Symantec. Website Security.
We go beyond

WHITE PAPER

Optimice toda su empresa, desde la arquitectura del sitio web hasta la junta directiva

UN NUEVO CONCEPTO DE CONFIANZA

Claves para optimizar desde la arquitectura del sitio web hasta la junta directiva

El sitio web de su empresa es su activo digital más importante, y protegerlo es tan esencial como tener un flujo de caja positivo, pagar los salarios o garantizar el buen funcionamiento de la oficina central.

Pero, para los responsables de seguridad de la información y otros ejecutivos de las grandes empresas, no es fácil proteger los sitios web de peligros cada vez mayores y, además, cumplir un sinfín de normativas que no cesa de crecer.

A pesar de la magnitud de las amenazas y de la importancia de combatirlas, la «arquitectura de seguridad del sitio web» (un concepto que engloba la organización, los objetivos y la tecnología del departamento de TI) suele ser inadecuada.

Lo que necesitan los directores de sistemas y de seguridad de la información es una arquitectura estratégica que les permita emprender iniciativas destinadas a garantizar la seguridad, la fiabilidad y la eficiencia a largo plazo.

Con una planificación y puesta en práctica correctas, será posible crear una empresa más capacitada para resolver problemas, más ágil y con un mayor nivel de autoconocimiento, características que ayudan a combatir mejor amenazas que cambian con rapidez. Este artículo analiza los retos que supone este cambio y propone un plan de actuación viable.

Peligros y desafíos

Hoy en día, las amenazas evolucionan muy deprisa y son tantas y tan complejas que las soluciones tradicionales ya no bastan. Veamos algunos ejemplos sacados del informe de Symantec sobre las amenazas para la seguridad de los sitios web[1] y de otras fuentes.

- En un año, hubo 318 incidentes de seguridad graves que comprometieron los datos de 429 millones de personas.
- Según Ponemon, se detectaron vulnerabilidades en más de la mitad de las aplicaciones probadas (el 52 %)[2].
- Tres cuartos de los sitios web presentaban vulnerabilidades.
- Los ataques de denegación de servicio distribuida (en especial el ataque DYN DNS) inutilizaron más aplicaciones y servicios conocidos[3].
- Las vulnerabilidades de día cero alcanzaron niveles sin precedentes, lo que demuestra que, por sí solo, el análisis contra software malicioso basado en firmas ya no es suficiente.
- Ahora los certificados digitales son el blanco de los ciberdelincuentes[4].

Impedir el acceso no autorizado a los sistemas y los datos más importantes es cada vez más difícil, un reto al que se suman obligaciones como el cumplimiento de la normativa reciente sobre protección de datos (p. ej., el nuevo reglamento general europeo de protección de datos[5]) o de los requisitos aplicables al procesamiento de pagos con tarjeta de crédito (como la última versión del estándar PCI-DSS).

Por otro lado, los equipos responsables de la seguridad de los sitios web tienen que hacer mejoras que beneficien a la empresa. Por ejemplo, cada vez más sitios web recurren al cifrado integral para inspirar más confianza a los consumidores y mejorar su posicionamiento, una tendencia que se acelerará con el lanzamiento de Google Chrome 56. Además, muchas empresas están abandonando el cifrado SHA-1 y los certificados con validación de dominio para pasar a los certificados SSL/TLS, que son más seguros.

Ahora que las empresas apuestan por los servicios alojados en la nube pública o híbrida y dan cada vez más cabida a dispositivos de usuario final, los profesionales informáticos deben cuidar más que nunca aspectos como la automatización y la facilidad de gestión. La gestión de sitios web tiene que reflejar esta realidad, como ya sucede en otros ámbitos informáticos. Por ejemplo, las empresas que gestionan sus certificados con sistemas coordinados y automatizados están más preparadas para responder a vulnerabilidades como el ataque «Drown» de 2016[6] que aquellas que utilizan procedimientos manuales.

Para los directores de seguridad de la información y otros profesionales con responsabilidades similares, detenerse equivale a retroceder y adelantarse exige un enfoque completamente nuevo.

Ahora que las empresas apuestan por los servicios alojados en la nube pública o híbrida y dan cada vez más cabida a dispositivos de usuario final, los profesionales informáticos deben cuidar más que nunca aspectos como la automatización y la facilidad de gestión.

Problemas relacionados con la infraestructura existente

1. En busca de la coordinación perdida

Por desgracia, en los departamentos de seguridad informática, la ambigüedad, la confusión y la falta de responsabilidad son habituales. Según Ponemon, dos tercios de las empresas tienen prácticas de seguridad fragmentadas[7]. El problema es que los puestos de trabajo se conciben de manera restrictiva y se da más importancia a las «cosas» —los servidores, las aplicaciones y los dispositivos— que al valor de los datos que contienen.

Si los departamentos y divisiones de una empresa son irrelevantes para los datos y para los atacantes, ¿por qué todo el mundo se concentra en lo suyo y supervisa únicamente sus propios sistemas? Una persona compra los certificados, otra gestiona los servidores, otra se ocupa de la protección antivirus para terminales y así sucesivamente. A veces, solo la junta directiva ve la gestión y la responsabilidad desde un punto de vista más amplio.

Los atacantes no se limitan a los servidores, los equipos de los usuarios o el correo electrónico, sino que están dispuestos a ir mucho más allá para conseguir su objetivo. Para detenerlos, sus empleados deberían tener la misma mentalidad.

Sin embargo, la seguridad de los sitios web, las aplicaciones y los dispositivos conectados suele ser responsabilidad de varios equipos. Si uno detecta una vulnerabilidad y otro se dedica a investigarla y repararla, la prevención y la resolución de problemas llevarán más tiempo. Cuando sucede algo grave, una mala organización puede dar lugar a infracciones de seguridad y demandas colectivas o poner en tela de juicio a la junta directiva.

La organización lo es todo

Los resultados de un equipo dependen de su estructuración, objetivos y decisiones, así como de su asignación de responsabilidades. «La estructura dicta la relación entre los distintos roles de una empresa y, por lo tanto, la forma de actuar de las personas —declara el experto en gestión Gill Corkindale[8]—. Una estructura desfasada puede provocar una ambigüedad, una confusión y una falta de responsabilidad innecesarias».

Los departamentos que están siempre «sobrecargados de trabajo» son otro ejemplo de las consecuencias de una mala organización. Según un informe reciente de NopSec[9], las empresas de servicios financieros tardan un promedio de 176 días en corregir una deficiencia de seguridad, lo que se debe en gran parte al uso de procedimientos manuales complejos. De nada sirve que tengan departamentos de TI de gran tamaño en los que, al igual que en su empresa, los empleados trabajan duramente.

No cabe duda de que hace falta un cambio. Lo mejor es partir del punto en que se encuentra y seguir las prácticas recomendadas, como los consejos de Forrester para crear un departamento de seguridad sólido[10] o la plantilla orientativa de Carnegie Mellon sobre cómo estructurar la empresa[11]. También resultan útiles modelos de gestión tan conocidos como el de las 7 eses de McKinsey[12], según el cual «la coordinación influye más que la estructura en la eficacia de una empresa».

Ni siquiera se necesitan más empleados, más presupuesto y más recursos. De hecho, una empresa bien diseñada aprovecha mejor los recursos existentes de forma automática.

Incluso hay quienes piensan que contratar más personal es un error. «Los estudios demuestran que cada vez que se duplica el tamaño de una ciudad, la tasa de innovación o productividad por residente aumenta en un 15 %. Pero cuando las empresas crecen, la innovación o productividad por empleado generalmente disminuyen», opina Tony Hsieh, fundador de Zappos.

En un contexto informático ocurre lo mismo, como se explica en el libro «El mítico hombre-mes», un clásico de Fred Brooks. Al asignar más personal a un proyecto de TI retrasado, el esfuerzo adicional que supone comunicarse con quienes se incorporan al proyecto aumenta a un ritmo más acelerado que el trabajo extra que realizan. «Agregar recursos humanos a un proyecto retrasado lo hace demorarse aún más», concluye Brooks.

La conocida metodología de desarrollo ágil[13], surgida en el ámbito del software, puede ayudar también a que los empleados asuman mejor los cambios y servir de inspiración en departamentos de seguridad informática sobrecargados de trabajo. Lo importante es que se trata de un modelo más basado en la adaptación que en la predicción, y que su eficacia en departamentos de TI de gran tamaño está demostrada.

El costo de un sitio web mal protegido

2. La dificultad de decidir lo mejor para todos
Los directores informáticos ya no tienen una visión integral de los sistemas que gestionan ni de los peligros que corren, pues cada vez se usan más soluciones desvinculadas entre sí.

Es posible que no siempre sea el departamento de TI quien configure las aplicaciones —al fin y al cabo, es una tarea sencilla— o que el deseo de conseguir más clientes lleve al departamento de marketing a adoptar nuevas tecnologías sin el conocimiento o la aprobación del personal informático. Dentro de una empresa, puede haber grupos que recurran al autoservicio o creen su propio entorno con la intención de ser más productivos o adoptar rápidamente determinadas tendencias. Mientras que una computadora portátil viene protegida de fábrica, la seguridad de un sitio web suele estar en manos de jefes de proyecto que no siempre conocen o comprenden las normas que deberían seguir.

En este contexto tan complejo, el personal tiende a saltarse las reglas simplemente para hacer su trabajo. Tal vez piense que todos sus certificados SSL/TLS son de un mismo proveedor, pero si no lo ha comprobado y los empleados no han seguido los procedimientos establecidos, es posible que los hayan emitido más de una decena de autoridades de certificación.

Estas prácticas hacen más vulnerable a su empresa, representan trabajo extra, crean entornos fragmentados y hacen que la gente no asuma los problemas como propios o se niegue a usar sistemas inventados por otros. En situaciones así, la seguridad informática no solo dificulta la innovación (por ejemplo, será difícil hacer una apuesta decidida por la tecnología en la nube), sino que también debilita el sentido de responsabilidad de los empleados

3. Automatizar o no automatizar, esa es la cuestión
La existencia de estructuras y procesos deficientes también puede afectar gravemente la gestión de certificados. Estos son algunos de los riesgos que implica el hecho de carecer de sistemas automatizados, normas coherentes y herramientas de gestión centralizadas:

- Si los certificados caducan de forma imprevista, los internautas verán mensajes de advertencia que minarán su confianza.
- Algunos de los certificados del entorno podrían incumplir la normativa establecida (p. ej., tal vez se usen certificados con validación de dominio o con un nivel de cifrado insuficiente en sistemas esenciales para la empresa).
- Puede que haya empleados que compren certificados a proveedores no autorizados, a pesar de que lo tengan prohibido.
- Es posible que las normas de la empresa se apliquen de forma irregular.

Se tiende a pensar que solo vale la pena automatizarlo todo, pero en realidad no es así. Automatizar procesos aislados tiene ventajas más pequeñas pero también valiosas, y las empresas que no se dan cuenta están perdiendo oportunidades. Por ejemplo, una empresa que analice los certificados y detecte los que presentan vulnerabilidades conocidas podrá reaccionar a incidentes de seguridad como Heartbleed.

Como dijo Warren Buffet, «El tiempo es amigo de los buenos negocios y enemigo de los mediocres». Los mejores departamentos de TI saben que aparentar estar ocupado no tiene sentido, y por eso apuestan por la automatización y usan menos procedimientos manuales. Pero esta filosofía solo es posible si la eficiencia se considera prioritaria, se reconoce y se premia.

4. La apuesta por la nube, una lucha entre el miedo y el deseo
La computación en la nube cobra cada vez más fuerza, y tres cuartos de las grandes empresas ya utilizan más de una nube. Sin embargo, la gestión de entornos híbridos (o de varios entornos en la nube) es complicada porque obliga a utilizar un sinfín de herramientas de distintos proveedores, algo que los departamentos de seguridad aceptan con resignación pero también con inquietud, ya que estos nuevos procesos podrían causar problemas internos o de seguridad.

En el caso de las nubes híbridas, cumplir la normativa y demostrarlo es aún más difícil. No basta con que la nube privada y la pública cumplan la normativa por separado; la coordinación y la transmisión de datos entre ambas también tendrá que ajustarse a ciertos requisitos. Por ejemplo, si su empresa maneja datos de tarjeta de crédito, tendrá que demostrar que tanto los sistemas internos como los de su proveedor de tecnología en la nube cumplen la normativa aplicable al sector de pagos con tarjeta. Cuando se adopta una nube híbrida, hay que asegurarse de que el intercambio de datos entre los dos entornos que la componen es seguro.

En un entorno híbrido, hay que supervisar toda la infraestructura de clave pública (PKI). Si usa un sistema de gestión para detectar los certificados del centro de datos y una herramienta distinta para supervisar los que estén en la nube (la proporcionada por el proveedor), acabará teniendo otra tecnología, otra consola de administración y otro elemento de la infraestructura desvinculado de los demás. Por eso es tan importante invertir en soluciones que permitan consultar al instante si los servidores web, las aplicaciones y los datos están protegidos en todo el entorno, sea cual sea la plataforma o el proveedor. Con este enfoque global, será más fácil detectar vulnerabilidades, bloquear ataques, mantener la integridad de las aplicaciones y los certificados, cumplir las normas, detectar pronto las infracciones y resolver cuanto antes los problemas.

Las cuatro claves para optimizar la seguridad del sitio web

1. Dar prioridad a la resolución de problemas

Aunque elegir la estructura adecuada y gestionar los cambios es importante, lo esencial es fijar bien los objetivos. En nuestra opinión, para que los sitios web estén bien protegidos, tanto los responsables de seguridad de la información como los directores de sistemas deberían seguir los siguientes pasos:

- designar a los responsables de la resolución de problemas y reconocer el trabajo que realizan;
- reforzar la importancia de que todos los cargos y equipos asuman sus responsabilidades;
- acabar con la pasividad e incentivar una actitud proactiva;
- fomentar la automatización y concentrar los esfuerzos en actividades de gran valor;
- adaptar la estructura a las necesidades de la empresa
- y a los activos que hay que proteger (en lugar de proteger únicamente los dispositivos o herramientas);
- actuar lo antes posible (no es necesario hacerlo todo a la vez; siempre es mejor hacer algo que no hacer nada).

2. Mejorar la visibilidad

Pasar de un enfoque reactivo a otro proactivo lleva su tiempo, pero la tecnología adecuada le ahorrará muchas horas de trabajo. Si la única solución de gestión que utiliza es Excel, está claro que su empresa no va por buen camino.

En Symantec, le recomendamos adoptar herramientas que permitan consultar más fácilmente si los servidores web, las aplicaciones y los datos están protegidos. Así, detectará cuanto antes las vulnerabilidades y podrá velar por la integridad de las aplicaciones y los certificados digitales de un modo más eficaz. Lo mejor es elegir soluciones capaces de:

- comprobar si los servidores web de la red cumplen la normativa y los requisitos de auditoría (verificando su huella digital);
- detectar certificados que vayan a caducar o sean fraudulentos, de alto riesgo o de origen desconocido;
- crear informes y registros de auditoría detallados que faciliten la atribución de responsabilidades (con una buena arquitectura de seguridad, es más fácil cumplir la normativa y demostrarlo, lo cual es una ventaja aunque esto último no mejore la seguridad de la empresa).

3. Automatizar el mayor número de tareas posible

La automatización debería convertirse en su próxima prioridad. Este enfoque puede aplicarse a los entornos, servidores, controles de seguridad y requisitos normativos, pero, en lo que respecta a la gestión de certificados, empiece por:

- automatizar las transferencias y renovaciones de certificados;
- adoptar flujos de trabajo basados en políticas y controles de acceso basados en roles;
- simplificar la compra y la instalación de certificados según la normativa establecida;
- utilizar herramientas de monitorización que detecten certificados irregulares (para evitar problemas a posteriori).

No hace falta que espere a poder automatizarlo todo. Cualquier mejora que haga, por pequeña que sea, le permitirá dedicar más tiempo a tareas más importantes. Por ejemplo, podría hacer un «sprint» inspirado en la metodología ágil y automatizar la gestión del 10 % de los certificados.

4. Sacar partido a la nube

Usar tecnología en la nube, siempre que sea posible, resulta rentable y reduce el tiempo de implementación, ya que no se necesita una infraestructura local.

Elija siempre tecnologías flexibles y orientadas a empresas que:

- permitan proteger entornos híbridos;
- sean compatibles con entornos locales y en la nube;
- ofrezcan modelos de suscripción basados en la nube que permitan gestionar todo el ciclo de vida de los certificados con una solución de seguridad adaptable que funcione de forma ininterrumpida;
- permitan adoptar la nube al ritmo más adecuado para su empresa.

Cambie las reglas, no el juego

En resumen, le recomendamos:

Poner fin a los compartimentos aislados;

- crear una estructura empresarial más ágil y coordinada;
- fijar bien sus objetivos;
- mejorar la visibilidad;
- automatizar el mayor número de tareas posible;
- aprovechar las posibilidades que ofrece la nube.

Las empresas que sigan estas recomendaciones no estarán a merced de los organismos reguladores ni de quien quiera atacarlas, sino que se regirán por sus propias reglas y tendrán la flexibilidad y la productividad necesarias para protegerse frente a las amenazas que surjan y resolver los problemas con rapidez. Si quiere acabar con la inercia, la descoordinación, los procedimientos manuales y la vulnerabilidad, optimizar la arquitectura de seguridad del sitio web es la única opción posible para su empresa.

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, le ayudarán a 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 respaldado por uno de los líderes mundiales en ciberseguridad, con el distintivo de confianza más reconocido en Internet y una de las mayores redes de ciberinteligencia del mundo, usted podrá velar por la seguridad del entorno de su sitio web, de sus clientes y de su empresa con las garantías de asistencia y protección adecuadas.

Más información

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

[1] https://websitesecurity.symantec.com/campaigns/16963-campaign/current/landing/assets/wstr-pt1-us.pdf
[2] https://securityintelligence.com/events/ponemonapplicationsecurityriskmanagement/
[3] http://searchsecurity.techtarget.com/news/450401962/Details-emerging-on-Dyn-DNS-DDoS-attack-Mirai-IoT-botnet
[4] http://www.pcworld.com/article/3044804/cyberespionage-groups-are-stealing-digital-certificates-to-sign-malware.html
[5] https://www.symantec.com/content/dam/symantec/docs/infographics/a-new-dawn-for-data-privacy-infographic-en.pdf
[6] http://www.computerweekly.com/news/4500277804/Drown-attack-sinks-SSL-security
[7] https://securityintelligence.com/events/ponemonapplicationsecurityriskmanagement/
[8] https://hbr.org/2011/02/the-importance-of-organization
[9] http://info.nopsec.com/rs/736-UGK-525/images/NopSec_StateofVulnRisk_WhitePaper_2015.pdf
[10] http://eval.symantec.com/mktginfo/enterprise/articles/b-article_security_organization_20_building_a_robust_security_organization.en-us.pdf
[11] https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf
[12] http://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/enduring-ideas-the-7-s-framework
[13] https://en.wikipedia.org/wiki/Agile_software_development

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,
México DF, México
www.symantec.com/es/mx/complete-website-security

Vaya siempre un paso por delante con Symantec