligence-center/index.html>

Más información

Visite nuestro sitio web

<http://www.verisign.es>

Para hablar con un especialista de producto

900 93 1298

+41 26 429 7727

Acerca de Symantec

Symantec es un líder mundial en soluciones de seguridad, almacenamiento y gestión de sistemas, que ayudan a consumidores y organizaciones a proteger y gestionar su información. Nuestros programas y servicios protegen contra una mayor cantidad de riesgos en más puntos y de una forma más completa y eficaz, lo que brinda tranquilidad sin importar dónde se utilice o se almacene la información. Con sede central en Mountain View, California (EE. UU.), Symantec está presente en más de 40 países. Para obtener más información, visite www.symantec.es.

Symantec Spain S.L.

Parque Empresarial La Finca – Somosaguas,
Paseo del Club Deportivo,
Edificio 13, oficina D1,
28223, Pozuelo de Alarcón,
Madrid,
España



Servicios de autenticación
VeriSign