Guía de Seguridad en Aplicaciones para CISOs

El Guía de Seguridad en Aplicaciones para CISOs versión 1.0 documento es una traducción al español del documento oficial en inglés **"Application Security Guide For CISOs"** de OWASP.

Tabla de contenido

Licenciamiento

1. Preámbulo

1.1. Introducción

Entre las partes interesadas en la seguridad de las aplicaciones, los Jefes de Seguridad de la Información (CISOs) son responsables de la seguridad de las aplicaciones desde la perspectiva de gobierno, cumplimiento y riesgo. Esta guía pretende ayudar a los CISOs a gestionar programas de seguridad en aplicaciones de acuerdo a sus roles, responsabilidades, perspectivas y necesidades. Las mejores prácticas de seguridad en aplicaciones y los recursos de OWASP están referenciados en esta guía. OWASP es una organización sin fines de lucro cuya misión es "hacer visible la seguridad en aplicaciones y potenciar a las partes interesadas con información adecuada para la gestión de riesgos de seguridad en las aplicaciones".

Esta guía está escrita para ayudar a los CISOs, quienes son responsables de la gestión de programas de seguridad de aplicaciones, desde las perspectivas de la seguridad de la información y la gestión de riesgos. Desde la perspectiva de la seguridad de la información, existe la necesidad de proteger activos de la organización tales como el ciudadano, los datos sensibles de los clientes, las bases de datos donde se almacenan estos datos, la infraestructura de red en la que los servidores de bases de datos residen y por último, pero no menos importante, las aplicaciones y el software utilizado para acceder y procesar estos datos. Además de los datos del negocio y de los usuarios, las aplicaciones y el software están entre los activos que los CISOs buscan proteger. Algunas de estas aplicaciones y softwares proporcionan funciones críticas de negocio a los clientes, generando ingresos para la organización. Los ejemplos incluyen aplicaciones y software que les proporcionan a los clientes servicios para sus negocios, así como también aplicaciones que son vendidas como productos a sus clientes. En el caso en que las aplicaciones se consideren activos de información críticos para el negocio, deben recibir una atención especial en recursos humanos, capacitación, procesos, normas y herramientas.

El alcance de esta guía es la seguridad de las aplicaciones web, los componentes de la arquitectura, como la seguridad de servidores web, servidores de aplicación y bases de datos. Esto no incluye otros aspectos de seguridad que no estén relacionados con la aplicación específica, tales como la seguridad de la infraestructura de red que soporta las aplicaciones y constituye un activo valioso cuyas propiedades de seguridad como la confidencialidad, integridad y disponibilidad también necesitan ser protegidas.

Objetivos

Esta guía ayuda a los CISOs a gestionar los riesgos de seguridad en aplicaciones, al considerar la exposición a amenazas emergentes y requisitos de cumplimiento. Esta guía ayuda a:

- Hacer visible la seguridad en aplicaciones a los CISOs.

- Garantizar la conformidad de las aplicaciones respecto a regulaciones sobre privacidad, protección de datos y seguridad de la información.
- Priorizar la remediación de vulnerabilidades basado en la exposición al riesgo para el negocio.
- Proporcionar orientación para la construcción y gestión de procesos de seguridad en aplicaciones.
- Analizar ciberamenazas contra aplicaciones e identificar contramedidas.
- Instituir capacitaciones sobre seguridad en aplicaciones para desarrolladores y administradores.
- Medir y gestionar riesgos de seguridad en aplicaciones y procesos.

Destinatarios

- Jefes de Seguridad de la Información (CISOs)
- Administradores de seguridad senior
- Administradores de tecnología senior

1.2. Resumen Ejecutivo

El hecho que las aplicaciones deban ser consideradas activos de la empresa es *"per se"* una buena razón para colocarlas dentro del alcance de cumplimiento de las políticas y normas de seguridad de la información. El impacto del cumplimiento de tales políticas y normas para las aplicaciones depende típicamente de la clasificación de los activos de información almacenados por la aplicación, el tipo de exposición de la aplicación ante los usuarios (por ejemplo, Internet, intranet, extranet) y los riesgos que la funcionalidad de la aplicación admite con los datos (por ejemplo, acceso a datos confidenciales, transferencia de dinero, pagos, administración de usuarios, etc.). Desde una perspectiva de seguridad de la información, las aplicaciones deben estar dentro del alcance de las evaluaciones de vulnerabilidades específicas y los requisitos de seguridad de la aplicación. Las validaciones de seguridad y la certificación de aplicaciones siguen requisitos específicos de seguridad, tales como el diseño seguro, programación segura y operaciones seguras. Estos son a menudo parte de los objetivos de las normas de seguridad en aplicaciones. Por lo tanto, el cumplimiento es un aspecto crítico de la seguridad en aplicaciones y de las responsabilidades del CISO, pero no el único. La seguridad en aplicaciones abarca otros dominios en los cuales los CISOs son responsables. Tales dominios se pueden resumir con la sigla GRC (Gobierno, Riesgo y Cumplimiento).

- Desde la perspectiva del gobierno, los CISOs son responsables por instituir procesos de seguridad en aplicaciones, roles y responsabilidades para gestionarlos, capacitación y concientización en seguridad de software para desarrolladores, tal como programación defensiva y gestión de riesgos/vulnerabilidades para oficiales/administradores de seguridad de la información.
- Desde la perspectiva de la gestión de riesgos, los gestionados por los CISOs también incluyen los riesgos de seguridad en aplicaciones, como los derivados de amenazas específicas dirigidas a aplicaciones que procesan datos confidenciales de usuarios buscando explotar brechas en controles de seguridad, así como vulnerabilidades en aplicaciones.
- Entre los dominios en los que actúan los CISOs, el cumplimiento de regulaciones y normas de seguridad, suele ser el que recibe la mayor atención por parte de la dirección ejecutiva de la organización. El objetivo de esta guía es ayudar a los CISOs a cumplir los requerimientos de

cumplimiento, así como utilizarlos como una de las razones para justificar inversiones relacionadas con seguridad en aplicaciones. Para algunas organizaciones, gestionar riesgos de incidentes de seguridad tales como fraudes con tarjetas de crédito, robo de información personal, robo de propiedad intelectual y datos confidenciales es lo que se lleva la mayor atención de la dirección ejecutiva, sobre todo cuando la organización se ha visto afectada por incidentes de seguridad de filtración de datos.

Parte I: Razones para invertir en seguridad de aplicaciones

En esta era digital, las organizaciones públicas y privadas sirven a un número cada vez mayor de ciudadanos, usuarios, clientes y empleados a través de aplicaciones web. A menudo, estas aplicaciones web ofrecen "servicios altamente confiables" a través de Internet, incluyendo funciones que tienen un alto riesgo para el negocio. Estas aplicaciones web son el objetivo de un número cada vez mayor de estafadores y ciberdelincuentes. Muchos incidentes resultan en una denegación del acceso en línea, filtración de datos de clientes y fraude en línea. Los CISOs tienen la tarea de hacer cumplir las medidas de seguridad en las aplicaciones con el fin de evitar, mitigar o reducir los riesgos que afectan la capacidad de la organización para cumplir su misión.

A este panorama de evolución de amenazas, se suman los requerimientos de manejo de auditoría, leyes y cumplimiento. Los CISOs deben crear un modelo de negocios para invertir en un programa de seguridad en aplicaciones. El modelo de negocios debería ser mapeado a las amenazas de seguridad del negocio y los programas de servicios necesarios para servir como contramedidas. La industria de la seguridad gasta en cálculos de riesgos cuantitativos y *benchmarks* para dar respaldo a la solicitud del presupuesto para invertir en seguridad.

Parte II: Criterios para gestionar riesgos de seguridad en aplicaciones

Los CISOs deben dar prioridad a los problemas de seguridad con el fin de identificar las áreas que necesitan atención primero. Para tomar decisiones con conocimiento sobre cómo gestionar riesgos de seguridad en aplicaciones, los CISOs a menudo necesitan evaluar los costos de corregir vulnerabilidades conocidas y adoptar nuevas contramedidas, además de considerar los beneficios de la mitigación de riesgos. La relación entre costos y beneficios es crucial para decidir en qué medidas de seguridad y controles en aplicaciones invertir para reducir el nivel de riesgo. Con frecuencia los CISOs deben explicar a la dirección ejecutiva los riesgos de las aplicaciones y articular el potencial impacto en el negocio de la organización, en caso que las aplicaciones sean atacadas y se produzcan filtraciones que afecten datos confidenciales. Los riesgos de seguridad pasan a ser riesgos del negocio sólo cuando existen estas tres características:

- Amenaza viable
- Vulnerabilidad que puede ser expuesta
- Activos de valor

Para priorizar sistemáticamente los riesgos relativos a la inversión, los CISOs deberían considerar una metodología de calificación de riesgos conocida como *Common Vulnerability Scoring System Version* 2.0 (CVSSv2, por sus siglas en inglés). Con el fin de ayudar a comunicar periódicamente a los ejecutivos de negocios acerca de los riesgos en las aplicaciones, los CISOs pueden considerar proveer informes de "reconocimiento sobre ciberamenazas emergentes" a la dirección ejecutiva.

Más información: http://nvd.nist.gov/

Comunicación a los ejecutivos de negocios

Los CISOs deben ser realistas con respecto a los riesgos de las ciberamenazas y presentar a la empresa la visión global de los riesgos de seguridad de la información, no sólo el cumplimiento y las vulnerabilidades, sino también los incidentes de seguridad enfocados en los activos de información de la organización, incluyendo las aplicaciones. La capacidad de comunicar los riesgos para el negocio permite a los CISOs articular el modelo de negocios inherente a la seguridad de las aplicaciones y justificar el gasto adicional en medidas de protección de tales aplicaciones. Su justificación debe tener en cuenta el impacto económico de los incidentes de seguridad en comparación con los costos de incumplimiento. Los costos actuales para el negocio debido al impacto económico de los incidentes de seguridad son mucho mayores que los costos por incumplimiento y omisión de auditorías. A menudo, la gravedad del impacto de los incidentes de seguridad puede costarle a los CISOs sus puestos de trabajo y, a la empresa, perder reputación e ingresos.

Modelado de amenazas

Con un enfoque de arriba hacia abajo para la identificación de amenazas y contramedidas, los CISOs deberían considerar una técnica de modelado de amenazas descrita en la **Parte III**. La técnica citada permite que la aplicación objetivo sea descompuesta para revelar su superficie de ataque, luego sus amenazas relevantes, contramedidas asociadas, y por último sus carencias y debilidades.

Manejo de nuevas tecnologías

En ámbitos tales como las aplicaciones móviles, la Web 2.0 y los servicios de computación en la nube, las nuevas tecnologías ofrecen diferentes amenazas y medidas de prevención. Los cambios en las aplicaciones también son una fuente de riesgos potenciales, especialmente cuando las tecnologías nuevas o diferentes se integran dentro de las aplicaciones. Dado que las mismas evolucionan ofreciendo nuevos servicios a ciudadanos, clientes y empleados, también es necesario planificar la mitigación de nuevas vulnerabilidades introducidas por la adopción y aplicación de nuevas tecnologías como dispositivos móviles, Web 2.0 y nuevos servicios tales como computación en la nube. La adopción de un *framework* de riesgo para evaluar los riesgos introducidos por las nuevas tecnologías, es esencial en la determinación de las contramedidas a tomar con el fin de mitigar estos nuevos riesgos. Esta guía proporciona orientación para los CISOs sobre cómo mitigar los riesgos de las nuevas amenazas a las aplicaciones, así como las vulnerabilidades que pueden resultar de la implementación de nuevas tecnologías.

- Aplicaciones móviles
  - Ejemplos referidos a: dispositivos perdidos o robados, software malicioso, exposición en canales de comunicación múltiple, autenticación débil.
  - Ejemplos de acciones del CISO: satisfacer las normas de seguridad en aplicaciones móviles, adaptar las auditorías de seguridad para evaluar las vulnerabilidades, aprovisionar datos de manera segura a las aplicaciones en los dispositivos personales.
- Web 2.0
  - Ejemplos referidos a: asegurar las redes sociales, gestión de contenidos, seguridad de tecnologías y servicios de terceras partes.
  - Ejemplos de acciones del CISO: APIs de seguridad, CAPTCHA, *tokens* de seguridad únicos en los formularios web y flujos de trabajo de aprobación de transacciones.
- Servicios de computación en la nube
  - Ejemplos referidos a: implementaciones multi-empresa, seguridad en implementaciones de computación en la nube, riesgo de terceras partes, filtración de datos, denegación de servicio generada por empleados internos malintencionados.
  - Ejemplos de acciones del CISO: evaluación de seguridad para computación en la nube, evaluación de auditoría y cumplimiento sobre proveedores de servicios de computación en la nube, debida diligencia, cifrado en tránsito y en almacenamiento y monitoreo.

Los agentes de amenaza actuales buscan obtener ganancias financieras derivadas de acciones tales como atacar aplicaciones para comprometer datos sensibles de los usuarios e información propietaria de la empresa con fines lucrativos, cometer fraude y obtener una ventaja competitiva (por ejemplo, a través del ciberespionaje). Para mitigar los riesgos planteados por estos agentes, es necesario determinar la exposición al riesgo, el factor de probabilidad y el impacto de estas amenazas, así como identificar el tipo de vulnerabilidades en las aplicaciones que pueden ser explotadas por tales agentes.

La explotación de algunas de estas vulnerabilidades en las aplicaciones podría afectar negativamente a la organización y poner en peligro el negocio.

Parte III: Programa de seguridad en aplicaciones

Desde el punto de vista estratégico de la gestión de riesgos, la mitigación de los riesgos de seguridad en aplicaciones no es un ejercicio a realizar solo una vez, sino que se trata de una actividad permanente que requiere prestar mucha atención a las amenazas emergentes y planificar a futuro la implementación de nuevas medidas de protección con el fin de disminuir el riesgo de estas nuevas amenazas. Esto incluye la planificación para la adopción de nuevas actividades de seguridad en aplicaciones, procesos, controles y entrenamiento. Al planificar nuevos procesos y controles de seguridad en aplicaciones, es importante para los CISOs saber en qué dominios de seguridad en aplicaciones invertir, de manera que la empresa cumpla sus misiones.

Para construir y hacer crecer un programa de seguridad en aplicaciones, los CISOs deben:

- Mapear las prioridades del negocio a las prioridades de seguridad
- Evaluar la situación actual utilizando un programa de modelo de madurez de seguridad
- Establecer el estado objetivo mediante un programa de modelo de madurez de seguridad

Mapear las prioridades del negocio a las prioridades de seguridad

Todas las prioridades de seguridad deben poder mapearse a las prioridades del negocio. Este es el primer paso para establecer la relevancia de cada iniciativa de seguridad y muestra a la gestión empresarial cómo la seguridad respalda la misión de la organización. También demuestra al personal de seguridad cómo apoya esta misión.

Evaluar el estado actual utilizando un programa de modelo de madurez de seguridad

Ingresar en la madurez de procesos es un requisito previo para la adopción de procesos de seguridad en aplicaciones y software. Uno de los criterios adoptados a menudo por las organizaciones, es considerar las capacidades de la organización en dominios de seguridad en aplicaciones y la madurez de la organización al operar en estos dominios. Ejemplos incluyen gobierno de la seguridad en aplicaciones, gestión de riesgos/vulnerabilidades, cumplimiento regulatorio e ingeniería en seguridad de aplicaciones, tal como diseñar e implementar aplicaciones seguras. Específicamente en el caso de la ingeniería en seguridad de aplicaciones, adoptar la garantía de seguridad en software es necesaria cuando no hay un control directo sobre la implementación de seguridad de este tipo de software, ya que es producido por un proveedor externo. Un factor que debe considerarse en este caso consiste en medir la garantía de la seguridad en el software usando un modelo de madurez. Un prerrequisito para la medición de la garantía de la seguridad en el software es la adopción de un S-SDLC (*Secure Software Development Lifecycle*, por sus siglas en inglés). A alto nivel, el S-SDLC consiste en introducir actividades de "seguridad integrada", además de entrenamiento y herramientas en el marco del SDLC. Ejemplos de estas actividades pueden incluir herramientas/procesos para seguridad en el software tales como modelado de amenazas/análisis de riesgos sobre la arquitectura, análisis estático de código fuente/revisión de seguridad de código, búsqueda de vulnerabilidades en aplicaciones/pruebas de seguridad en aplicaciones y programación segura para desarrolladores. En esta guía también se proporciona una referencia al modelo de madurez para la garantía de software de OWASP, así como a sus diversos proyectos dedicados a la seguridad en el software y al S-SDLC.

Establecer el estado objetivo mediante un programa de modelo de madurez de seguridad

No todas las organizaciones necesitan tener la madurez más alta. La misma debería tener un nivel que pueda gestionar el riesgo de seguridad que afecta el negocio. Obviamente, esto varía entre las organizaciones y es impulsado por el negocio, que acepta tal riesgo como parte de una colaboración y transparencia continua por parte de la organización de seguridad.

Una vez que se identifica el estado objetivo, los CISOs deberían crear una hoja de ruta que identifique su estrategia para abordar los problemas conocidos, así como la detección y mitigación de riesgos nuevos.

OWASP proporciona varios proyectos y una guía para ayudar a los CISOs a desarrollar e implementar un programa de seguridad en las aplicaciones.

Además de leer esta sección de la guía, consulte el **Apéndice B "Referencia Rápida de Guías y Proyectos OWASP",** para obtener más información sobre el tipo de actividades en el dominio de ingeniería de seguridad que pueden ser incorporadas dentro de un programa de seguridad en aplicaciones.

Parte IV: Métricas para gestionar riesgos e inversiones en seguridad en aplicaciones

Una vez que se realizan las inversiones en seguridad en aplicaciones y software, es importante para los CISOs medir e informar a la Dirección Ejecutiva sobre el estado del gobierno, riesgo y cumplimiento del programa de seguridad en las aplicaciones. Por otra parte, los CISOs deben demostrar la eficacia de las inversiones en programas de seguridad en aplicaciones y su impacto en el riesgo del negocio.

Los CISOs también necesitan métricas para gestionar y controlar a la gente, los procesos y las tecnologías que componen el programa de seguridad en las aplicaciones. También se incluyen indicadores de ejemplo para medir el gobierno, riesgo y cumplimiento de los procesos de seguridad de la aplicación.

Las métricas de seguridad constan de tres categorías:

- Métricas de procesos de seguridad en aplicaciones
- Métricas de riesgos de seguridad en aplicaciones
- Métricas de seguridad en el SDLC

Métricas de procesos de seguridad en aplicaciones

Estas apoyan a las decisiones fundamentadas para determinar dónde concentrar los esfuerzos de mitigación de riesgos y para gestionar con mayor eficacia los riesgos de la seguridad en aplicaciones. Dichas metas de gestión de riesgos determinan cuáles riesgos de seguridad en aplicaciones deben ser priorizados para ejecutarse. Por lo general son muy específicas de la organización y dependen del tipo de entidad y el sector de la industria con el que hace negocios.

- ¿Qué tan bien cumple la organización con políticas de seguridad, normas técnicas y prácticas de la industria?
- ¿Qué tan consistentemente estamos ejecutando los Acuerdos del Nivel de Servicio *(SLA - Service Level Agreement)* de seguridad? ¿Por aplicación? ¿Por departamento? ¿Por canal?

Métricas de riesgos de seguridad en aplicaciones

- Métricas de gestión de riesgos/vulnerabilidades: ¿Cuál es el tiempo medio de reparación sobre una base anual? ¿Sobre una base mensual? ¿Por aplicación? ¿Por departamento? ¿Cuáles son los problemas de seguridad conocidos en producción?
- Métricas de incidentes de seguridad: ¿Qué problemas de seguridad han sido explotados? ¿Eran problemas conocidos que fueron liberados en producción? ¿Cuál fue el costo para el negocio?
- Métricas de monitoreo de ataques y reporte de inteligencia sobre amenazas: ¿Qué aplicaciones reciben más ataques que otras? ¿Qué aplicaciones tienen picos de uso cercano al máximo esperado?

Métricas de seguridad en el SDLC

Un aspecto a menudo desatendido con respecto al gasto en seguridad es el matiz económico de tener que lidiar con software inseguro. La inversión en seguridad del software para identificar y corregir los problemas antes de liberar el software en producción realmente se paga sola, ya que ahorra dinero a la organización. La instalación de parches para corregir vulnerabilidades, con posterioridad a la liberación de las aplicaciones en producción, es muy costosa; resulta mucho más barato invertir en revisiones de seguridad de arquitectura con el fin de identificar fallas en el diseño y corregirlas antes de la programación, así como invertir en revisiones de seguridad de código para identificar y corregir errores de seguridad en el software durante la programación, y garantizar que las entregas están configurados correctamente.

- Métricas para la toma de decisiones en materia de mitigación de riesgos: ¿Cuál es el tiempo medio de reparación por categoría de riesgo de una aplicación? ¿Cumple con las expectativas? ¿Cuál es el "mapa de calor" de riesgo por aplicación? ¿Por departamento? ¿Por canal?
- Métricas para la identificación de las causas raíces que dan lugar a vulnerabilidades: ¿Cuáles son las causas raíces de vulnerabilidades en cada aplicación? ¿Hay un problema sistémico? ¿Qué prácticas de seguridad han sido mejor adoptadas por cada equipo de desarrollo? ¿Qué equipos de desarrollo necesitan más atención?
- Métricas sobre las inversiones en seguridad de software: ¿En qué fase del SDLC han identificado los mayores problemas en cuanto a seguridad? ¿Cuál es la madurez para las prácticas en seguridad correspondientes a cada fase del SDLC? ¿Qué resulta urgente en cada fase del SDLC respecto a personas, procesos y tecnología? ¿Cuál es la relación costo/beneficio comparando las pruebas de seguridad contra pruebas de penetración, descendentes o por etapas, para búsqueda de vulnerabilidades? ¿Cuáles son los costos/beneficios de identificar problemas en cada fase?

Prefacio

Esta guía ha sido apoyada por el programa de reinicio de proyectos OWASP y desarrollada en alineación a los valores principales de OWASP reflejando el carácter abierto de los contenidos, ideas y conceptos innovadores, alcance global a la comunidad de seguridad en aplicaciones y la integridad de los contenidos que se publican estrictamente neutral y sin estar sesgado a intereses comerciales específicos. Esta guía también se ha desarrollado en base a valores fundamentales de OWASP como "Promover la implementación y el cumplimiento de normas, procedimientos y controles de seguridad de aplicaciones", y los principios de OWASP de entregar contenido libre y abierto, con un enfoque basado en riesgos para la mejora de la seguridad en aplicaciones y no lucrativo. El líder del proyecto "Guía de seguridad de aplicaciones de OWASP" es Marco Morana, quien desarrolló el contenido original de esta guía con la contribución de Colin Watson, Eoin Keary, Tobias Gondrom y Stephanie Tan. Este proyecto está siendo desarrollado por OWASP en paralelo con el líder del proyecto "Encuestas para CISO" Tobias Gondrom.

El objetivo es ejecutar estos dos proyectos en sincronía y utilizar los resultados de la "Encuesta para CISO 2013" para adaptar la guía a las necesidades específicas de CISOs resaltando lo que abordan los proyectos/recursos de OWASP a dichas necesidades. La versión de Noviembre de 2013 de la "Guía de seguridad de aplicaciones OWASP para CISOs" se presentó en la conferencia AppSec 2013 de EE.UU., celebrada en la ciudad de Nueva York del 18 al 23 de noviembre de 2013.

Sobre esta versión en español

La presente versión en español fue traducida por Walter Heffel, Lucas Barbero, Franco Cian, Javier Albano, Daniel J. Fernández y German Chiovetta; editada y corregida por Mauro Gioino, Mauro Graziosi y Cristian Borghello y; publicada en marzo de 2015.

2. La Guía del CISO

Parte I: Razones para invertir en Seguridad de Aplicaciones

I-1 Resumen ejecutivo

En esta era digital, las organizaciones públicas y privadas brindan servicios a un creciente número de ciudadanos, clientes y empleados a través de aplicaciones web. Frecuentemente, estas aplicaciones proporcionan "servicios altamente confiables" a través de Internet, incluyendo funciones que conllevan un alto riesgo para el negocio. Estas aplicaciones web son el objetivo de un número cada vez mayor de estafadores y ciberdelincuentes. Muchos incidentes traen como consecuencia una denegación del acceso online, filtración de datos de clientes y fraude online.

Los jefes de seguridad de la información (CISOs) tienen la tarea de hacer cumplir las medidas de seguridad de aplicaciones para evitar, mitigar y reducir los riesgos de seguridad que afecten la capacidad de la organización para cumplir su misión. Este panorama de amenazas en evolución, impulsa aún más los requisitos de cumplimiento, de auditoría y cuestiones legales. Los CISOs deben crear un modelo de negocio para invertir en un programa de seguridad en aplicaciones. El modelo de negocio debería estar mapeado a las amenazas de seguridad que afectan al negocio y el programa de servicios necesarios para servir como contramedida. Los *benchmarks* de gastos de seguridad por industria y los cálculos de riesgos cuantitativos proveen soporte a las solicitudes de presupuesto para invertir en seguridad.

I-2 Introducción

Las aplicaciones se han vuelto cada vez más críticas en las organizaciones. A menudo, proveen servicios críticos con requisitos legales y regulatorios. Para los clientes de bancos, estas son funciones de valor que les permiten abrir cuentas bancarias, pagar cuentas, solicitar préstamos, contratar recursos y servicios, transferir fondos, negociar en bolsa de valores, ver información de cuentas, descargar el estado de cuentas bancarias, entre otros. Esta experiencia online es conveniente para las personas porque les permite realizar las mismas transacciones financieras como si estuvieran en la sucursal/oficina/punto de venta, pero con el valor agregado de llevar a cabo estas operaciones remotamente desde su ordenador personal o teléfono móvil. Al mismo tiempo, esta comodidad para los clientes representa un costo para las entidades financieras involucradas en el desarrollo y mantenimiento de estas aplicaciones. Por ejemplo, los sitios de comercio electrónico y banca online se han convertido en el objetivo de un mayor número de estafadores y cibercriminales, y las víctimas de incidentes de seguridad. Varios de estos incidentes resultaron en una denegación de acceso online, filtración de datos y fraude online.

En el caso de incidentes de filtración de datos, frecuentemente estos ataques de estafadores y cibercriminales implican la explotación de aplicaciones, como inyección SQL para comprometer los datos almacenados en la base de datos de aplicaciones y *Cross-site Scripting* para ejecutar código malicioso, como ser software malicioso sobre el navegador del usuario. Los objetivos de estos ataques son los datos y las funciones de negocio de las aplicaciones para el procesamiento de esos datos. En el caso de las aplicaciones de banca online, los datos objetivos del *hacking* y el software malicioso incluyen datos personales de individuos, datos de cuentas bancarias, datos de tarjetas de crédito y débito, credenciales online, tales como contraseñas y PINs, y por último pero no menos importante, la alteración de los datos de las transacciones financieras online, tales como transferencias de dinero para cometer fraude. El informe de investigación de Verizon en 2012 de filtración de datos identifica al *hacking* y al software malicioso como los tipos de ataques más prominentes, obteniendo contraseñas y credenciales robadas, y plantea una amenaza importante para cualquier organización que realiza negocios online.

Para hacer frente al aumento de incidentes contra las aplicaciones tal como denegación de servicios y filtraciones de datos, que a menudo son causadas por *hacking* y software malicioso, los CISOs han sido llamados por ejecutivos de empresas, como el CIO, Asesor Jurídico o CFO, para construir y hacer cumplir las medidas de seguridad de las aplicaciones para gestionar los riesgos de seguridad de la organización. Para las organizaciones financieras, por ejemplo, las crecientes amenazas para aplicaciones como ser las de *homebanking*, desafían a los CISOs a hacer cumplir los controles adicionales de seguridad de las aplicaciones y aumentar la inversión en esto para enfrentar el aumento de los riesgos.

Debido al cambiante panorama de amenazas y la creciente presión desde auditoría, legales y cumplimiento de normas y regulaciones en la última década, las inversiones en seguridad de aplicaciones han aumentado en proporción a otros rubros en los presupuestos generales de seguridad de la información y tecnologías de información. Esta tendencia también es captada por encuestas de seguridad en aplicaciones, tal como en el informe del proyecto *OWASP Security Spending Benchmarks 2009* que, por ejemplo, declaró: *"A pesar de la crisis económica, más de un cuarto de los encuestados esperan que el gasto en seguridad de aplicaciones aumente en 2009 y un 36% espera que se mantenga igual"*. Además, en la encuesta OWASP CISO 2013, alrededor del 87% de los encuestados indicó que la inversión en seguridad

de aplicaciones podría aumentar o permanecer constante. No obstante, realizar un modelo de negocio para aumentar el presupuesto para seguridad de las aplicaciones, hoy sigue siendo un desafío debido a la recesión de la economía y la priorización del gasto para el desarrollo de nuevas características de aplicaciones y plataformas (por ejemplo, dispositivos móviles), iniciativas para ampliar el consumo de servicios o la rentabilidad, y marketing para atraer a nuevos clientes y retener los existentes. En última instancia, en el tipo de recesión económica actual y en un escenario de bajo crecimiento en inversiones empresariales incluido el software integrado de las compañías, para los CISOs cada vez es más importante establecer el "modelo de negocio" para la inversión en seguridad de aplicaciones. Dado que también parece haber una desconexión entre las amenazas percibidas por la organización (las amenazas de seguridad en aplicaciones son mayores) aún el gasto en seguridad de redes e infraestructura sigue siendo mucho más alto y nos gustaría aclarar como es el impacto en el negocio de las filtraciones de datos debido a la explotación de vulnerabilidades en aplicaciones y lo costoso que podría llegar a ser para las organizaciones. Por lo general, la asignación de un presupuesto adicional para seguridad en aplicaciones incluye el desarrollo de los cambios en la aplicación para corregir las causas del incidente (por ejemplo, corrección de vulnerabilidades), así como el despliegue de medidas de seguridad adicionales, tanto controles preventivos como correctivos para mitigar los riesgos de *hacking* y software malicioso, y limitando la probabilidad y el impacto de futuros incidentes de filtración de datos.

Los CISOs pueden construir un modelo de negocios para el presupuesto adicional de seguridad en aplicaciones de hoy por diferentes razones, algunos directamente adaptados a la cultura específica de riesgos de las empresas o al apetito de riesgo, mientras que otros se adaptan a las necesidades de la seguridad en aplicaciones. Algunas de estas necesidades pueden ser identificadas por el análisis de los resultados de las encuestas. Para evaluar estas necesidades, se invita a los lectores de esta guía a participar en la Encuesta para CISOs de OWASP para que el contenido se pueda adaptar a las necesidades de los CISOs que participan de dicha encuesta.

Encuesta para CISOs sobre Seguridad en Aplicaciones: Enfoque creciente

Una mayor percepción del riesgo debido a las amenazas dirigidas a las aplicaciones, desplaza la inversión de la organización en seguridad de red tradicional a la seguridad en aplicaciones. En comparación al presupuesto anual de la compañía para seguridad en aplicaciones:

- ~ 47% de los CISOs han visto un aumento.
- ~ 39% lo considera relativamente constante.
- ~ 13% han visto una disminución.

El presupuesto para las medidas de seguridad en aplicaciones puede depender de diferentes factores, tales como el cumplimiento de políticas y normas de seguridad, gestión de riesgos operativos incluyendo los riesgos debido a las vulnerabilidades de las aplicaciones y la respuesta a incidentes de seguridad relacionados con las aplicaciones. Para el caso de la presente guía nos centraremos en las siguientes áreas para orientar el gasto en seguridad en aplicaciones:

- El cumplimiento de las normas de seguridad, políticas de seguridad y regulaciones
- La detección y corrección de las vulnerabilidades en las aplicaciones
- La implementación de contramedidas contra las amenazas emergentes dirigidas a aplicaciones

Sin embargo, suponiendo que los casos de negocio se pueden hacer para acompañar estos objetivos, todavía hoy los CISOs tienen la difícil tarea de determinar "cuánto" dinero debe gastar la empresa para la seguridad en aplicaciones y "dónde", es decir, en qué "medidas de seguridad" gastarlo. Respecto al "cuánto", a menudo proviene de lo que se necesita invertir para satisfacer los requisitos de cumplimiento y pasar la revisión del auditor. Cuando el enfoque es el cumplimiento, el foco es desarrollar e implementar normas de seguridad en las aplicaciones y asignar estos requisitos de seguridad para los proyectos en curso. Cuando el foco es la gestión de riesgos de la vulnerabilidad, el objetivo principal es el de corregir las vulnerabilidades de alto riesgo y reducir el riesgo residual a un valor aceptable para el negocio. Cuando el foco es la gestión de incidentes, el enfoque es cómo investigar y analizar las brechas de seguridad sospechosas y recomendar acciones correctivas. Cuando el foco es la concientización de seguridad en aplicaciones, la atención se centra en instituir el entrenamiento al personal en seguridad de aplicaciones.

Para los CISOs de hoy en día, existe una mayor concentración en la toma de decisiones para la reducción de riesgos. Tanto para la mitigación de los riesgos reales (por ejemplo, los incidentes, los *exploits* de vulnerabilidades) como para la disminución de los riesgos por incumplimiento (por ejemplo, en caso de incumplimientos legales), la pregunta para los CISO es "dónde" y "cómo" priorizar el gasto del presupuesto de seguridad en aplicaciones. A menudo, la pregunta es qué contramedida, proceso de seguridad de las aplicaciones, actividad o herramienta de seguridad entrega "más valor por el mismo dinero" para la organización. Con respecto al "dónde", todo se reduce a equilibrar correctamente los diferentes dominios de seguridad de aplicaciones y riesgos (por nombrar los más importantes: gobierno empresarial, gestión de riesgos de seguridad, gestión operativa (que incluye la seguridad de red, gestión de identidades, control de acceso y gestión de incidentes). Dado que, como disciplina, la seguridad en aplicaciones abarca todos estos dominios, es importante tener en cuenta a todos ellos y observar la inversión en seguridad en aplicaciones desde diferentes perspectivas.

I-3 Estándares de Seguridad de la Información, Políticas y Cumplimiento

Identificar estándares, políticas y otros mandatos en el cumplimiento de las normas

Uno de los principales factores para la financiación de un programa de seguridad en aplicaciones, es el cumplimiento de las normas de seguridad de la información, políticas y reglamentos establecidos por las normas aplicables de la industria de organismos reguladores. Inicialmente, es importante que el CISO defina lo que está al alcance del cumplimiento y cómo afecta a la seguridad en aplicaciones. Dependiendo del sector industrial y la ubicación geográfica en la que opera la organización, habrá varios diferentes tipos de requerimientos de seguridad que la organización necesita cumplir. El impacto de estos requerimientos también se encuentra en las aplicaciones que gestionan y procesan datos cuya seguridad cae bajo el alcance de aplicación de estas normas y reglamentos. El impacto sobre las aplicaciones consiste en la realización de una evaluación de riesgos programada e informar sobre el estado de cumplimiento a los auditores.

Los ejemplos de estándares de seguridad de datos y privacidad que se aplican a las aplicaciones en EE.UU. incluyen:

- *Payment Card Industry (PCI) Data Security Standard (DSS)* para los comerciantes de tarjetas de crédito y procesadores.
- Directrices del FFIEC para las organizaciones financieras, cuyas aplicaciones le permiten a los clientes y consumidores realizar operaciones bancarias en línea, realizar transacciones como pagos y transferencias de dinero.
- Ley FISMA para agencias federales gubernamentales, cuyos sistemas y aplicaciones necesitan proporcionar seguridad de la información para sus operaciones y activos.
- Ley HIPAA para proteger la privacidad de los datos de salud cuyas aplicaciones manejan los registros de pacientes en la industria de salud.
- Ley GLBA para las instituciones financieras cuyas aplicaciones recolectan y almacenan información financiera personal de los individuos.
- Las leyes de divulgación de filtración de datos para las organizaciones cuyas aplicaciones almacenan y procesan Información Personal de Identificación (PII) de residentes cuando estos datos se pierden o son robados en texto plano (por ejemplo, sin cifrar).
- Las reglas de privacidad FTC para las organizaciones cuyas aplicaciones manejan información privada de los consumidores, así como también cuando se opera en países de la UE para cumplir con las reglas de “puerto seguro”.

OWASP proporciona varios proyectos y una guía para los CISOs para ayudar a desarrollar e implementar políticas, normas y directrices para la seguridad en aplicaciones. Por favor, para más información consulte el Apéndice B.

Capturando requerimientos de seguridad en aplicaciones

PCI-DSS

La mayoría de las aplicaciones que llevan a cabo operaciones de pago, como ser las aplicaciones de comercio electrónico (*e-commerce*) que manejan datos de titulares de tarjetas de crédito están obligados

a cumplir con el Estándar de Seguridad de Datos para la Industria de Pagos con Tarjetas - *Payment Card Industry (PCI) Data Security Standard (DSS)*. Los requisitos para la protección de los datos de los titulares de tarjetas cuando son almacenados por una aplicación, incluye varios requisitos de PCI-DSS, como presentación o cifrado del número de cuenta primario *(PAN – Primary Account Number)* y el enmascaramiento del PAN cuando es mostrado. El requisito de PCI-DSS para los datos de autenticación de las tarjetas, como el PIN, CVC2/CVV2/CIDs, es no guardar estos datos, ni siquiera cifrados después de que el pago haya sido autorizado. Los datos de los titulares de tarjetas de crédito deben ser protegidos con cifrado cuando se transmiten a través de redes abiertas. Estos requisitos para la protección de los números de las cuentas personales de los titulares de tarjetas y los datos de autenticación, motivan al CISO a documentar los requisitos de seguridad internos para cumplir con estas disposiciones y adoptar las medidas de seguridad de aplicaciones y evaluaciones para verificar que estos requisitos se cumplan por las aplicaciones que están en su alcance. Además de la protección de los datos de titulares de tarjetas, PCI-DSS tiene disposiciones para el desarrollo y mantenimiento de sistemas y aplicaciones seguras, para las pruebas de seguridad de sistemas y procesos, y para las pruebas de aplicaciones en busca de vulnerabilidades comunes, como las que se definen en el OWASP Top Ten.

La necesidad del cumplimiento de los requisitos de PCI-DSS pueden ser una razón para justificar una inversión adicional en tecnología y servicios para pruebas de seguridad en aplicaciones: los ejemplos incluyen revisiones de seguridad del código fuente con evaluaciones/herramientas utilizando Pruebas de Seguridad de Análisis Estático *(SAST - Static Application Security Testing),* y revisiones de seguridad en aplicaciones con Pruebas de Seguridad de Análisis Dinámico *(DAST - Dynamic Analysis Security Testing)*. Para un comerciante que desarrolla y mantiene una aplicación web como un sitio de comercio electrónico (*e-commerce*) que maneja pagos con tarjetas de crédito, la cuestión principal es determinar si se debe asignar presupuesto para cumplir con las medidas y actividades de seguridad en aplicaciones para cumplir con PCI-DSS o para incurrir en multas (por ejemplo, hasta U$D 500.000 cuando los datos de titulares de tarjetas de crédito se pierden o son robados). Desde este punto de vista, el incumplimiento legal de las regulaciones y las normas podría ser considerado como otro riesgo para la organización y como cualquier otro riesgo, ya que puede ser mitigado, transferido o aceptado. Si se acepta el riesgo de incumplimiento, el CISO debería considerar que el riesgo de filtración de datos, debido a no implementar controles básicos de seguridad como el cifrado de datos o las validaciones de entrada, puede ser mucho más alto que el riesgo por incumplimiento.

Más información: https://www.pcisecuritystandards.org/

Ejemplo: el incumplimiento de T.J.Maxx con PCI-DSS

T.J.Maxx no cumplía con PCI-DSS cuando fueron comprometidos 94 millones de números de tarjetas de crédito en una filtración de datos. Sin embargo, los costos de incumplimiento por no cifrar o truncar los números de tarjetas y remediar las vulnerabilidades en las aplicaciones, tales como inyección SQL, fueron menores a los costos totales incurridos por el impacto en el negocio debido a este incidente de seguridad. En el caso de este incidente de filtración de datos de tarjetas de crédito a T.J.Maxx, los costos económicos incurridos a causa del mismo fue un factor por lo menos mil veces más alto (si no más) que los costos del no cumplimiento con PCI-DSS: cientos de millones de dólares vs cientos de miles de dólares.

FFIEC

En el sector bancario de EE.UU., las aplicaciones que manejan información sensible de sus clientes y se les permite procesar transacciones financieras, tales como transferencias de dinero entre diferentes cuentas bancarias (por ejemplo, cables electrónicos) deben cumplir con las directrices para la autenticación online del Examen del Consejo Federal de Instituciones Financieras (*FFIEC - Federal Financial Institutions Examination Council's*). Los requisitos incluyen autenticación fuerte como la autenticación de factores múltiples (MFA).

Más información: http://www.ffiec.gov/

Los conductores de negocios para la inversión de seguridad en aplicaciones

Los requisitos para la autenticación del Examen del Consejo Federal de Instituciones Financieras (FFIEC) de los sitios de banca en línea pueden justificar el presupuesto de las medidas de seguridad para asegurar el diseño, la implementación y las pruebas de las prestaciones de controles de MFA en las aplicaciones.

GLBA

Para los consumidores estadounidenses, la privacidad está regulada por diversas leyes y reglamentos dependiendo del sector de la industria. En los sectores financieros de Estados Unidos, las leyes que rigen a los consumidores, incluyen las leyes de privacidad GLBA *(Gramm–Leach–Bliley Act)* y las reglas de FTC *(Federal Trade Commission).* Desde una perspectiva de cumplimiento de GLBA, las aplicaciones financieras deben proporcionar una descripción a los usuarios de aplicaciones de cómo es recogida, procesada y almacenada la PII (información de identificación personal), y cómo se comparte entre las instituciones financieras, incluyendo afiliados y terceras partes. Desde el punto de vista del cumplimiento de la FTC, las organizaciones que almacenan información de identificación personal de consumidores tienen que revelar sus prácticas de seguridad de diligencia debida a los consumidores y pueden ser considerados responsables cuando tales prácticas no se siguen como es el caso de una filtración de información privada de los consumidores y en una clara violación de los acuerdos de licencia con los consumidores. Debido a las leyes de privacidad de los EE.UU. en su mayoría los consumidores requieren reconocer cómo están protegidos los datos personales, el impacto de seguridad se limita a notificaciones, reconocimientos y controles de "exclusión". Las excepciones son los casos en los que los controles de privacidad son implementados como la configuración de privacidad de la aplicación (por ejemplo, como el caso de Facebook), y ofrecen preferencias a los usuarios como el "controles de inclusión" para cumplir con las reglas de puerto seguro de la FTC.

Más información: www.ftc.gov/ - http://en.wikipedia.org/wiki/Gramm–Leach–Bliley_Act

Leyes de privacidad

En general, las aplicaciones que almacenan y procesan datos que son considerados personales y privados, por las leyes de privacidad específicas de cada país, deben proteger cuando se almacenan o procesan éstos. Lo que se considera información privada varía país a país. Para los países que forman parte de la Unión Europea (UE) por ejemplo, los datos personales se definen en la Directiva de la UE 95/46/EC, a efectos de la Directiva: el artículo 2a: "datos personales": es toda información relativa a una persona física

identificada o identificable ("dato del sujeto"); una persona identificable es aquella que puede determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o más factores específicos de su identidad física, fisiológica, psíquica, económica, identidad cultural o social".

Para la mayoría de los estados de EE.UU., la protección de la Información de Identificación Personal (PII por sus siglas en Inglés) es impulsada por las leyes de notificación de filtración de datos como *California Security Breach Information Act (SB-1386)* donde la PII está definida más estrictamente que en la directiva de la UE, como el primer nombre de la persona o la primera inicial y el apellido combinado con uno o más de los siguientes elementos cuando el nombre o los elementos de datos no están cifrados: (1) Número del Seguro Social. (2) Número de licencia de conducir o el número de la tarjeta de identificación del estado. (3) Número de cuenta, de la tarjeta de crédito o débito, en combinación con cualquier código de seguridad requerido, código de acceso o contraseña que le permitirá el acceso a la cuenta financiera del individuo. Para efectos de estas leyes, la "información personal" no incluye la información disponible públicamente que está legalmente a disposición del público en general desde los gobiernos federales, estatales o registros del gobierno local.

Las aplicaciones que procesan y almacenan datos que se consideran personales y privados por las leyes de privacidad de la UE o las leyes de notificación de filtración de datos de la PII de los estados de EE.UU., necesitan implementar controles de seguridad tales como autenticación, autorización, cifrado, *logging* y auditoría para proteger la confidencialidad, disponibilidad e integridad de estos datos. Estos requisitos de seguridad de la información son típicamente parte de la política de seguridad de la información aplicada por la organización. Estos requisitos de seguridad, se traducen indirectamente en los requisitos de seguridad para las aplicaciones que almacenan y procesan datos que sean considerados confidenciales o información de identificación personal confidencial. Presupuestos para el programa de seguridad en aplicaciones para cumplir con los requisitos de privacidad de datos personales y de consumidores son justificables tanto como para cumplimiento interno de la política de seguridad de la información, así como también para mitigar los daños a la reputación de la organización en el caso de que estos datos sean perdidos o comprometidos. Además de dañar la reputación, las organizaciones podrían incurrir en multas regulatorias y costos legales a causa de incumplimiento de leyes de privacidad locales.

Más información:

Directiva de la UE 95/46/EC - http://www.sb-1386.com/ - http://j.mp/1vSYra4 [PDF]

I-4 Gestión de riesgos

La gestión de riesgos es sin duda una de las funciones básicas de un CISO. El propósito de esta sección de la guía es ayudar a los CISOs a desarrollar, articular y poner en práctica un proceso de gestión de riesgos. OWASP también proporciona guías de documentación que le pueden ser útiles a los CISOs para implementar una estrategia de gestión de riesgos para las aplicaciones. Después de leer esta sección, consulte el Apéndice B para tener una referencia a las guías y proyectos de OWASP.

Gestión de riesgos proactiva vs reactiva

La **gestión de riesgos proactiva** consiste en enfocarse en la mitigación de riesgos de eventos de amenazas antes de que éstas posiblemente podrían ocurrir y afectar negativamente a la organización. Las organizaciones, cuyo objetivo es la gestión proactiva de riesgos, planean proteger los activos críticos a la misión, incluyendo las aplicaciones antes que las amenazas potenciales apunten a ellas. Las actividades de mitigación de riesgos proactivas para aplicaciones incluyen centrarse en la información sobre amenazas para aprender de los agentes; modelado de amenazas para aprender cómo la aplicación puede ser protegida contra ataques; pruebas de seguridad y corrección de posibles vulnerabilidades en la aplicación, así como en el código fuente, antes de que éstas puedan ser explotadas por potenciales atacantes.

Un pre-requisito para la gestión proactiva de riesgos es tener un inventario de las aplicaciones de misión crítica con perfiles de riesgos asociados que permitan a los CISOs identificar activos digitales críticos, tales como datos y funciones que deben ser priorizadas y planificadas para las actividades de mitigación de riesgos proactiva. Los CISOs cuyas organizaciones se centran en las medidas de mitigación proactivas han adoptado por lo general una estrategia de mitigación de riesgos y actúan sobre la información de inteligencia de amenazas, eventos de seguridad monitoreados y alertas para elevar el nivel de riesgos técnico y de negocio aceptables. Los CISOs que orientan sus esfuerzos a la mitigación de riesgos proactiva, por lo general requieren el despliegue de medidas adicionales con antelación a las nuevas amenazas y nuevos requisitos de cumplimiento.

La **gestión de riesgos reactiva** consiste en responder a los eventos de riesgo a medida que van ocurriendo para mitigar los impactos negativos en la organización. Algunos ejemplos de actividades de gestión de riesgos reactiva incluye la respuesta a incidentes de seguridad, investigaciones de incidentes de seguridad y análisis forenses, y la gestión del fraude. Para el caso de seguridad en aplicaciones, las actividades de gestión de riesgos reactiva incluyen la gestión de parches para vulnerabilidades, reparación de vulnerabilidades detectadas en las aplicaciones en respuesta a incidentes de seguridad o cuando éstos son identificados por terceras partes, evaluación de riesgos en la aplicación debido a requerimientos puntuales (no planificados) para satisfacer cumplimientos específicos y requisitos de auditoría. Los CISOs cuyas organizaciones se centran en la gestión de riesgos reactiva suelen poner más énfasis en responder a eventos de gestión de riesgos no planificados. A menudo, el enfoque de la gestión de riesgos reactiva es "la contención de daños" para "detener la hemorragia" y se pone menos atención a la planificación para la mitigación de riesgos futuros de posibles eventos negativos dirigidos a las aplicaciones. Típicamente, en las organizaciones cuya atención se centra en la gestión de riesgos reactiva, los CISOs tienden a pasar la mayor parte de su tiempo en la gestión y respuesta a incidentes, y a la remediación de vulnerabilidades en las aplicaciones, tanto las que están por liberarse en producción o parchear las que ya se liberaron. Cuando

el foco principal de la función del CISO es la gestión de riesgos reactiva, es importante reconocer que la mitigación de riesgos reactiva, incluso si esta no siempre se puede evitar debido a que los incidentes de seguridad ocurren, no es rentable ya que el costo de las remediaciones después de que hayan sido informadas o explotadas por un atacante es varios factores de magnitud superior a la identificación y la corrección de la misma mediante la adopción de medidas de mitigación de riesgos preventiva.

Un enfoque de mitigación de riesgos proactivo es preferible a un enfoque de mitigación de riesgos reactivo cuando se hace el caso de negocio para la seguridad en aplicaciones. Un enfoque de mitigación de riesgos proactivo podría consistir en utilizar la oportunidad de una actualización de la tecnología necesaria de una aplicación para introducir nuevas funcionalidades o cuando una aplicación antigua llega al final de su vida, y tiene que migrar a un sistema/plataforma más nueva. El diseño de nuevas características para las aplicaciones representa una oportunidad para los CISOs para exigir la actualización de tecnología de seguridad a las nuevas normas y poner en práctica las medidas de seguridad más fuertes.

La gestión del riesgo centrada en activos

Los CISOs cuyas políticas de seguridad de la información son derivadas del cumplimiento de las normas de seguridad de la información, tales como ISO 17799/ISO 27001, incluyen la gestión de activos como uno de los dominios de seguridad que deben ser cubiertos. En el caso que estos activos incluyan a las aplicaciones, la gestión de activos requiere un inventario de las aplicaciones gestionadas por la organización con el fin de aplicar un enfoque de gestión de riesgos. Este inventario incluye información sobre el tipo de aplicaciones, el perfil de riesgos para cada aplicación, el tipo de datos que se almacena y procesa, los requisitos para implementar parches y las evaluaciones de seguridad, tales como las pruebas de penetración que sean requeridas. Este inventario también es fundamental para realizar un seguimiento de las evaluaciones de seguridad y los procesos de gestión de riesgos realizados a las aplicaciones, las vulnerabilidades que se han identificado y corregidas, así como también los que todavía están abiertas para ser remediadas. El perfil de riesgo que se asigna a cada aplicación también se puede almacenar en la herramienta de inventario de aplicaciones: en función del riesgo inherente de la aplicación que depende de la clasificación de los datos y el tipo de funciones que ofrece la aplicación, es posible planificar la gestión de riesgos y la priorización para la mitigación de las vulnerabilidades existentes, así como también la planificación para futuras evaluaciones de vulnerabilidades y actividades para la evaluación de la seguridad en las aplicaciones. Una de las actividades de seguridad en aplicaciones que toman ventaja de la gestión de riesgos centrada en activos es el modelado de amenazas. Desde la perspectiva de la arquitectura, los activos se componen de varios componentes, tales como servidores de aplicaciones, softwares de aplicación, bases de datos e información sensible. A través del modelado de amenazas de aplicaciones, es posible identificar las amenazas y contramedidas para las amenazas que afectan a cada activo. Los CISOs cuya atención se centra en la gestión de riesgos en los activos, deben considerar la implementación de un modelado de amenazas como seguridad proactiva y actividades de gestión de riesgos centrada en los activos.

Gestión de riesgos de negocios vs Gestión de riesgos técnicos

Al decidir la forma de mitigar los riesgos de seguridad en las aplicaciones, es importante hacer un equilibrio entre los riesgos técnicos y los riesgos de negocio. Los **riesgos técnicos** son los riesgos de

cualquier vulnerabilidad técnica o brechas de control en una aplicación cuya explotación podría causar un impacto técnico como por ejemplo, la pérdida y compromiso de datos, compromiso de servidores/hosts, accesos no autorizados a los datos y funciones de una aplicación, la denegación o interrupción de servicios, etc. Los riesgos técnicos se pueden medir como el impacto en la confidencialidad, integridad y disponibilidad de los activos, causada por un evento/causa técnica, tales como vulnerabilidades identificadas mediante una evaluación de seguridad. La gestión de estos riesgos típicamente depende del tipo de vulnerabilidad y la calificación de riesgo asignado al mismo, y también se hace referencia como "la gravedad" de una vulnerabilidad. La gravedad de una vulnerabilidad se puede calcular sobre la base de métodos de calificación de riesgos, como CVSS de FIRST, mientras que el tipo de vulnerabilidad puede ser clasificado en base al grupo en el que cae la vulnerabilidad tal como el uso de CWE de MITRE. Los CISOs pueden usar la puntuación de riesgos de una vulnerabilidad ALTA, por ejemplo, para dar prioridad a dicha vulnerabilidad para la mitigación antes de las vulnerabilidades que se califican con un riesgo MEDIO o BAJO. Al tomar esta decisión de gestión de riesgos técnica de vulnerabilidades, los CISOs no tendrán en cuenta el impacto económico de la vulnerabilidad para el negocio, tal como el caso del valor de los activos afectados por la vulnerabilidad los cuales son perdidos o comprometidos.

Más información: https://www.first.org/cvss/cvss-guide - http://cwe.mitre.org/

La **gestión de riesgos de negocios** ocurre cuando el valor del activo se tiene en cuenta para determinar el impacto a la organización. Esto requiere la asociación de riesgos técnicos de vulnerabilidades con el valor de los activos para cuantificar el riesgo. El riesgo se puede factorizar como la probabilidad que el activo esté en peligro y el impacto en el negocio causado por la explotación de la vulnerabilidad.

Por ejemplo, en el caso que una vulnerabilidad técnica de alto riesgo se explote, como ser la inyección SQL (es completamente asumido, 100% expuesto como un problema en la pre-autenticación), el impacto en el negocio se puede determinar como el impacto a un activo, como ser los datos, que se clasifican como información confidencial y si son comprometidos su valor se estima como U$D 250/registro (por ejemplo, en base a estimaciones de costos de incidentes internos o reportes de estimaciones publicados). Por tanto, el valor agregado de los datos sensibles de 100.000 registros almacenados en una base de datos que podrían ser explotados por inyección SQL, es U$D 25 millones. Si la probabilidad que sean comprometidos datos sensibles debido a la explotación de una vulnerabilidad con inyección SQL se calcula como el 10% (1 incidente exitoso de filtración de datos causado por inyección SQL cada diez años), el impacto potencial económico es una pérdida de U$D 2.500.000. Sobre la base de estas estimaciones, es posible calcular cuánto es el presupuesto para las medidas de seguridad (por ejemplo, en controles de detección y prevención) para la mitigación de riesgos para el negocio.

Cabe señalar que la estimación de riesgos de negocio es mucho más difícil que la estimación de riesgos técnicos ya que las estimaciones de los primeros requieren estimaciones de la probabilidad de determinados tipos de incidentes de seguridad (por ejemplo, violaciones de datos), así como las estimaciones de las pérdidas económicas (por ejemplo, pérdida de ingresos, costos legales de cumplimiento, costos por la reparación de la causa del incidente) que resultan de tal incidente. Normalmente estas estimaciones no son fáciles de hacer en ausencia de datos específicos y herramientas de cálculo que puedan factorizar la frecuencia de incidentes de seguridad por violaciones de datos y el mantenimiento de registros de costos directos e indirectos sufridos por la organización como resultado de

estos incidentes. Sin embargo, los datos estadísticos, las estimaciones de los costos, así como también los cálculos de riesgos cuantitativos de incidentes de filtración de datos, pueden ayudar.

El **Apéndice A "Valor de los datos y costo de un incidente"** proporciona ejemplos, formulaciones y calculadoras online para ayudar a los CISOs a asignar un valor económico a los activos de información y determinar el impacto económico para la organización en el caso que tales activos se pierdan a causa de un incidente de seguridad. El propósito de estos cálculos de riesgos cuantitativos es ayudar a los CISOs a decidir cuánto es razonable gastar en medidas de seguridad de aplicaciones para reducir los impactos en el negocio de la organización en el caso de un incidente de filtración de datos.

Estrategias de Gestión de Riesgos

Una vez que los riesgos de seguridad se han identificado y asignado un valor cualitativo como ser riesgo alto, medio y bajo, el siguiente paso para el CISO es determinar qué hacer con ese riesgo. Para decidir "qué hacer con los riesgos" los CISOs generalmente dependen de los procesos de gestión de riesgos de su organización y la estrategia de mitigación de riesgos. Los procesos de gestión de riesgos son generalmente diferentes para cada tipo de organización. A alto nivel, la gestión del riesgo depende de la estrategia de mitigación de riesgos que es adoptada por la organización. En función de la evaluación del nivel de impacto de los riesgos y la probabilidad, por ejemplo, una organización puede decidir aceptar los riesgos que por su probabilidad e impacto son bajos, mitigar o reducir los riesgos (por ejemplo, mediante la aplicación de medidas de seguridad) que tienen alta probabilidad y bajo impacto, transferir o compartir los riesgos (por ejemplo, para con un tercero, por medio de acuerdos contractuales) que son de baja probabilidad y alto impacto, y evitar los riesgos (por ejemplo, no implementar funciones de alto riesgo, por no adoptar tecnologías de alto riesgo) que tienen una alta probabilidad e impacto. Un ejemplo visual de esta estrategia de mitigación de riesgos factorizada por la probabilidad y el impacto de eventos se muestra en el siguiente diagrama:

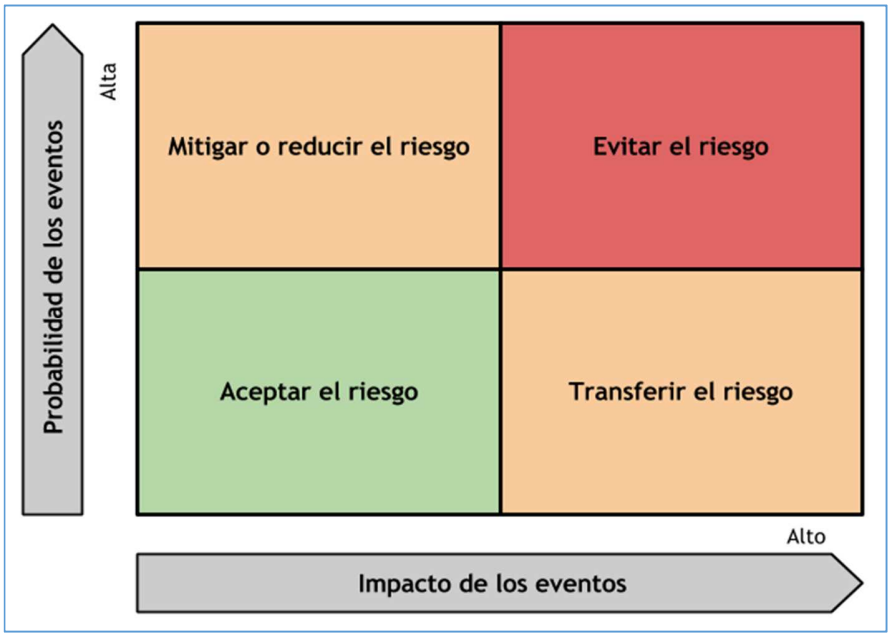

Figura 1 - Mitigación de riesgos - Estrategia basada en la Probabilidad de ocurrencia de un evento y el Impacto

En el caso que los riesgos calificados como altos no se puedan evitar debido a decisiones de negocios que se requieren para mitigarlos, y no puedan ser transferidos a terceros por medio de acuerdos contractuales y seguros, una posible estrategia de riesgos de la organización podría ser mitigar todos los riesgos que son medios y altos, y aceptar (por ejemplo, no hacer nada) sólo aquellos cuyos riesgos residuales son bajos (por ejemplo, el riesgo remanente después de que medidas o controles compensatorios son aplicados o considerados). Las estrategias de mitigación de riesgos también pueden factorizar los riesgos del negocio mediante el análisis de riesgos cualitativo que factoriza riesgos, como la probabilidad y los impactos económicos.

Una vez que el riesgo se ha determinado, el siguiente paso para la organización es decidir qué riesgos está dispuesta a aceptar, mitigar, transferir o evitar. Para los riesgos que la organización está dispuesta a aceptar es importante que los CISOs tengan un proceso de aceptación del riesgo que califique el nivel de riesgo bajo en base a la presencia de controles compensatorios que puede ser firmado por él y la dirección ejecutiva. Para los riesgos que son elegidos para mitigarlos, es importante determinar qué medidas de seguridad/acciones correctivas se consideran aceptables por la organización y decidir cuál de estas medidas son más eficaces en la reducción de riesgos, minimizando los costos (por ejemplo, mayor beneficio vs los costos totales de medidas mínimas de seguridad). Aquí es donde la estrategia de mitigación de riesgos debe tener en cuenta el costo de los incidentes de seguridad potenciales, como violaciones de datos, para decidir qué presupuesto es razonable para que la organización realice inversiones en medidas de seguridad en la aplicación. Un aspecto importante de la estrategia de riesgos para los CISOs es decidir qué medidas de seguridad funcionan mejor juntas como *"pluribus unum"* (de muchos, uno), que incluye la aplicación de controles preventivos y detectivos para proporcionar defensa en profundidad de los activos de la aplicación. Por último, para los riesgos que se transfieren o comparten con un tercero, es importante para el CISO trabajar con el área de Legales para asegurarse que las cláusulas de responsabilidad de riesgos estén documentados en los acuerdos legales y que los acuerdos de licencia de servicios son firmados por la organización con la entidad legal del proveedor de servicios.

El análisis y el conocimiento de las nuevas amenazas

Hacer el caso de negocio para gastos adicionales en medidas de seguridad de la aplicación no siempre es justificable sin datos sobre riesgos a partir del análisis del impacto de las amenazas emergentes y el aumento del nivel de riesgo que debe ser mitigado. El análisis de datos sobre amenazas permite tomar decisiones de gestión de riesgos con conocimiento de causa. En ausencia de estos datos, la gestión se queda con consideraciones subjetivas sobre las amenazas.

Las consideraciones subjetivas sobre las amenazas son a menudo decisiones basadas en el miedo, incertidumbre y duda (FUD del inglés). Actuando según FUD para mitigar los riesgos que plantean las amenazas emergentes tardío y poco efectivo. Algunas acciones de ejemplo basadas en FUD incluyen, pero no se limitan a:

- El temor a las violaciones de datos
- El temor a fallar en la auditoría y cumplimiento
- La incertidumbre con respecto a las amenazas del negocio

- Las dudas sobre la eficacia de las medidas de seguridad existentes a la luz de los recientes incidentes de seguridad

La intención de esta parte de la guía, es ayudar a los CISOs a crear un caso de negocio adicional para la inversión en seguridad de aplicaciones basado en un análisis de amenazas objetivo en lugar de consideraciones subjetivas. Desde una perspectiva de cumplimiento de normas, las consideraciones objetivas se basan en una justificación para invertir en seguridad de aplicaciones que incluye el cumplimiento de las nuevas normas de seguridad y regulaciones que afectan a las aplicaciones. Desde una perspectiva de análisis de amenazas, las consideraciones objetivas se basan en datos sobre el impacto en el negocio de los agentes de amenaza emergentes que intentan comprometer las aplicaciones para obtener ganancias financieras. Específicamente en cuanto a hacer el caso para mitigación de riesgos, es necesario que los CISOs eviten suposiciones y respalden el modelo con datos, tales como informes y análisis de ciberamenazas e incidentes de seguridad, costos de las violaciones de datos para estimar las responsabilidades y cálculos cuantitativos de riesgos según estimaciones de probabilidad e impactos. Basado en los cálculos de riesgos y las estimaciones de costos de filtración de datos, es posible que el CISO exprese cuánto debe invertir la organización en seguridad de aplicaciones y determinar en qué medidas concretas invertir.

Desde una perspectiva de temor, es cierto que los CISOs también pueden aprovechar el momento, ya sea un evento negativo o positivo, pero esto es parte de un enfoque de gestión de riesgos reactiva y baja madurez en el control de riesgos. A menudo, el gasto en seguridad de aplicaciones puede ser desencadenado por un evento negativo, como un incidente de seguridad, ya que esto cambia la percepción de la alta gerencia sobre los riesgos. Sin embargo, los CISOs deberían encontrar que el uso de una hoja de ruta de uno a dos años para impulsar la inversión en seguridad sería más eficaz, tal como se encuentra en la Encuesta para CISOs de OWASP del 2013.

La inversión en seguridad es...	3 meses	6 meses	1 año	2 años	3 años	+5 años	Total General
Decreciente	1.69%	3.39%	5.08%	1.69%	3.39%	3.39%	18.64%
Creciente en % del total de gastos	3.39%	1.69%	18.64%	16.95%	3.39%	0.00%	44.07%
Relativamente constante	5.08%	3.39%	11.86%	10.17%	3.39%	3.39%	37.29%
Total General	10.17%	8.47%	35.59%	28.81%	10.17%	6.78%	100.00%

Figura 2 - Análisis de soporte en la inversión de seguridad

En este caso, el dinero es probable que ya se gaste para limitar el daño, como para remediar el incidente e implementar contramedidas adicionales. La pregunta principal es si una mayor inversión en seguridad de aplicaciones reducirá la probabilidad y el impacto de otro incidente similar que ocurra en el futuro. Un enfoque consiste en centrarse en las aplicaciones que podrían convertirse en un blanco para los futuros ataques.

Responder a las expectativas del negocio después de un incidente de seguridad

La implementación de un proceso de respuesta a incidentes de seguridad es una actividad esencial para todos los CISOs. Tal proceso requiere la identificación de un punto de contacto para las cuestiones de seguridad, la adopción de un proceso de divulgación de problemas de seguridad y la creación de un equipo/s informal de respuesta a dichos incidentes. En el caso que ocurra un incidente de seguridad, los CISOs a menudo se encargan de llevar a cabo el análisis de la causa raíz de los incidentes, recopilar métricas por incidente y recomendar acciones correctivas. El Apéndice B le proporciona al CISO una referencia rápida a las guías y proyectos de OWASP para ayudarlos a investigar y analizar incidentes, sospechosos o reales, de seguridad en aplicaciones y recomendar acciones correctivas.

Una vez que las causas raíces del incidente han sido identificadas y se han tomado medidas correctivas para contener el impacto del incidente, la cuestión principal para los CISOs es, qué debe hacerse para prevenir la ocurrencia en el futuro de incidentes de seguridad similares. Si una aplicación ha sido el objetivo de ataque y se han perdido o comprometido datos sensibles, la cuestión principal es determinar si aplicaciones y softwares similares, también pueden correr riesgo de ataques e incidentes parecidos en el futuro. La pregunta principal para el CISO es qué medidas y actividades de seguridad en aplicaciones deben ser seleccionadas para gastar en mitigar los riesgos de filtración de datos sensibles debido a *malware* y ataques de terceros, a aplicaciones y software desarrollados y gestionados por la organización.

Después que se seleccionen estas medidas, la siguiente pregunta es cuánto se debe gastar en contramedidas. Desde la perspectiva costos vs beneficios, el gasto en seguridad en aplicaciones correspondiente a todos los costos de impacto en el negocio por una posible filtración de datos no es justificable, ya que a la empresa le costará tanto como no hacer nada, por lo tanto, sin riesgos no hay beneficios para invertir en contramedidas. Por lo tanto, la cuestión principal para los CISOs es, cuánto se debe gastar para reducir el riesgo de un incidente de filtración de datos en una fracción del costo de la implementación de una medida de seguridad: si no es 100%, el 50%, 25% o 10% de todas las posibles pérdidas monetarias. Además, ¿cómo se estiman las pérdidas monetarias de un incidente de seguridad? ¿Qué métodos se deben utilizar? ¿La estimación de la pérdida incluye las no monetarias, como la pérdida de reputación?

Los objetivos de las siguientes secciones de esta guía es ayudar a los CISOs con la presupuestación de las medidas de seguridad en aplicaciones para mitigar los riesgos de incidentes de filtración de datos mediante el análisis de dichos riesgos, la monetización de los impactos económicos y la estimación de la probabilidad y el impacto para el negocio. Sólo después que el trabajo de "diligencia debida a los riesgos" se lleva a cabo, es posible determinar los costos y comparar con los beneficios de la mitigación de riesgos y decidir en qué medidas de seguridad invertir. En el Apéndice A de esta guía, se proporciona una referencia rápida para asignar un valor monetario a los activos de información y determinar el impacto monetario de un incidente de seguridad en base a datos estadísticos. Después que se implementen las medidas es importante medir y monitorear la seguridad y los riesgos. En el Apéndice B se proporcionan ejemplos de proyectos de OWASP que pueden ayudar al CISO a medir y monitorear la seguridad y los riesgos de los activos de aplicaciones dentro de la organización.

Presupuestación de medidas de seguridad en aplicaciones para mitigar los riesgos de incidentes de filtración de datos

Para guiar al CISO en la toma de decisiones sobre "cuánto presupuesto necesita la organización para la seguridad en aplicaciones", nos centraremos en los criterios de mitigación de riesgos en lugar de otros factores como el porcentaje del presupuesto en tecnología de información (IT) y la asignación presupuestaria anual para la seguridad en aplicaciones como una fracción del presupuesto general de seguridad de la información que incluye los costos de cumplimiento y operativos/de gobierno. Un criterio de presupuestación de seguridad en aplicaciones basado en riesgos documentado en esta guía consiste en lo siguiente:

- Estimación del impacto de los costos incurridos en caso de un incidente de seguridad
- Cálculo cuantitativo de riesgos sobre el costo anual de las pérdidas debido a incidentes de seguridad
- Optimización de los costos de seguridad en relación al costo de incidentes y el costo de medidas de seguridad
- El retorno de inversión en seguridad en las medidas de seguridad en aplicaciones

En las siguientes secciones de esta guía explicaremos cada uno de estos criterios y la forma en que pueden ser utilizados para la cuantificación de la cantidad de dinero para gastar en medidas de seguridad.

Analizando de los riesgos de incidentes de filtración de datos

Hay dos factores importantes para determinar el riesgo de un incidente de seguridad: estos son los efectos negativos causados por el incidente de seguridad y la probabilidad del incidente. Para obtener una estimación del impacto de los costos incurridos en el caso de un incidente de seguridad, el factor clave es la capacidad de determinar los costos incurridos debido al incidente de seguridad. Los ejemplos de impactos negativos a una organización a causa de un incidente de seguridad podrían incluir:

- Pérdida de reputación, como el caso de una empresa que cotiza en bolsa, una caída en el precio de las acciones como consecuencia de una filtración de seguridad anunciada;
- Pérdida de ingresos como en el caso de una denegación de servicio a un sitio que vende bienes o servicios a clientes;
- La pérdida de datos que se considera un activo para la empresa, como datos confidenciales de usuarios, información de identificación personal (PII), datos de autenticación y datos comerciales secretos/ de propiedad intelectual;
- Incapacidad para prestar un servicio estatutario a los ciudadanos;
- Impacto adverso sobre las personas cuyos datos se han expuesto.

Monetizando los impactos económicos de los incidentes de filtración de datos

En el caso de un incidente de seguridad que provoque una pérdida de datos confidenciales de clientes o empleados, tales como información de identificación personal, de tarjetas de débito y crédito, los costos incurridos por la organización que sufrió la pérdida, incluyen varios costos operacionales también conocidos como costos de falla. En el caso de una compañía de servicios financieros, éstos son costos por el cambio de números de cuenta, costos de remisión por nuevas tarjetas de crédito y débito, costos de

responsabilidad debido a un fraude cometido por un estafador utilizando datos robados, tales como operaciones de pago ilícitas y retiro de dinero de cajeros automáticos. Muchas veces, la determinación de tales costos de "falla" no son directamente cuantificables por una organización; por ejemplo, cuando la pérdida monetaria no es causada directamente por un incidente de seguridad, por lo tanto, debe ser estimado como un posible impacto. En este caso, los CISOs pueden utilizar datos estadísticos para determinar los posibles costos de responsabilidad de la empresa en caso de incidentes de pérdida de datos. Mediante el uso de datos estadísticos reportados desde incidentes de pérdida de datos, es posible estimar los costos incurridos por las empresas para reparar los daños causados por tal incidente que dio lugar a la fuga de datos sensibles o pérdida de identidad.

El valor de los datos será diferente para cada organización, pero los valores en el rango de U$D 500 a U$D 2.000 por registro parece ser común.

Valor del dato: U$D 200 a U$D 2.000 por registro

Vamos a utilizar este rango para el debate, pero cada CISO tiene que llegar a alguna valoración propia que luego puede ser utilizada para calcular el impacto de una pérdida de datos.

Nota: el **Apéndice A** contiene una discusión detallada, ejemplos y una herramienta de cálculo de filtración de datos para estimar el costo de una filtración de datos en base a datos estadísticos.

Estimando de la probabilidad de incidentes de filtración de datos

Uno de los desafíos del cálculo de los cargos para la empresa debido a una posible pérdida de datos, es obtener una estimación precisa de la cantidad perdida por víctima y la probabilidad o posibilidad de que tal pérdida se produzca. Datos estadísticos sobre incidentes de pérdida de datos reportados a distintas jurisdicciones de los Estados Unidos y reunidos por *DataLossDB* de *Open Security Foundation*, muestran que el porcentaje de incidentes de pérdida de datos en 2010 por incumplimiento de una interfaz web es del 9% y el porcentaje que informó como *hackeo* es del 12%, 10% de fraude y 2% virus. El incidente más reportado según el tipo de infracción es el robo de portátiles con un 13%.

Más información: http://www.*DataLossDB*.org/

Los datos de *DataLossDB* relacionados con la web como tipo de infracción difieren de las estadísticas de las investigaciones de violaciones de datos de Verizon de 2011 donde informan el que *hacking* (por ejemplo, la fuerza bruta y ataques a credenciales) y *malware* (por ejemplo, *backdoors*, *keyloggers*/*form grabbers*, *spyware*) representan la mayoría de las amenazas de violaciones de seguridad (50% y 49% respectivamente), los ataques contra las aplicaciones representan el 22% de todos los vectores de ataque y el 38% como porcentaje de los registros vulnerados.

Estas diferencias podrían explicarse por el hecho que el estudio de Verizon se basa en un subconjunto de datos del Servicio Secreto de EE.UU. y no incluye, por ejemplo, los casos relacionados con el robo y el fraude que en cambio sí fueron contados con los datos estadísticos de *DataLossDB*. Además, según el informe de Verizon, *"el alcance de la encuesta se redujo a sólo aquellos que involucran violaciones de datos confirmados desde las organizaciones"*. En el caso de *DataLossDB*, los datos de la encuesta incluyen las violaciones de datos cubiertos por la ley de notificación de filtración de datos de EE.UU., tales como la

divulgación de información de identificación personal del cliente (PII) y reportado por organizaciones con cartas de notificación enviadas a distintas jurisdicciones en EE.UU.

Cuantificación del impacto al negocio por incidentes de filtración de datos

En los casos en que el impacto de una filtración de datos producida debido a un incidente de seguridad no se registra ni notifica al público en cumplimiento de las leyes de notificación de filtración de datos aplicadas por diferentes países y jurisdicciones, es necesario estimarlo basado en cálculos de la estimación de riesgos. Además del cálculo de los costos de responsabilidad basados en el valor de los datos (consulte el **Apéndice A** para estimar el valor de los datos), el análisis cuantitativo de riesgos se puede utilizar para estimar el gasto en medidas de seguridad de la aplicación sobre una base anual, calculando el impacto de un incidente de seguridad también en forma anual.

Los riesgos cuantitativos pueden ser calculados por la evaluación de la Expectativa de Pérdida Simple *(SLE - Single Loss Expectancy)* que es la probabilidad de una pérdida como resultado de un incidente de seguridad; y de la Tasa Anual de Ocurrencia *(ARO - Annual Rate of Occurrence)* que es la frecuencia anual de los incidentes de seguridad.

Mediante el uso del análisis cuantitativo de riesgos y el uso de los informes públicos de violaciones de datos, los CISOs pueden estimar la cantidad que una determinada organización perdería con una aplicación y lo que debería gastar en medidas de seguridad de aplicaciones para mitigar el riesgo de una pérdida de datos debido a la explotación de una la vulnerabilidad en la aplicación. La precisión de esta estimación de riesgos depende de qué tan confiable y pertinente es el incidente de filtración de datos para la seguridad de la aplicación. Por lo tanto, es importante elegir cuidadosamente los datos, ya que se está informando cómo son causadas las vulnerabilidades en las aplicaciones por un *exploit*, como la inyección SQL (por ejemplo, las violaciones de datos de Sony y *TJX Inc*.).

El SLE se puede calcular con la siguiente fórmula:

```
SLE = AV x EF
```

Donde, **AV** es el Valor de los Activos *(AV - Asset Value)* y **EF** es el Factor de Exposición *(EF - Exposure Factor)*. EF representa el porcentaje de la pérdida de activos debido a la concreción de una amenaza o un incidente. En el caso de los de incidentes de 2003 de la Comisión Federal de Comercio de EE.UU. (FTC), representa la cantidad de la población que ha sufrido fraude de identidad y es un 4,6%.

Suponiendo que un AV de un millón de cuentas es de U$D 655 millones (U$D 655 por cuenta basándose en los datos de la FTC de 2003) y un factor de exposición del 4,6%, el SLE estimado del incidente de filtración de datos es de U$D 30.130.000 (655.000.000 x 0,46).

Suponiendo una frecuencia de un ataque cada 5 años, como en el caso del incidente de filtración de datos de *TJX Inc* (descubierto a mediados de diciembre de 2006, y debido inyección SQL) el **ARO** es del 20%. De ahí que el **ALE** la pérdida anual estimada o Expectativa de Pérdida Anual *(ALE - Annual Loss Expectancy)* se puede calcular con la siguiente fórmula:

```
ALE = ARO x SLE
```

Entonces, el cálculo de Expectativa de Pérdida Anual (ALE) por incidentes de pérdida de datos es de U$D 6.026.000 (30.130.000 x 0,20) dólares/año durante 10 años.

Considerando costos y beneficios de las medidas de seguridad de aplicaciones antes de la realización de inversiones

Ahora la pregunta es si el uso del análisis de riesgos cuantitativo conduce a una estimación de la inversión óptima de medidas de seguridad en aplicaciones. Una respuesta honesta es, no necesariamente. La respuesta correcta es utilizar un análisis de costos vs beneficios para determinar el valor óptimo. Mediante la comparación de los costos de los incidentes de seguridad contra los costos de las medidas de seguridad, es posible determinar cuándo se maximiza el beneficio, es decir, la seguridad general de la aplicación.

En el caso de los costos de seguridad de software, por ejemplo, el costo debido a fallas de seguridad, incluyendo los incidentes de seguridad, disminuye a medida que la empresa gasta más dinero en medidas de seguridad, como se muestra en la (Fig. 3). La suposición es que un aumento de la inversión en medidas de seguridad se traduce en un menor riesgo y un menor impacto para el negocio. Esto se basa en la suposición que los riesgos disminuyen cuando las inversiones en seguridad aumentan. El otro supuesto es que las inversiones se dirigen hacia medidas efectivas de mitigación de riesgos de seguridad. Decidir qué medidas de seguridad es una mitigación eficaz del riesgo y en qué se debe invertir, implica que los CISOs han hecho un análisis de riesgos para determinar las medidas de seguridad más rentables (por ejemplo, procesos, controles técnicos, herramientas, formación y concientización, etc.) y seleccionaron las que reducen el riesgo de la mayoría y cuestan menos implementar, desplegar y mantener.

Nota: esto no siempre puede ser cierto, un mayor gasto en medidas de seguridad no siempre se traduce en un aumento de la mitigación de riesgos; por ejemplo, un mayor gasto en una protección antivirus no va a reducir el riesgo de compromiso por *malware* ya que tal *malware* está diseñado para evadir las firmas de detección de los antivirus.

Es de suma importancia tener en cuenta la eficacia de las medidas de seguridad para mitigar el posible impacto de amenazas específicas antes de decidir si es rentable invertir en ellas. En la **Parte II** de esta guía le ofrecemos una guía para ayudar a los CISOs a identificar qué vulnerabilidades se deben priorizar para corregir y qué medidas de seguridad son más efectivas en la mitigación de amenazas específicas dirigidas a las aplicaciones web. Antes de tomar decisiones sobre qué las medidas de seguridad invertir, por favor consulte la **Parte II "Criterios para el manejo de riesgos de seguridad en aplicaciones"**.

Con estos supuestos, cuanto más dinero se gaste en medidas de seguridad para evitar incidentes de seguridad, menos dinero se perderá cuando ocurra un incidente de seguridad; tales como costos para recuperarse de un incidente, corregir vulnerabilidades, poner en marcha nuevas medidas y pago de multas reglamentarias, costos de responsabilidad contractual y costos legales. El supuesto es que, debido a un aumento en el gasto en controles de protección y detección, en las pruebas y en correcciones de las vulnerabilidades y otras medidas, es menos probable que ocurran incidentes de seguridad, y cuando se produzcan, tendrán un impacto reducido para la organización. En el caso de las aplicaciones, la implementación de medidas de seguridad entra en el ámbito del programa de seguridad en aplicaciones. Los CISOs pueden mirar la **Parte III** de esta guía **"Programa de seguridad en aplicaciones"**, para saber qué

procesos de seguridad, herramientas y formación deben ser consideradas antes de invertir en medidas de seguridad en aplicaciones.

Con estas advertencias, cuanto más dinero se gasta en seguridad de aplicaciones, se puede alcanzar un punto en donde los costos superan los beneficios. Este, obviamente, no es el objetivo de la gestión de riesgos y un límite al que no se debe llegar si es posible, ya que esto socavaría toda la estrategia de mitigación de riesgos y presionaría a los CISOs a justificar sus presupuestos. Una buena estrategia de mitigación de riesgos es más bien la que busca identificar con qué valor de inversión en seguridad se maximizarán los beneficios para el negocio, y reducirán al mínimo los impactos. Este es el valor óptimo de la inversión en medidas de seguridad y se puede estimar mediante la medición de costos incurridos a causa de los incidentes, así como la inversión en medidas de seguridad. Al suponer que tales indicadores de medición de costos han sido adoptados por la organización, sería posible determinar si un aumento del presupuesto en la mitigación de riesgos se correlaciona con un menor número de incidentes de seguridad y se reduce el impacto global causado por estos incidentes. En la Parte IV de esta guía proveemos una orientación a los CISOs para el establecimiento de **"Métricas para la gestión de riesgos e inversiones de seguridad en aplicaciones"**.

En ausencia de tales parámetros, para determinar el valor óptimo de las inversiones en seguridad de aplicaciones, los CISOs pueden mirar algunos estudios de investigación que apuntan a la inversión óptima donde el costo de las medidas de seguridad es aproximadamente del 37% de las pérdidas estimadas. Para nuestro ejemplo, asumiendo que las pérdidas totales estimadas son U$D 6.026.000 dólares/año debido a incidentes de pérdida de datos, el gasto óptimo para las medidas de seguridad, utilizando un valor empírico del estudio, es U$D 2.229.62 dólares/año.

En la imagen se muestra el Costo de la Inversión en medidas de seguridad de software contra los costos de fallos debido a los incidentes que explotan las vulnerabilidades de software. En el punto (A), los costos debido a fallas de seguridad exceden en magnitud el gasto en contramedidas y la garantía de seguridad del software es muy baja. Por el contrario, en (B) los costos de las medidas de seguridad son mayores que los costos debido a fallos, el software puede ser considerado muy seguro, pero se gasta demasiado dinero para el aseguramiento del mismo. En el punto (C), el costo de las pérdidas es casi dos veces más grandes que los costos de las medidas de seguridad; mientras que en el punto (D) el costo debido a incidentes es igual al costo de las medidas de seguridad.

El valor óptimo para el gasto de las medidas de seguridad es el que minimiza tanto el costo de los incidentes como el de las medidas de seguridad, y maximiza el beneficio o la seguridad del software.

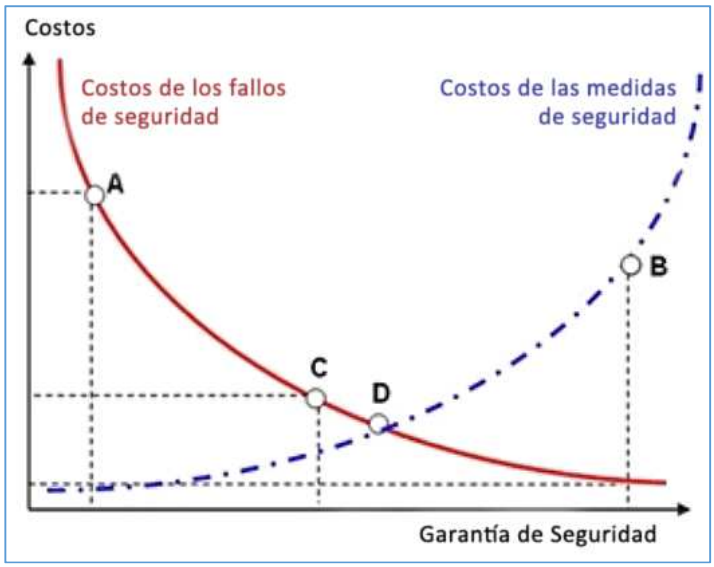

Figura 3 - Costo de los fallos vs los costos de las medidas de seguridad

Analizando las medidas de seguridad como inversión

Para la mayoría de las organizaciones de hoy en día, la seguridad en aplicaciones no se ve como una inversión sino como un costo impuesto por la necesidad de cumplir las normas y reglamentos. Algunas organizaciones podrían justificar el gasto en seguridad de aplicaciones debido a los requisitos de gestión de riesgos, otras debido a una mayor conciencia de la exposición a las amenazas de los delincuentes cibernéticos, estafadores y *hacktivistas*. Algunas organizaciones podrían considerar ese ahorro de costos que proporciona la inversión en seguridad en "tiempos de comercialización" más cortos, de manera que se lance un producto de seguridad antes que la competencia. Algunas organizaciones podrían darse cuenta que el gasto de seguridad en aplicaciones web puede aumentar el nivel de confianza que los clientes tienen en las aplicaciones de red que están acostumbrados a usar y ayudar a retener estos negocios con el cliente, y así venderles más servicios: estas organizaciones podrían ver el gasto de seguridad en aplicaciones de una forma positiva, como una inversión y no como un costo. Para las organizaciones que consideran la seguridad como inversión y no como un costo, es importante determinar la forma más eficiente de gastar el presupuesto para la seguridad en aplicaciones desde la perspectiva de que esto sea una inversión. Si el CISO considera el gasto en seguridad de aplicaciones como una inversión y no como un gasto por ejemplo, el presupuesto puede ser justificable como un ahorro adicional que la empresa obtiene, por haber gastado menos dinero para hacer frente a los incidentes de seguridad.

Un ejemplo de este "pensamiento de ahorro de dinero" podría ser "si gasto un total de $$ en medidas de seguridad para evitar los incidentes en los próximos dos años, voy a ahorrar un total de $$ en posibles pérdidas, corrección de vulnerabilidades y, otros costos directos e indirectos causados por un número estimado de incidentes de seguridad en los próximos dos años". Uno de los métodos para calcular los ahorros en términos de inversión en seguridad es el Retorno Sobre la Inversión en Seguridad *(ROSI - Return On Security Investment)*. El uso del ROSI puede ayudar al CISO a determinar si la inversión en contramedidas

para frustrar ataques específicos se justifica como una inversión de seguridad a largo plazo: si el ROSI no es positivo la inversión no se justifica, mientras que si es nulo no hay ahorro o rendimiento de la inversión.

Hay varias fórmulas empíricas para calcular el ROSI; uno es el factor de ahorro sobre las pérdidas de datos evitadas por el costo total de los controles de seguridad/medidas. Suponiendo que el Costo Total de Propiedad *(TCO - Total Cost of Ownership)*, para el costo del control/medida de seguridad, es de U$D 2.229.620 (calculado previamente como valor óptimo del gasto en los controles de seguridad para la mitigación de inyección SQL anual), que incluye costos de desarrollo y adquisición de nuevas tecnologías, procesos y herramientas, así como costos de operación y mantenimiento; con esto es posible calcular los ahorros en los costos de incidentes de seguridad. El ROSI se puede calcular utilizando la siguiente fórmula empírica:

ROSI = [(ALE x % de la eficacia del control) - costo de controles] / costo de controles

Con esta fórmula del ROSI, asumiendo un ALE (Expectativa de Pérdida Anual) calculada previamente para incidentes de seguridad causados por la explotación de vulnerabilidades de inyección SQL es U$D 6.026.000 y la eficacia de la mitigación del riesgo de control es del 75 % (por ejemplo, suponiendo el caso de una inyección SQL, la mitigación de riesgos como la defensa en profundidad como diferentes capas de controles que incluyen el uso de sentencias preparadas/procedimientos almacenados en el código fuente, así como filtrado de caracteres maliciosos en el servidor web y servidor de aplicaciones); el costo de los controles de seguridad es U$D 2.229.620; el valor del ROSI para la empresa es de 102% por año:

ROSI = (6.026.000 x 0,75) - 2.229.620 / 2.229.620 = 1,02

Con este valor del retorno de la inversión en seguridad, el gasto en medidas de control de seguridad vale la pena y hará que cada año la empresa ahorre dinero. El mejor uso del ROSI es comparar alternativas de inversión en medidas de seguridad como para decidir si invertir en el desarrollo de una nueva contramedida o ampliar las capacidades de una existente.

Como medida comparativa, por ejemplo el ROSI puede ser utilizado por los CISOs para determinar qué proceso de seguridad en aplicaciones es más eficiente o brinda a la organización mayores ahorros y retorno de inversión durante el ciclo de vida de desarrollo del software (SDLC).

Según la investigación de *Soo Hoo* (IBM) del ROSI, sobre las diversas actividades de seguridad en el SDLC, el máximo retorno de inversión 21% (por ejemplo, un ahorro de U$D 210.000 en una inversión de U$D 1 millón), es cuando la mayor parte del dinero se invierte en actividades que permiten identificar y remediar los defectos de seguridad durante la fase de diseño del SDLC, como el análisis de riesgos de la arquitectura y el modelado de amenazas de la aplicación.

El retorno de inversión es menor (15%) cuando los defectos son identificados y remediados durante la fase de implementación (código) del SDLC, con análisis de código fuente; e incluso inferior (12%) cuando éstos son identificados y remediados durante la fase de pruebas de validación del SDLC como ser pruebas de intrusión/hacking ético.

Al utilizar el ROSI como métrica comparativa para la inversión en actividades del S-SDLC, la inversión más rentable en seguridad de la aplicación, por tanto, es en las actividades que puedan identificar defectos tan pronto como sea posible, como en la fase de requisitos y de diseño del SDLC. En esencia, la mayoría de

los CISOs piensan en invertir en programas de seguridad en aplicaciones y, especialmente, en las actividades de ingeniería de requisitos de seguridad, como las actividades de modelado de amenazas/análisis de riesgos de arquitectura y revisión de seguridad del código, donde más se va a ahorrar sobre los costos de implementar y solucionar problemas de seguridad con otras actividades tales como pruebas de penetración.

Conclusión

Finalmente, es importante recalcar que las estimaciones de costos utilizando las fórmulas empíricas de riesgo y costo abordadas en esta guía, son tan buenas como la fiabilidad de los valores de los datos que son utilizados. Cuanto más precisos son estos valores, más precisos son los cálculos de costos. Sin embargo, cuando se utilizan constantemente estos criterios de costo-riesgo y se basan en cálculos de riesgo cuantitativos probados y fiables, pueden ser utilizados por los CISOs para consideraciones objetivas de riesgos y costos para decidir si la inversión en medidas de seguridad en aplicaciones es económicamente justificable. Estas consideraciones de riesgo y costo también pueden ser utilizadas por los CISOs para defender sus presupuestos a la luz de medidas de la reducción de costos o pedir más presupuesto. Hoy en día, el aumento del presupuesto en seguridad de aplicaciones puede justificarse a la luz del aumento de la exposición de riesgos en aplicaciones web y las pérdidas monetarias provocadas por incidentes de seguridad. Dado que la inversión en seguridad de aplicaciones tiene que ser justificada en términos de negocio, estos criterios de costo-riesgo se pueden utilizar para los casos de negocio, así como para decidir cuánto y dónde gastar en medidas de seguridad de aplicaciones.

Parte II: Criterios para gestionar riesgos de seguridad en aplicaciones

II-1 Resumen Ejecutivo

Los CISOs deben priorizar las cuestiones de seguridad a fin de identificar las áreas que necesitan atención primero. Para tomar decisiones informadas acerca de cómo gestionar los riesgos de seguridad, los CISOs a menudo necesitan evaluar los costos de reparar vulnerabilidades conocidas y de la adopción de nuevas contramedidas, y considerar los beneficios, en cuanto a mitigación de riesgos, de llevar a cabo estas acciones. Las relaciones costo/beneficio son críticas para decidir en cuáles medidas y controles de seguridad invertir para reducir el nivel de riesgo. Con frecuencia los CISOs necesitan explicar a la gerencia ejecutiva los riesgos inherentes a las aplicaciones y manifestar el impacto potencial al negocio de la organización en caso de presentarse un ataque a las aplicaciones y una filtración a la información confidencial.

Los riesgos de seguridad constituyen riesgos para el negocio sólo cuando las tres características de riesgo se presentan:

- Amenaza viable
- Vulnerabilidad que puede ser expuesta
- Activo de valor

Para priorizar sistemáticamente los riesgos técnicos a fin de remediarlos, los CISO deberían considerar una metodología de clasificación del riesgo conocida como el Sistema Común de Clasificación de Vulnerabilidades Versión 2.0 *(CVSSv2 - The Common Vulnerability Scoring System)*. Para ayudar a comunicar regularmente los riesgos de las aplicaciones a los ejecutivos de negocios, los CISOs deben considerar proporcionar informes de concientización sobre ciberamenazas emergentes a la gerencia ejecutiva.

Comunicar a los ejecutivos de negocios: los CISOs necesitan ser realistas acerca de los riesgos de las ciberamenazas y presentar al negocio el panorama general de los riesgos de seguridad de la información, no sólo respecto a cumplimiento y vulnerabilidades sino también sobre incidentes de seguridad e inteligencia de amenazas de los agentes de amenaza que tienen como blanco los activos de información de la organización, incluyendo las aplicaciones. La habilidad para comunicar los riesgos al negocio le otorga al CISO la facultad de presentar la seguridad de las aplicaciones como un caso de negocio, y justificar de este modo el gasto adicional en medidas de seguridad para las aplicaciones. Esta justificación debe considerar el impacto económico de los incidentes de seguridad en comparación con los costos del incumplimiento legal. Hoy día, los costos de negocio debido a los impactos económicos de los incidentes de seguridad son mucho más altos que los costos del incumplimiento y de no superar las auditorías. Con frecuencia, la severidad del impacto de los incidentes de seguridad puede costarle a los CISO sus puestos de trabajo y, a la compañía perder reputación e ingresos.

Modelado de amenazas: en un enfoque de arriba hacia abajo para identificar amenazas y contramedidas, los CISOs deberían considerar una técnica de modelado de amenazas también descrita en la **Parte III**. La técnica de modelado de amenazas permite descomponer a la aplicación objetivo para revelar

su superficie de ataque y, a continuación, las amenazas relevantes, las contramedidas asociadas, y finalmente, las brechas y fallas de diseño en sus controles de seguridad.

Manejando los riesgos de las nuevas tecnologías: nuevas tecnologías y plataformas, tales como las aplicaciones móviles, web 2.0 y los servicios de *Cloud Computing* proponen diferentes amenazas y técnicas de contramedidas. Los cambios en las aplicaciones también constituyen fuentes de potenciales riesgos, especialmente cuando nuevas o diferentes tecnologías se encuentran integradas en las aplicaciones. A medida que las aplicaciones evolucionan ofreciendo nuevos servicios a los ciudadanos, clientes y consumidores, también se hace necesario planificar la mitigación de nuevas vulnerabilidades que surgen con la adopción e implementación de nuevas tecnologías, tales como dispositivos móviles, web 2.0 y nuevos servicios como el *Cloud Computing*. Adoptar una estrategia de riesgo para evaluar los riesgos introducidos por las nuevas tecnologías es esencial para determinar qué contramedidas adoptar para mitigar estos nuevos riesgos. Esta guía provee orientación respecto de la mitigación de riesgos de las nuevas amenazas que podrían surgir por la implementación de nuevas tecnologías.

- Aplicaciones móviles
    - Ejemplos de preocupaciones: dispositivos perdidos o robados, *malware*, exposición de la comunicación, autenticación débil.
    - Ejemplos de acciones de los CISOs: alcanzar los estándares de seguridad móvil, realizar auditorías de seguridad para evaluar las vulnerabilidades de las aplicaciones móviles, la seguridad del aprovisionamiento y los datos de aplicaciones en dispositivos personales.
- Web 2.0
    - Ejemplos de preocupaciones: protección de medios sociales, gestión de contenido, seguridad de las tecnologías y servicios de terceros.
    - Ejemplos de acciones de los CISOs: API de seguridad, CAPTCHAs, *tokens* de seguridad únicos en los formularios y *workflows* de aprobación de transacciones.
- Servicios de Cloud Computing
    - Ejemplos de preocupaciones: implementaciones multi-cliente, seguridad de las implementaciones en la nube, riesgo de terceros, brechas de datos, denegación de servicios provocada por personal interno malicioso.
    - Ejemplos de acciones de los CISOs: evaluaciones de seguridad de *Cloud Computing*, evaluaciones de conformidad con las auditorías por parte de los proveedores, diligencia debida, cifrado en tránsito y almacenamiento, y monitoreo.

Los agentes de amenaza hoy en día buscan provecho financiero atacando aplicaciones para comprometer la información sensible de los usuarios y la información propiedad de la compañía, y de esta manera obtener una ventaja financiera, cometer fraude, o lograr una ventaja competitiva (por ejemplo, a través del ciberespionaje). Para mitigar los riesgos planteados por estos agentes de riesgo, se necesita determinar la exposición al riesgo y calcular la probabilidad y el impacto de estas amenazas así como también identificar el tipo de vulnerabilidades de las aplicaciones que pueden ser explotadas por estos agentes de amenaza. El aprovechamiento de algunas de estas vulnerabilidades de las aplicaciones podría impactar en la organización de forma severa y negativa, poniendo en peligro el negocio.

II-2 Introducción

Una vez que una aplicación se ha convertido en el blanco de un ataque y la organización ha sufrido ya sea un incidente de infiltración en sus datos o el fraude resultante, es importante entender las causas primarias (por ejemplo vulnerabilidades, fallas en los controles, etc.) del incidente e invertir en medidas de seguridad para evitar que tal incidente vuelva a ocurrir. En esta sección de la guía, abordamos cómo enfocar la inversión para mitigar el riesgo que presentan ataques y *exploits* específicos de vulnerabilidades que causan incidentes de infiltración en la información. Como mejor práctica, no proponemos solamente corregir las vulnerabilidades que pueden haber sido la causa del incidente, incluso si éstas son las que se necesita priorizar para corregir de modo de limitar mayor daño. Las vulnerabilidades que pueden haber sido ya explotadas para atacar las aplicaciones ciertamente presentan la más alta probabilidad de ser también aprovechadas en futuros ataques.

El mayor interrogante para el CISO es si las mismas vulnerabilidades pueden ser utilizadas en ataques en el futuro contra aplicaciones que poseen funcionalidades y tipos de datos similares. De todos modos, la aplicación puede tener otro tipo de vulnerabilidades que podrían ser oportunamente explotadas por un atacante. Estas son vulnerabilidades que permiten o facilitan al atacante dirigir ataques contra las aplicaciones. Dado que el riesgo de filtración o acceso no permitido a los datos y el fraude por Internet son factores de probabilidad e impacto de las vulnerabilidades, es importante considerar probabilidad e impacto como factores para determinar en qué elementos enfocarse para la inversión. En general, las prioridades de las vulnerabilidades se fijan en base a los riesgos técnicos y no de acuerdo al impacto al negocio. Por ejemplo, a las vulnerabilidades que presentan riesgos técnicos altos se les da más prioridad para remediación que aquellas de bajo riesgo. Una vulnerabilidad de alto riesgo técnico puede ser por ejemplo inyección SQL, independientemente del activo de información y del valor que dicho activo representa para la organización. Claramente si esa vulnerabilidad a ataque por inyección SQL afecta la autenticación o información confidencial, puede representar un riesgo muy diferente para la organización al de una vulnerabilidad a ataque por inyección SQL que afecte datos considerados de bajo riesgo para la organización tales como información de investigación de mercado, por ejemplo. El impacto en este caso puede ser más del tipo reputacional que de pérdida de información.

En la **Parte I** de esta guía proveemos casos de negocio que los CISOs pueden usar para solicitar presupuesto para seguridad de las aplicaciones. El presupuesto para la seguridad de aplicaciones típicamente debe cubrir varias necesidades de seguridad de la información y gestión del riesgo de gobierno. Más allá de la habitual necesidad de invertir para lograr conformidad con los estándares, políticas y regulaciones sobre seguridad de la información, los CISO deberían recomendar un presupuesto adicional para cubrir la mitigación del creciente riesgo de incidentes de fuga de datos. Un factor crítico es cuantificar el impacto del incidente de acceso a los datos ocurrido. Esto implica que los CISOs estén autorizados a acceder a información relacionada con dicho incidente, tal como reportes de incidentes generados por el Equipo de Respuesta a Incidentes de Seguridad *(SIRT - Security Incident Response Teams),* información del área legal, relacionada con demandas y multas, y datos sobre fraudes, incluyendo la cantidad de dinero perdido a causa del fraude online. Todo este tipo de información es esencial para determinar el impacto general. En ausencia de estos datos, lo mejor que el CISO puede hacer es usar información y reportes de fuentes públicas sobre incidentes de fuga de datos. En la **Parte I** de esta guía, proporcionamos algunos

ejemplos sobre cómo esta información se puede utilizar para estimar el impacto. Documentamos cuáles son los factores críticos para estimar impactos de incidentes de fuga de datos: con respecto al valor de los activos de información (por ejemplo, información confidencial y personal de identificación de ciudadanos, clientes o empleados, tarjetas de crédito y datos de cuentas bancarias) y la responsabilidad de la organización en caso que los activos se pierdan. Una vez que el potencial impacto es estimado, el próximo paso consiste en determinar cuánto se debería invertir para mitigar el riesgo. A alto nivel, esta es una decisión estratégica de riesgo que depende de la cultura de riesgo de la organización y de sus prioridades para mitigar el riesgo.

Dependiendo del tipo de organización, la prioridad número uno puede ser "no ser atrapado en incumplimiento legal" como en el caso de sufrir filtración de la información y adicionalmente fallar en el cumplimiento de los estándares PCI-DSS. Este puede ser el caso de compañías pequeñas que proveen servicios de procesamiento de pagos online y que podrían perder parte del negocio en manos de los emisores de tarjetas de crédito, o por multas, demandas legales y auditorías y otros costos legales. Para una organización del tipo de un organismo de ingeniería o investigación cuyas patentes y secretos comerciales son activos críticos, la protección contra amenazas internas de espionaje comercial pueden representar la prioridad número uno. En general, es importante abordar la seguridad de las aplicaciones como un facilitador de los negocios al proteger los activos digitales cuyo valor se encuentra representado en términos de los costos de las medidas de seguridad versus los beneficios de proteger los activos digitales. En la Parte I de la guía comentamos que un criterio que puede ser utilizado es aquel que optimiza el gasto al maximizar el valor de la mitigación del riesgo mientras minimiza los costos en seguridad. Otro criterio consiste en considerar la seguridad no como un impuesto sino como una inversión, este criterio se conoce como Retorno de Inversión en Seguridad (ROSI por sus siglas en inglés). El ROSI puede ser utilizado para tomar decisiones de mitigación de riesgo tanto tácticas como estratégicas. Tácticamente, ROSI puede ser utilizado para decidir cuáles medidas de seguridad se deberían seguir para invertir, considerando el costo versus la efectividad de la medida en la atenuación del impacto de la pérdida de datos. Estratégicamente, ROSI puede ser usado para decidir en cuáles actividades de seguridad de aplicaciones invertir en el SDLC, aquellas que generarán ahorro de dinero en el largo plazo.

II-3 Definir el riesgo

Antes de discutir cómo gestionar los riesgos de seguridad de las aplicaciones, necesitamos utilizar una terminología consistente. De acuerdo al **Top Ten de Riesgos de Aplicaciones Web de OWASP**, la caracterización del riesgo de la vulnerabilidad es la siguiente: *"Los atacantes pueden potencialmente utilizar muchos caminos diferentes a través de tu aplicación para dañar tu negocio u organización. Cada uno de estos caminos representa un riesgo que puede, o no, ser lo suficientemente serio como para justificar su debida atención"*.

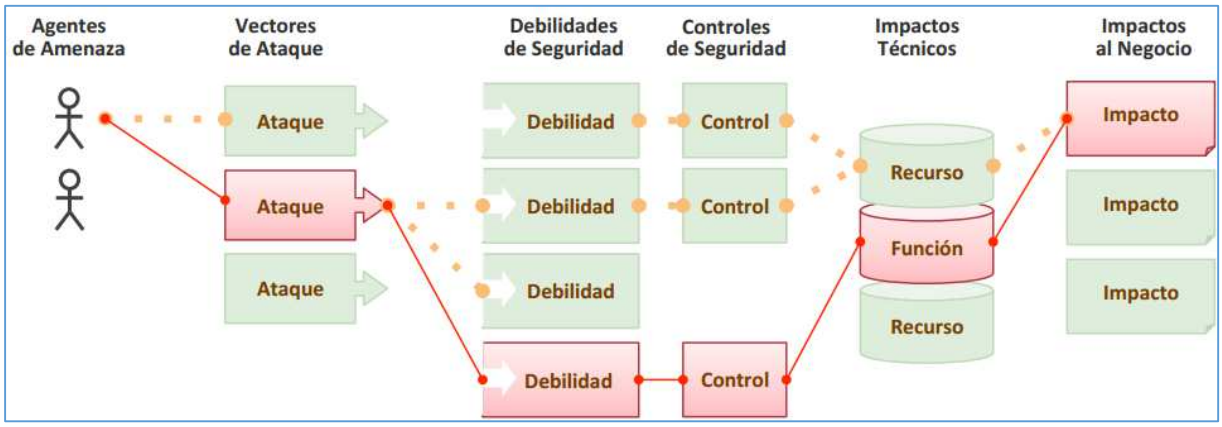

Figura 4 – Los atacantes tienen diferentes caminos para atacar una aplicación

Esta sección tratará:

- Priorizar el Riesgo Global
- Comprender los Factores de Riesgo
    - Agentes de amenaza
    - Ataques, debilidades (vulnerabilidades), y controles (contramedidas)

II-4 Priorizar el riesgo global

Priorizar riesgos a partir de vulnerabilidades conocidas es un enfoque reactivo pero tangible para la gestión clara del riesgo del negocio. Estas características de los riesgos son útiles para los CISOs en la determinación de los riesgos al negocio, en donde un agente de amenaza aprovecha vulnerabilidades o debilidades en los controles para comprometer un activo y causar un impacto negativo al negocio. Cabe remarcar que el valor del activo no tiene nada que ver con el costo financiero del activo, es el valor relativo que la organización le otorga al activo en caso que éste se pierda o se vea comprometido.

El riesgo de negocio ocurre cuando hay una probabilidad de ocurrencia de una amenaza a un sistema, una vulnerabilidad y un activo de valor.

El riesgo de negocio por cuestiones de seguridad está impulsado por:

- Probabilidad de Amenaza (PA): la probabilidad de que ocurra la amenaza.
- Exposición de la Vulnerabilidad (EV): la probabilidad de exposición de la vulnerabilidad a la amenaza.
- Valor del Activo (VA): el impacto sobre el negocio.

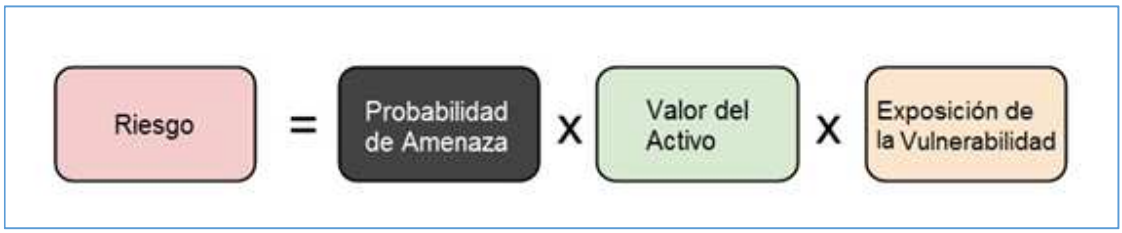

Figura 5 – Cálculo del riesgo

Los CISOs deberían utilizar un abordaje consistente para describir los riesgos técnicos de las vulnerabilidades conocidas. Hay muchas metodologías clasificación de riesgos en uso en la actualidad y una de ellas es CVSSv2. Al utilizar una metodología de clasificación de riesgos, es crítico no sólo puntuar una vulnerabilidad en base a la probabilidad y el impacto al negocio, sino también teniendo en cuenta el contexto de la misma dentro de la organización. Esto permite a los CISOs clasificar los riesgos para llevar adelante la inversión en seguridad de aplicaciones. OWASP es la fuente principal que las organizaciones obtienen el Top Ten de riesgos de aplicaciones web que deben ser mitigados. El chequeo del Top Ten de OWASP puede requerir que las organizaciones rutinariamente realicen pruebas de seguridad de estas vulnerabilidades en aplicaciones web. Una vez que las vulnerabilidades se han identificado y se les ha asignado el nivel de severidad correspondiente, es importante contar con un proceso de gestión de vulnerabilidades que permita a los administradores dar prioridad a los parches de estas vulnerabilidades de acuerdo a la severidad del riesgo, pero también teniendo en cuenta los impactos al negocio que podrían causar en caso que sean aprovechadas por un atacante. Pero las vulnerabilidades son solo un aspecto en la mitigación de los riesgos de seguridad en aplicaciones.

Acerca de CVSSv2: Una Metodología para Priorizar riesgos

Calculadora online: http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2

Guía CVSSv2: http://www.first.org/cvss/cvss-guide.html

Este sistema de clasificación del riesgo utiliza múltiples puntos de datos para evaluar riesgos:

- Métricas Básicas
  - Vector de Acceso (AV)
  - Complejidad de Acceso (AC)
  - Autenticación (Au)
  - Impacto a la Confidencialidad (C)
  - Impacto a la Integridad (I)
  - Impacto a la Disponibilidad (A)
- Métricas Temporales
  - Explotabilidad (E)
  - Nivel de Remediación (RL)
  - Confianza del Reporte (RL)
- Métricas ambientales
  - Daño Colateral Potencial (CDP)
  - Distribución del Objetivo (TD)
  - Requerimientos de Seguridad (CR, IR, AR)

II-5 Comprender los factores de Riesgo: Amenazas y Contramedidas

Los CISOs deberían adoptar una técnica de modelado de amenazas para llevar adelante la calificación de riesgos. Según el **Modelado de Amenazas a las Aplicaciones de OWASP** *"el modelado de amenazas es una estrategia para analizar la seguridad de una aplicación. Se trata de una estrategia estructurada que permite identificar, cuantificar y encarar los riesgos de seguridad asociados con una aplicación"*.

Más información:

https://www.owasp.org/index.php/Application_Threat_Modeling

https://www.owasp.org/index.php/Modelado_de_Amenazas

Agentes de amenaza

Un agente de amenaza *"se utiliza para señalar un individuo o grupo que puede manifestar una amenaza. Es fundamental identificar quien querría aprovecharse de los activos de una compañía, y como podrían usarlos contra la compañía".* Un agente de amenaza puede ser definido como la función de sus capacidades, intenciones y actividades previas:

Agente de amenaza = Capacidades + Intenciones + Actividades Previas

Más información: https://www.owasp.org/index.php/Category:Threat_Agent

Un agente de amenaza puede ser descrito como la intersección entre los motivos del agente, los tipos específicos de ataques utilizados y las vulnerabilidades que son explotadas.

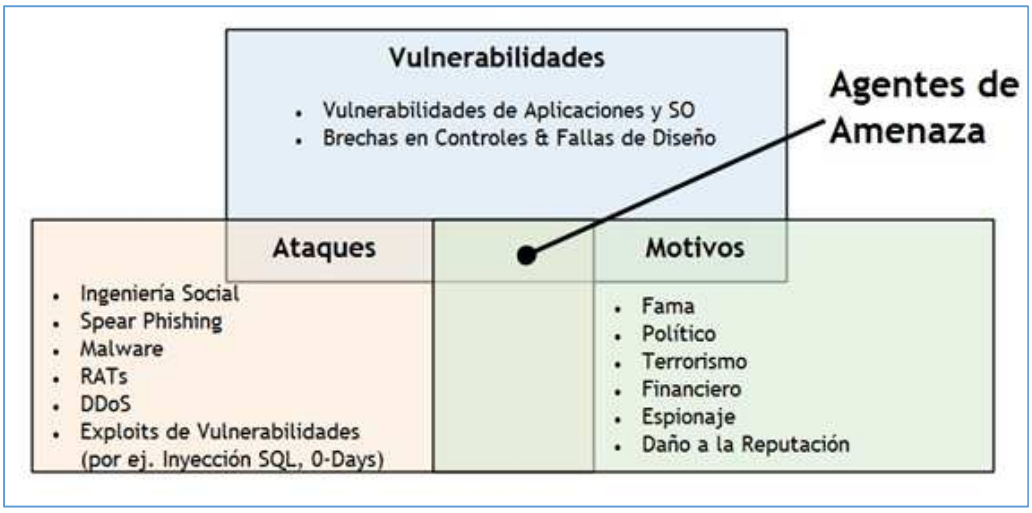

Figura 6 - Agentes de Amenazas

La creciente madurez de los agentes de amenaza

Al identificar las intenciones y capacidades del agente de amenaza, tales como los tipos de ataques utilizados contra las aplicaciones y las vulnerabilidades que son explotadas, los CISOs pueden evaluar la probabilidad y el impacto al negocio. A medida que las ciberamenazas evolucionan, se hace importante comprender cuáles son estos agentes de amenaza, sus intenciones y sus actividades previas, es decir, los

tipos de ataques que éstos utilizaron. Al analizar cómo evolucionan las amenazas, los CISOs pueden adaptar las medidas de seguridad de las aplicaciones para mitigar los riesgos de esas amenazas.

En la década pasada, los agentes de amenaza cambiaron y maduraron radicalmente. Históricamente, los agentes de amenaza comenzaban como una aventura oportunista, atacando a cualquiera que tuviera una vulnerabilidad, sin importar el valor del activo. Las amenazas de hoy en día son focalizadas, usualmente se las conoce como Amenazas Persistentes Avanzadas *(APT – Advanced Persistent Threat).*

- *Script Kiddies*, Gusanos y virus de autor
- Estafadores y cibercriminales
- Hacktivistas
- Ciberespías
- Agentes del tipo APT

Script Kiddies, Gusanos y Virus de Autor

Entre los años 2000 y 2005, los principales agentes de amenaza eran los llamados *"script kiddies"* que buscaban ganar notoriedad *"hackeando"* los sistemas del gobierno mediante el uso de técnicas y *scripts* fáciles-de-conseguir para buscar y explotar debilidades en otras computadoras, como por ejemplo la propagación de gusanos o virus de autor para causar una notable gran cantidad de interrupciones de computadoras, y obtener fama como resultado. Históricamente, los objetivos principales de estos agentes de amenaza no eran sitios web, sino las computadora, en pro de obtener notoriedad al infectarlas con virus, troyanos y gusanos. Entre los *script kiddies* famosos se encuentran:

- Jonathan James, conocido en la Red como *"cOmrade"*, que se declaró culpable de la intercepción de 3.300 emails, robo de contraseñas, y robo de información utilizando *sniffers* de red instalados en servidores infiltrados del Departamento de Defensa de EE.UU., a través de *backdoors*.
- En el año 2000, Jeanson James Ancheta creó un gusano que le permitió infectar tantas computadoras en Internet como pudo mediante Troyanos de Acceso Remoto *(RATs - Remote Access Trojan)*. Con el tiempo, acumuló más de 40.000 computadoras de acceso remoto infectadas por el gusano (más conocidas como *"bots"*).
- En el mismo año 2000, Onel Degusman creó el virus *ILoveYou* que se propagó por email a 10 millones de computadoras en todo el mundo, costándoles a las compañías un estimado de 5.500 millones de dólares para eliminarlo.
- También en el año 2000, un *script kiddie* de 15 años, Michael Calce, conocido como *"mafia boy"* dejó fuera de servicio los sitios de *eBay, Amazon y CNN* durante 90 minutos por el uso accidental de la herramienta de compartición de archivos.
- Un autor de gusanos notorio del año 2004 es Sven Jascham, autor del gusano *Sasser* que se estima afectó a 10 millones de computadoras. El impacto del gusano *Sasser*, incluye la desactivación de hosts relacionados a las comunicaciones satelitales, operaciones de vuelos transatlánticos de aerolíneas, hospitales y organizaciones financieras.

Los CISOs de hoy en día necesitan estar alerta de las amenazas que representan los agentes de amenaza *script kiddies* del presente, usando herramientas que se encuentren fácilmente disponibles y que buscan los más conocidos exploits para luego exponerlos al público. Los CISOs necesitan asegurarse que

los sistemas y aplicaciones no son vulnerables a estas vulnerabilidades dado que podrían impactar severamente en las operaciones de la organización cuando sistemas críticos son infectados y deshabilitados, como también dañar la reputación de la compañía cuando las noticias de estos *exploits* se exponen en los medios sociales (por ejemplo, Twitter o Facebook).

Estafadores y Cibercriminales

Entre los años 2005 y 2010 los motivos de los agentes de amenaza se desplazaron del hackeo para obtener notoriedad y fama al hackeo para obtener beneficio financiero. Durante este período los blancos de los ataques también se trasladaron de los hosts a los sitios web y los motivos de los ataques cambiaron de causar alteración utilizando virus y gusanos al robo de información confidencial y sensible, tal como datos personales para el robo de identidad, y datos de tarjetas de crédito y débito para el fraude con tarjetas de crédito.

- En el año 2007, por ejemplo, Albert Gonzales y otros tres conspiradores tuvieron éxito en su intento de robar 130 millones de números de tarjetas de crédito de *Heartland Payment Systems*, una procesadora de tarjetas de pago de Nueva Jersey; *7-Eleven*, la cadena con base en Texas de tiendas de autoservicio; y *Hannaford Brothers*, una cadena con base en Maine de tiendas de supermercados. Los atacantes utilizaron ataques por medio de inyección SQL que resultaron en la colocación de *malware* para espiar la red en busca de datos de tarjetas de crédito usadas en las tiendas de venta al por menor. Luego cometieron fraude a cajeros automáticos al codificar los datos en cintas magnéticas de tarjetas en blanco y retirar decenas de miles de dólares de los cajeros, en diversas oportunidades.
- En 2010, una banda cibercriminal de 37 delincuentes rusos tuvo éxito en su intención de robar 3 millones de dólares de cuentas bancarias online al infectar PCs de usuarios de banca online con el troyano bancario ZEUS. El troyano ZEUS está específicamente diseñado para robar información bancaria al utilizar las técnicas de *"Man in the Browser"* y *"Key Logging"*, y atacar aplicaciones de banca online interceptando las sesiones y asumiendo el control de las cuentas bancarias de las víctimas.
- En 2012 el *malware* bancario *ZEUS* evolucionó en algo nuevo y más sofisticado denominado *"GameOver"*, diseñado para robar las credenciales bancarias online del usuario al vencer los métodos comunes de autenticación multifactor empleados por las instituciones financieras, y para realizar transferencias utilizando las credenciales de la víctima, sin requerir ninguna interacción de la víctima durante el ataque.

Para los CISOs en las instituciones financieras, entender cómo estos agentes de amenaza y ataques por medio de *malware* buscan comprometer las credenciales online de los usuarios y superar la autenticación multifactor, es crítico para determinar las contramedidas a implementar para proteger a las instituciones financieras de estos ataques. A menudo los CISOs en las organizaciones financieras suscriben a los "servicios de inteligencia de amenazas" de modo de ser notificados cuando las credenciales online de un cliente y la información bancaria y de tarjeta de crédito han sido recuperadas de los servidores de Comando y Control (C&C) de *ZEUS* que fueron desactivados. Típicamente estas alertas son el resultado del desmantelamiento de *botnets* que alojan el *malware ZEUS* por parte de las fuerzas de la ley. Basándose en

esta información el CISO puede informar al negocio de modo de tomar las acciones que limiten el impacto, como puede ser notificar a los clientes y suspender y reemplazar las cuentas bancarias y crediticias.

Hacktivistas

Entre los años 2.010 y 2012 emergió una nueva clase de agentes de amenaza que buscaba atacar sitios web del gobierno y corporaciones por motivos políticos. Se trata de grupos de atacantes como *Lulzec* y *Anonymous*. En 2011 *Lulzec* asumió la responsabilidad por un ataque que comprometió cuentas de usuarios y datos de tarjetas de crédito de usuarios de la red de la consola *PlayStation de Sony*, mientras que *Anonymous* se adjudicó la responsabilidad por la modificación del sitio de la compañía *HBGary Federal* y la publicación de varios miles de cuentas de correo de sus clientes. Estos agentes de amenaza son comúnmente denominados "hacktivistas" y no buscan atacar sitios web para obtener una ganancia financiera, sino para exponer al público información propiedad del gobierno y corporaciones.

Es importante para los CISOs observar que, de acuerdo al Reporte de Investigación de filtración de Datos de Verizon de 2012 (publicado el 22 de Marzo de 2012), aun cuando los *hacktivistas* causaron un pequeño porcentaje de incidentes (3%) afectando de esta manera una baja probabilidad, en general, representan el mayor impacto en cuanto al volumen de registros de datos comprometidos (58%). De acuerdo al reporte de Verizon, los hacktivistas son más propensos a atacar grandes organizaciones en lugar de las más pequeñas, dado que aquellas les generan un mayor retorno de inversión (desde la perspectiva del atacante) en términos de los datos que pueden ser comprometidos y divulgados al público. Los CISOs de grandes organizaciones privadas y públicas (por ejemplo, Gobierno) que tienen una marca pública y conocida deberían considerar el riesgo de los datos confidenciales (por ejemplo, nombres, apellidos y emails) y de los datos confidenciales de identificación personal (por ejemplo, nombres, apellidos y números de tarjetas) como un riesgo alto.

Los CISOs responsables de la seguridad de los sitios web, tanto gubernamentales como corporativos, que almacenan información confidencial y de identificación personal, posiblemente podrían convertirse en blanco de los hacktivistas por razones políticas y necesitan preocuparse además por el daño a la reputación resultante de la revelación al público de las vulnerabilidades del sitio web. Los hacktivistas a menudo atacan a los empleados y clientes de las organizaciones mediante la técnica del "*Spear Phishing"* y a sus sitios web con inyección SQL, *Cross-site Scripting (XSS)* y *exploits* de las vulnerabilidades de los sitios con el fin de robar información y publicarla online. Otro tipo de ataques por los que deben preocuparse los CISOs que administran los sitios de las corporaciones y el gobierno son los ataques por Denegación Distribuida de Servicio (DDoS por sus siglas en inglés). Normalmente los hacktivistas dirigen sus ataques a los sitios alojados en organizaciones financieras o de gobierno, mediante DDoS, por razones políticas. Por ejemplo, varios sitios de tarjetas de crédito, como *Mastercard* o *VISA* fueron atacados en 2011 por *Anonymous* usando DDoS en represalia por la eliminación de los operadores de *WikiLeaks* como clientes de *VISA* y *MasterCard*.

Ciberespías

Desde los años 2011 y 2012, además de los hacktivistas, estafadores y cibercriminales, hay una nueva clase de agentes de amenaza con los cuales deben lidiar los CISOs de organizaciones internacionales y gobiernos, compañías financieras, de defensa y alta tecnología. Se trata de los espías, que buscan

comprometer los sitios web para robar información secreta, información financiera restringida o de propiedad intelectual, como pueden ser los secretos de negocio de la compañía. Estos tipos de ataques a menudo implican el uso de herramientas de acceso remoto (RAT).

En su informe de 2011 sobre *ShadyRAT*, McAfee publicó que los ataques se mantuvieron durante varios años, iniciando a mediados de 2006, e impactando *"al menos 72 organizaciones, incluyendo contratistas de defensa, empresas de todo el mundo, las Naciones Unidas y el Comité Olímpico Internacional"*. Este tipo de ataques de ciberespionaje involucraron la utilización de *Spear Phishing* mediante emails conteniendo *exploits*, enviados a individuos con el nivel adecuado de acceso en la compañía, los cuales, al ser abiertos en un sistema sin los parches necesarios disparará la descarga del *malware*. El *malware* espía generalmente ejecuta e inicia un canal de comunicación del tipo *backdoor* hacia el servidor web e interpreta las instrucciones codificadas, ocultas y embebidas en el código de la página web. Además, las herramientas de ciberespionaje se pueden extender al comprometer servidores web vía inyección SQL, USBs infectados, y hardware o software infectado.

Más información:

http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

http://www.mcafee.com/uk/about/night-dragon.aspx

El análisis de algunos de los *malware* de ciberespionaje más recientemente utilizados indica que éstos son desarrollados en países involucrados en el ciberespionaje. En 2012, por ejemplo, Kaspersky Labs identificó un *malware* de ciberespionaje conocido como *Gauss*, que tiene similitudes en su código con otras herramientas de espionaje, tales como *Flame* y herramientas de ciberguerra, como *Stuxnet*. Según Kaspersky, Gauss está *"diseñado para robar información sensible, con un foco específico en contraseñas de navegadores, credenciales de cuentas de banca online, cookies, y configuraciones específicas de máquinas infectadas"*.

Agentes de Amenazas Persistentes Avanzadas (APT)

Frecuentemente, las actividades de ciberespionaje están asociadas con Amenazas Persistentes Avanzadas. Las APT se describen como avanzadas, es decir, utilizan métodos sofisticados, como los *exploit "Zero Day"*, y persistentes, es decir, los atacantes vuelven a los sistemas objetivo una y otra vez con una meta de largo plazo y logran su finalidad sin ser detectados.

Entre los APTs históricos se incluyen la *Operación Aurora*, cuyo blanco eran las compañías *Google, Juniper, Rackspace y Adobe*, así como las operaciones *Nitro, Lurid, Night Dragon, Stuxnet y DuQu*. Los CISOs de las organizaciones gubernamentales y de las corporaciones cuya principal preocupación es la protección de la propiedad intelectual y de la información restringida y confidencial, necesitan estar al tanto de que pueden convertirse en blancos de APTs que buscan atacar a empleados y clientes con *Spear Phishing* para infectar PCs con spyware, como también aprovechar vulnerabilidades en los sistemas y aplicaciones web mediante, por ejemplo, inyección SQL, para instalar y diseminar herramientas de espionaje.

Sobre Ataques y Vulnerabilidades

En esta sección de la guía describiremos cómo gestionar proactivamente los riesgos planteados por tipos específicos de ataques, como los agentes de amenaza cuyos motivos y metas de ataques han sido analizados previamente. Comúnmente la mitigación de riesgo consiste en reparar vulnerabilidades como así también en aplicar nuevas contramedidas. La elección de cuáles vulnerabilidades son críticas para mitigar comienza con la comprensión de los escenarios de amenazas y los motivos de los agentes de amenaza, especialmente en relación al *hacking* y el *malware*, y cómo estos agentes de amenaza podrían dirigir sus ataques a aplicaciones provocando que se vean comprometidos datos que son activos de la organización, como así también funciones críticas del negocio. Una herramienta crítica que los CISOs pueden usar para priorizar el riesgo es la utilización de *frameworks* o sistemas que clasifiquen los agentes de amenaza, los riesgos técnicos planteados por las vulnerabilidades en las aplicaciones que los agentes de amenaza buscan aprovechar, y los impactos en el negocio. El perfil de riesgo de cada aplicación difiere dependiendo de los valores inherentes del activo, del cual depende el impacto de negocio, y la probabilidad de que la aplicación pueda ser blanco de un agente de amenaza. Luego que las vulnerabilidades han sido priorizadas para su remediación, es importante considerar la efectividad de las contramedidas existentes e identificar cualquier brecha en las medidas de mitigación de riesgo que requieran que los CISOs consideren nuevas contramedidas. El análisis de la brechas del control se puede utilizar para determinar qué contramedidas necesitan ser implementadas, sobre la base de los principios de seguridad. El principio de defensa en profundidad puede ser usado para identificar brechas y estas brechas se pueden cubrir aplicando contramedidas. Para decidir en cuáles contramedidas invertir, los CISOs deberían considerar tanto el costo como la efectividad de las nuevas contramedidas en la mitigación del riesgo. Para decidir cuánto se debería gastar en contramedidas, se puede usar como criterio el cálculo de las potenciales pérdidas económicas como factor de probabilidad e impacto para determinar la obligación económica.

Ataques de Script Kiddies

En el caso de los *script kiddies*, los ataques para los cuales los CISOs deben estar preparados para defenderse son aquellos que buscan ejecutar *scripts* y herramientas de escaneo de vulnerabilidades cuya meta es identificar vulnerabilidades en las aplicaciones. Entre los objetivos de los *script kiddies* se encuentra el de sondear los sitios web en busca de vulnerabilidades comunes y cuando éstas son identificadas, a menudo las revelan al público para obtener fama y notoriedad.

Dado que con frecuencia buscan identificar vulnerabilidades y no necesariamente explotarlas para comprometer la información, el impacto para el negocio muchas veces tiene que ver con el daño a la reputación. Asumiendo que el descubrimiento de una vulnerabilidad se limita a la ejecución de herramientas de escaneo de vulnerabilidades, las principales vulnerabilidades por las cuales los CISOs necesitan preocuparse son aquellas más comunes, más precisamente, aquellas que el Top 10 de OWASP clasifica como “extendidas” y “fáciles de detectar”, como pueden ser *Cross-site Scripting* (2013-OWASP A3: XSS), *Cross Site Request Forgery* (2013-OWASP A8: CSRF) y configuraciones incorrectas de seguridad (2013-OWASP A5-Configuración de seguridad incorrecta).

Otras de estas vulnerabilidades son reveladas al público sin contactar a la organización cuya aplicación web se ha identificado como vulnerable. Cuando estas vulnerabilidades son publicadas, también pueden obviamente incrementar el riesgo para la organización ya que podrían ser aprovechadas para

comprometer el sitio web, como así también los datos. Por lo tanto, es importante que los CISOs presten atención a las amenazas que representan los *script kiddies* y remedien este tipo de vulnerabilidades. En algunos casos, estas vulnerabilidades se publican en una base de datos de acceso libre luego que los dueños de la vulnerabilidad han sido contactados y se les ha ofrecido ayuda para su remediación.

Por ejemplo, www.wssed.org recoge y valida información acerca de vulnerabilidades a XSS y las monitoriza públicamente su reparación, además de ofrecer un servicio para notificar a las organizaciones cuando estas vulnerabilidades han sido reveladas.

Los CISOs no pueden asumir que el daño a la reputación se restringe sólo a las vulnerabilidades de la organización que son reveladas al público, dado que éstas pueden ocasionalmente ser explotadas para hacer un *Deface* (desfiguración) del sitio web y publicar contenido no autorizado. Ejemplos de vulnerabilidades que pueden ser aprovechadas para *defacing* incluyen los *exploits* a vulnerabilidades de inyección de archivos como puede ser *Cross Frame Scripting* (XFS), parte del grupo (2013-OWASP A1: Inyección). Para mitigar el riesgo de estas vulnerabilidades, los CISOs necesitan invertir en herramientas de escaneo de vulnerabilidades para realizar pruebas antes que la aplicación web sea liberada al ambiente de producción. Adicionalmente, el foco debería estar en la construcción de software seguro, con componentes y librerías como OWASP ESAPI (Enterprise Security API) *"una librería de control de seguridad de aplicaciones web libre, de código abierto, que facilita a los programadores la escritura de aplicaciones de bajo riesgo".*

Además de invertir en pruebas de vulnerabilidad y software seguro para mitigar el riesgo de impactos relacionados a la reputación, los CISOs pueden también invertir en medidas de monitoreo y detección de ataques, como los firewalls de aplicaciones web *(WAF – Web Applicacition Firewall).* Dado que este tipo de vulnerabilidades son fáciles de identificar y las más extendidas entre las aplicaciones web, también son las que más se prueban en los sitios web. Por lo tanto, saber cuándo una aplicación web es blanco de un ataque *script kiddie* puede ser útil para controlar aún más las actividades y emitir alertas en caso que los ataques no sólo se limiten a sondear el sitio web sino a intentar explotar la vulnerabilidad para comprometer la información.

Ataques de estafadores y cibercriminales

Los estafadores y cibercriminales atacan aquellos sitios web que les representan una oportunidad para obtener una ganancia económica. Por ejemplo, los sitios web que procesan pagos con tarjeta de crédito, como las webs de *e-commerce*, sitios que permiten acceder a información de tarjetas de crédito, débito y de cuentas bancarias y realizar transacciones financieras y transferencias electrónicas, tales como las páginas de banca online, y cualquier sitio web que almacene y recoja información privada, como puede ser la información de identificación personal de un individuo. Además de cometer fraude al atacar las transacciones financieras tales como pagos y transferencias de dinero soportadas por estas webs, otros tipos de ataques buscados por los estafadores son aquellos que permiten obtener acceso no autorizado a información sensible, como datos de tarjetas de crédito y débito, que pueden ser utilizados para transacciones sin tarjeta o para falsificar tarjetas, o a información de identificación personal que puede usarse para hacerse pasar por la víctima y suplantar su identidad.

Teniendo en cuenta los objetivos financieros de estos atacantes, cualquier vulnerabilidad que le permita al estafador/cibercriminal controlar pagos y transferencias de dinero, como también la obtención de acceso no autorizado a datos sensibles, es muy probable que se convierta en el blanco de un ataque. Primero y principal, estas vulnerabilidades pueden ser explotadas para ganar acceso no autorizado a aplicaciones financieras y de *e-commerce*. Estas incluyen aprovechamiento de vulnerabilidades relacionadas con la débil autenticación y gestión de sesiones (2013-OWASP A2: Filtración en la Autenticación y Gestión de Sesiones) dado que el *exploit* podría comprometer las credenciales para acceder a las aplicaciones web, tales como nombre de usuario y contraseña, como también ID de sesiones para hacerse pasar por la víctima. Otros posibles *exploits* de vulnerabilidades podrían incluir el aprovechamiento de la vulnerabilidad al Cross Site Request Forgery (2013-OWASP A8: CSRF) para tomar la sesión y realizar transacciones financieras no autorizadas, como pagos y transferencias de dinero. Entre las más peligrosas vulnerabilidades a las aplicaciones web que los estafadores y cibercriminales podrían buscar explotar se encuentra la vulnerabilidad a la Inyección SQL (2013-OWASP A1: Inyección), acceso a datos sensibles mediante la manipulación de parámetros no protegidos, tales como referencias directas (2013-OWASP A4), fallos por parte de la aplicación web para restringir el acceso a URL (2013-OWASP A10), controles criptográficos pobres o inexistentes para proteger información confidencial almacenada o en tránsito (2013-OWASP A5 y 2013-OWASP A6).

En el caso en que los CISOs son responsables de gestionar el riesgo de sitios web intrínsecamente peligrosos, como los de *e-commerce*, banca online, y sitios que procesan información confidencial y personal, por ejemplo para seguros, préstamos y créditos, necesitan enfocarse en el prueba y corrección de estas vulnerabilidades dado que son las que más probablemente sean explotadas y causen el mayor impacto de negocio a la organización.

Se pueden incorporar reglas de detección de intrusos (IDS por sus siglas en inglés) de capa de aplicación en las aplicaciones web, como en ESAPI OWASP, o en el servidor web, como en el caso de los firewalls de aplicaciones web (WAF), para registrar y monitorear actividades sospechosas y disparar alertas por potenciales intentos de fraude.

El análisis y modelado de amenazas a aplicaciones es la actividad clave para determinar la exposición de aplicaciones a amenazas y cómo proteger los datos del impacto de estas amenazas. Desde la perspectiva del análisis de amenazas, luego que los agentes de amenaza y sus motivos y ataques son identificados es importante analizar los probables escenarios de ataque, identificar los vectores de ataque utilizados y las vulnerabilidades que pueden ser explotadas. Un árbol de ataque puede ayudar a traducir los objetivos del atacante en los medios para alcanzar estos objetivos. Desde la perspectiva del atacante, la meta principal es la persecución de ataques baratos y fáciles de llevar a cabo y con la mayor probabilidad de tener éxito, en lugar de lo contrario. Por ejemplo, considerar que las tarjetas de crédito e información de cuentas pueden ser adquiridas en el mercado negro por las organizaciones de cibercriminales, y si esta práctica resultará más fácil, económica y menos riesgosa para los estafadores que intervenir una aplicación, esto es probablemente lo que los estafadores harán. Si en cambio el sitio web que almacena datos de tarjetas de crédito tiene vulnerabilidades que son fácilmente aprovechables para obtener información de las tarjetas de crédito, probablemente los estafadores atacarán este sitio primero. Desde la perspectiva de los CISOs, se puede justificar la reparación de las vulnerabilidades que pueden ser aprovechadas por un

estafador desde la perspectiva de la reducción de oportunidades de que éstas sean aprovechadas. Los árboles de ataque también pueden ser útiles para entender la realización de posibles amenazas mediante el seguimiento de los mismos patrones de ataque utilizados por un estafador. Esto permite identificar cualquier debilidad o punto de menor resistencia que pueda perseguir un atacante. Por ejemplo, si las aplicaciones son accesibles a través de diferentes interfaces de datos o canales, el estafador se enfocará en aquellos que ofrecen menor resistencia y mayor oportunidad para comprometer los datos, tales como los canales móviles, en lugar de los canales web. Tal como indica uno de los principios de seguridad "eres tan seguro como tu punto más débil", indicar dónde se encuentran estos puntos débiles es crítico en la evaluación de seguridad de cualquier sistema expuesto a ataques, incluyendo las aplicaciones. La identificación de los puntos de entrada de datos para una aplicación dada, interna o externa, es una tarea crítica para determinar la superficie de ataque de la aplicación y usualmente se identifica como parte de la evaluación del modelado de amenazas de la aplicación.

Otro análisis crítico que forma parte del modelado de amenazas de la aplicación consiste en analizar qué amenazas pueden hacerse realidad aprovechando cierta clase de vulnerabilidades de modo que los CISOs puedan enfocarse en aplicar las contramedidas para mitigar estas vulnerabilidades. Un análisis en profundidad del impacto de las amenazas al software y aplicaciones se puede llevar delante de mejor manera utilizando árboles de amenazas y *frameworks* de riesgo. Estos son métodos formales que permiten mapear las amenazas a las vulnerabilidades y contramedidas. OWASP ha incluido guías para el modelado de amenazas de aplicaciones, así como referencia a los *frameworks* de "árboles de amenaza" y "amenazas-contramedidas" que pueden utilizarse para este análisis de amenazas.

Ataques a la Lógica de Negocios

Un tipo de vulnerabilidades a menudo explotadas por los estafadores y no probadas en las aplicaciones son las fallas de diseño y las vulnerabilidades lógicas. Una de las principales razones por las cuales éstas no son probadas es que las herramientas automatizadas de escaneo de vulnerabilidades no comprenden la lógica de negocio de la aplicación como para estar en condiciones de identificarla. En ausencia de pruebas manuales específicas de seguridad que prueben por ejemplo posibles casos de uso y abuso de la aplicación, estas vulnerabilidades muy probablemente no son identificadas ni corregidas y pueden causar serias pérdidas económicas e impactos al negocio cuando se las explota. Ejemplos de ataques que aprovechan estas vulnerabilidades son los llamados "ataques a la lógica de negocios". Entre los ejemplos de ataques a la lógica de negocios que aprovechan fallas en el diseño de aplicaciones se incluyen el salteo de los controles de acceso basados en roles para recolectar información confidencial no autorizada y realizar transacciones financieras no autorizadas, atacando la lógica de los carritos de compra para alterar el precio de un ítem antes de pagar la cuenta y alterar la dirección de envío de un ítem adquirido antes de que se completen las validaciones de la tarjeta de crédito durante el proceso de pago. Generalmente, los ataques a la lógica de negocios explotan vulnerabilidades de validación, tales como la falta de algún parámetro de validación en las transacciones de negocio (por ejemplo, RolID, ReglaID, PrecioID), controles débiles en el flujo de las transacciones, fallas al confirmar transacciones financieras antes que todos los chequeos se hayan completado y errores de configuración en los Controles de Acceso Basados en Roles *(RBAC - Role Based Access Controls)* y reglas de políticas de negocio. La mayoría de estas vulnerabilidades necesitan ser probadas manualmente en base a casos de mal uso, una técnica considerada parte del modelado de

amenazas a las aplicaciones y también documentada en la metodología de modelado de amenazas de aplicaciones de OWASP.

Con frecuencia los defectos de diseño radican en cómo se diseñan los controles de seguridad de las aplicaciones y requieren pruebas específicas de seguridad para ser identificados. Por ejemplo, este es el caso de defectos en el diseño de reinicios de contraseñas, usos de preguntas de seguridad adivinables en la autenticación multi-factor, fallas en la gestión de sesiones que permiten sesiones que no expiran o no se cierran, errores en los controles de autorización y acceso. Estas fallas de diseño usualmente se clasifican como vulnerabilidades comunes, como la filtración en la autenticación y gestión de sesiones (2013-OWASP A2), Referencia directa insegura a objetos (OWASP A4), configuraciones de seguridad incorrectas (OWASP A5) y ausencia de control de acceso a funciones (OWASP A7), y pueden ser probadas mediante pruebas manuales específicas. OWASP, además, proporciona directrices específicas para el control de vulnerabilidades de seguridad en aplicaciones. Un tipo de vulnerabilidades que es también aprovechada por los ataques a la lógica de negocios incluye la Anti-Automatización Insuficiente (WASC 21).

WASC *(Web Application Secure Consortium)* es el Consorcio de Seguridad en Aplicaciones Web.

Más información:

http://projects.webappsec.org/w/page/13246978/Threat%20Classification

http://projects.webappsec.org/w/page/13246975/Threat%20Classification%20Taxonomy%20Cross%20Reference%20View

Esta es una vulnerabilidad que puede ser explotada por atacantes para ejecutar spam sobre registros online, publicación de información mediante herramientas de automatización, pero también para fraude, como la enumeración y validación automática de datos de tarjetas de crédito, números y PINs, usando *scripts* automatizados que prueban los códigos de error y respuestas de éxito de las aplicaciones.

El criterio más importante para los CISOs en la protección contra los ataques a la lógica de negocio es no asumir que el control de defectos de diseño y errores en la lógica está cubierto con las pruebas de seguridad y escaneos de vulnerabilidades normales. Las fallas en diseño y lógica de negocios constituyen una clase de vulnerabilidades que requieren pruebas de seguridad específicas, utilizando casos de uso y abuso, producidas por equipos de seguridad involucrados específicamente en aplicaciones de modelado de amenazas. Los CISOs deberían considerar la inversión en procesos de modelado de amenazas a las aplicaciones, específicamente en la identificación y testeo de este tipo de vulnerabilidades cuando éstas no son identificadas ni testeadas por otros procesos de seguridad.

Ataques de Phishing

Dado que a menudo una de las técnicas de ataque adoptadas por los estafadores y cibercriminales consiste en aplicar ingeniería social a la víctima para que ingrese en enlaces maliciosos que contienen *malware*, las vulnerabilidades en aplicaciones web que facilitan el Phishing sobre la víctima también pueden convertirse en blanco de ataque. Estos ataques incluyen la utilización de vulnerabilidades de *Cross-site Scripting* para correr *scripts* maliciosos que pueden robar *cookies* o ejecutar *keyloggers*. Otras vulnerabilidades de las aplicaciones web que pueden ser utilizadas para engañar a la víctima para que visite

un sitio malicioso y se vea infectada con *malware* es 2013-OWASP A10: redireccionamientos y reenvíos no validados.

Otras vulnerabilidades que facilitan la instalación de *malware* mediante *phishing* incluyen los *exploits* XFS *(Cross Frame Scripting)* para ataques de captura de clic. Estos ataques engañan a la víctima para que realice acciones no deseadas haciendo *clic* en un enlace oculto y malicioso.

Más información: https://www.owasp.org/index.php/Cross_Frame_Scripting

Estas son vulnerabilidades que los CISOs deben priorizar para su remediación ya que facilitan la instalación de *malware* en el sistema de la víctima. Puesto que la identificación de estas vulnerabilidades con frecuencia requiere pruebas de seguridad manuales, como por ejemplo pruebas de *Ethical Hacking y penetration Test*, como también revisión manual del código fuente para identificar estas vulnerabilidades en el código fuente, es crítico para los CISOs invertir en la contratación y formación de *testers* de penetración como también en desarrolladores de software con experiencia en codificación segura, procesos de revisión de código seguro, estándares de codificación segura y herramientas estáticas de análisis de código fuente.

Ataques "Man in the Browser" y "Man in the Middle"

Desafortunadamente, identificar y corregir estas vulnerabilidades no constituye una garantía de inmunidad a ataques de estafadores, sino que presenta un mínimo nivel de garantía de seguridad de software. El software resiliente de hoy en día requiere que los CISOs consideren invertir en contramedidas para proteger las aplicaciones web de otra clase de ataques tales como *"Man in the Browser" (MitB)* y *"Man in the Middle" (MitM).* Valiéndose de MitB los estafadores pueden recolectar información confidencial, datos de autenticación y tarjetas de crédito de la víctima al inyectar campos HTML en el browser, excediendo el control de la aplicación web. Adicionalmente, las credenciales de acceso *(login)* de la víctima son recogidas a través de *keyloggers* y enviadas al estafador para que se haga pasar por la víctima. Por ejemplo, en una sesión de transferencia de dinero el estafador se conectará al sistema de la víctima desde su servidor de comando y control y tomará posesión de la sesión para transferir dinero a una cuenta bajo control del atacante. Mediante MitM los estafadores podrán redirigir a la víctima a un sitio malicioso cuyo tráfico web y los datos estarán bajo el control del atacante.

Para proteger las aplicaciones financieras y de *e-commerce* de ataques MitB y MitM, los CISOs necesitan adoptar un enfoque de defensa en profundidad que incluye diferentes capas de control, la capa de la PC del cliente, la capa del servidor web y servidor de aplicaciones web y las capas de bases de datos y servicios. En la capa de la PC del cliente es muy importante invertir en informar y concientizar sobre las amenazas que representa el *malware*. Medidas simples tales como mantener las PCs y navegadores actualizados y con las actualizaciones y parches correspondientes, así como también fortalecerlas con la implementación de privilegios limitados de usuarios y la instalación de un acotado número de aplicaciones (por ejemplo, idealmente sin correos ni redes sociales instalado en la PC), pueden limitar las chances de infecciones por *malware*. Información específica embebida en las páginas de *logueo* de los sitios web pueden mantener a los usuarios informados sobre los riesgos que representa el *malware* cada vez que inician sesión.

Adicionalmente, los CISOs pueden invertir en la provisión gratuita de software antimalware a sus clientes, dado que estos son más efectivos en la detección y protección de la PC que el tradicional antivirus. Suponiendo que la PC o navegador del cliente ha sido infectada con *malware* bancario, las contramedidas adicionales que los CISOs pueden considerar incluyen el agregado de validaciones y controles adicionales de identidad para las transacciones de alto riesgo, como por ejemplo para el caso de transferencias bancarias y pagos. Entre estos controles se incluyen pago positivo, doble verificación y autorización, y detección de anomalías y fraudes. Una vez que se supone que el canal online fue comprometido por el atacante, la utilización de validación/autenticación de transacción fuera de banda para pagos y transacciones financieras con confirmación de notificación de dos vías mediante canales independientes de voz y mensajes pone al ciudadano/cliente/usuario/empleado en control de la transacción y le permite rechazar cualquier transacción que no pueda ser confirmada o cuya integridad de parámetros haya sido modificada por el atacante y no pueda ser validada. Medidas de detección tales como la recepción de alertas fuera de banda para transacciones financieras así como también el registro, auditoría y monitoreo de tráfico web mediante WAF y SIEM, y el uso de detección de comportamiento fraudulento para encontrar tasas/parámetros de transacciones anormales, puede también permitir a los CISOs recibir reportes de detección de *malware* en base a eventos transaccionales y recomendar acciones proactivas para limitar el impacto de pérdidas económicas (por ejemplo, suspender las cuentas que se marcaron como sospechosas hasta una nueva validación).

Al decidir qué contramedidas implementar para mitigar el riesgo de ataques MitB y MitM, los CISOs podrían necesitar realizar un balance entre el riesgo, la efectividad de las contramedidas y los costos. Las contramedidas que cuestan menos y mitigan la mayor cantidad de ataques MitB y MitM pueden ser priorizadas al momento de invertir. Normalmente el software antimalware basado en cliente puede ser efectivo para mitigar riesgos de *malware* en el punto de entrada y es bastante económico para adquirir y desplegar si este costo no incluye el costo total de mantenimiento de la solución para una gran cantidad de usuarios. Las campañas de concientización a usuarios sobre la seguridad pueden ser las medidas menos caras pero pueden no resultar tan efectivas ya que a menudo los usuarios no prestan atención a las advertencias de seguridad. La adquisición e implementación de autenticación y validación/autorización fuera de banda de transacciones puede resultar costoso pero ofrece una potente mitigación contra ataques MitM y puede ser una opción viable para proteger transacciones de alto riesgo. La instalación de sistemas de detección de fraude para monitorear tráfico malicioso puede ser cara para implementar y mantener y puede requerir justificación para cada caso. Por ejemplo, si se sabe que ciertas aplicaciones web se encuentran constantemente bajo ataque por *malware* e impactadas por fraude, la inversión en sistemas de detección de fraude puede resultar justificable debido a la probada capacidad de dichos sistemas para detectar ataques antes que mediante otros métodos (por ejemplo, analizando los *logs* de transacciones de los SIEMs). Los CISOs pueden seleccionar cuáles aplicaciones web deberían estar dentro del alcance de la remediación de vulnerabilidades buscadas por los estafadores y la implementación de nuevas contramedidas contra ataques MitB y MitM basándose en el perfil de riesgo de la aplicación. El perfil de riesgo de la aplicación web puede ser una función del valor de los activos de datos y del riesgo de las transacciones que la aplicación web provee a los clientes. Un análisis de brechas de control puede ser utilizado para identificar grietas en los controles de protección y detección y para determinar el grado de mitigación de riesgo que se puede obtener cuando estos controles son implementados. Una vez que las

medidas de seguridad se han adoptado, un cálculo de los riesgos residuales pone de manifiesto si el riesgo puede ser aceptado o necesita ser reducido aún más desplegando controles adicionales.

Ataques de Denegación de Servicio

Los ataques de denegación de servicio (DoS por sus siglas en inglés) pueden impactar severamente la disponibilidad del sitio web a los usuarios. Dependiendo del tipo de servicios que el sitio provee a los clientes, una pérdida en el servicio puede resultar en una pérdida considerable de ingresos para la organización. Los CISOs deberían considerar la mitigación del riesgo de ataques de denegación de servicio como prioridad máxima, especialmente para aplicaciones web que generan ingresos considerables y cuya disponibilidad se considera crítica para la organización.

Los ataques DoS pueden resultar facilitados por vulnerabilidades en las aplicaciones web, OWASP incluyó a DoS dentro del Top 10 de OWASP de vulnerabilidades en 2004 (2004-OWASP A9: DoS) pero ésta salió del ranking en 2007 debido al ranking MITRE de 2006. De todos modos, aún sin ser parte del Top 10 de OWASP en 2010, dependiendo de la exposición y el valor de los activos impactados, las vulnerabilidades de denegación de servicio podrían representar un alto riesgo para la organización y una prioridad para la mitigación. En el nivel de aplicación, una denegación de servicio podría ser el resultado de vulnerabilidades 2013-OWASP A1: Inyección, específicamente vulnerabilidades que permiten inyecciones de comandos SQL, XPATH y LDAP, que pueden provocar la caída de la aplicación web. En el nivel de usuario, los ataques por denegación de servicio pueden apuntar a la usabilidad de la aplicación por parte de un usuario registrado, por ejemplo los atacantes pueden utilizar scripts para bloquear cuentas de usuario al adivinar IDs válidos de usuarios y forzar las cuentas de usuarios a que se bloqueen luego de varios intentos erróneos de *logueo*. En ausencia de bloqueos temporales de cuentas (por ejemplo, la cuenta del usuario se desbloqueará automáticamente en 24 hs), este ataque causa que los usuarios no puedan loguearse. Un efecto colateral de esto son los clientes llamando al servicio de atención al cliente en busca de que se desbloqueen sus cuentas, posiblemente desbordando los *call centers* con llamadas para desbloqueos de cuentas.

A nivel del código fuente, los ataques de DoS podrían ocurrir por vectores de ataque que se aprovechan de cuestiones relacionadas con codificación insegura, causando sobrecarga de los recursos computacionales. Se trata de problemas de codificación insegura tales como la no liberación de memoria desde recursos asignados (por ejemplo memoria de objetos) al salir de programas, causando como resultado que la aplicación falle. Entre los ejemplos se incluyen el aprovechamiento del código inseguro con referencias a punteros NULL y terminaciones inadecuadas, aprovechar excepciones no capturadas, y explotar debilidades en el procesamiento de archivos XML causando que el proceso de análisis o *parsing* agote la memoria con archivos XML recursivos maliciosos. En los casos en los que el código fuente de la aplicación está escrito en lenguajes de programación que permiten a los programadores gestionar memoria, tales como C o C++, los errores de codificación en la administración de las adjudicaciones de memoria y el uso de funciones no seguras puede exponer al código fuente y la aplicación a posibles vulnerabilidades de desbordamiento de búfer y causar que la aplicación se corrompa o tomen control sobre ella. Las vulnerabilidades de desbordamiento de búfer pueden ser también aprovechadas a nivel de servidor debido a ataques que buscan comprometer servidores web y de aplicaciones que no tienen los parches necesarios y son vulnerables a desbordamiento de búfer. Los CISOs necesitan asegurarse que las

vulnerabilidades en las aplicaciones y código fuente que podrían ser explotadas por denegación de servicio se encuentran dentro del alcance de las pruebas de seguridad ya que éstas están generalmente cubiertas por herramientas de pruebas de seguridad de aplicaciones estáticas y dinámicas.

Ataques de Denegación de Servicio Distribuida

En la capa 4 de transporte del modelo OSI, los ataques por denegación de servicio típicamente buscan explotar vulnerabilidades en los protocolos de la capa de red, por ejemplo suplantando paquetes con el fin de inundar el tráfico de red. Un tipo de ataque por denegación de servicio, llamado Denegación de Servicio Distribuida (DDoS, por sus siglas en inglés) generalmente busca desbordar el servidor web blanco del ataque con un nivel inusualmente alto de tráfico de datos enviados desde una red coordinada y controlada de bots. Debido al inusual tráfico de red que se le pide al servidor web que maneje, éste tal vez no sea capaz de servir todas las peticiones en la red y rechace las solicitudes de servicio a los usuarios de la aplicación. En la capa más exterior, que constituye el borde de la Internet, es posible filtrar el tráfico malicioso antes que ataque la capa interna, el centro de datos donde se aloja la aplicación y se hayan implementadas otras contramedidas. Cuando tienen lugar los ataques DDoS, la defensa en profundidad permite que la organización sea alertada y prepare nuevas reglas de filtrado y bloqueo para el tráfico malicioso. Pero aplicar el principio de defensa en profundidad, incluso cuando puede reducir la velocidad de los atacantes, no es suficiente y se necesitan seguir otros principios de seguridad defensiva cuando se despliegan contramedidas, como por ejemplo considerar el control de seguridad en el punto más débil, considerar la simplicidad y apertura del mecanismo de seguridad para que pueda ser administrado y examinado de manera segura, aplicar la seguridad del mínimo privilegio para el acceso de usuarios, todos esenciales para la confiabilidad del diseño de los controles de seguridad de aplicaciones y software.

Los ataques de DDoS más conocidos, originados en *bots*, incluyen ataques *"Ping de la Muerte"* que crean paquetes electrónicos enormes y los envían a las víctimas; *"Mailbomb"* que envían cantidades masivas de correos, congestionando los servidores de correos; *"Smurf Attack"* que envían mensajes ICMP *(Internet Control Message Protocol)* a otros equipos "reflectores" para amplificar el ataque y; *"Teardrop"* que envían piezas deformadas de paquetes que hacen caer al sistema que intenta recombinarlas.

Hoy en día los *script kiddies*, hacktivistas, cibercriminales y atacantes patrocinados por el estado utilizan herramientas de código abierto para realizar DDoS contra posibles blancos. Los blancos típicos, más probables de los ataques DDoS son organizaciones públicas y privadas con alta visibilidad. Los objetivos generales de estos ataques son causar interrupciones, llamar la atención y dañar la reputación de la compañía. Los motivos específicos para llevar adelante ataques DDoS varían dependiendo del tipo de agentes de amenaza y sus motivos. Los *script kiddies* pueden usar ataques DDoS con motivos oportunistas, tales como aprovechar vulnerabilidades a la denegación de servicio y ganar notoriedad, los hacktivistas pueden utilizar estos ataques por razones políticas y para atraer la atención de los medios de comunicación públicos. Los estafadores y cibercriminales pueden realizar ataques DDoS para desviar la atención de otros ataques, como en el caso de un ataque de toma de control de una cuenta para defraudar clientes de banca online. Los cibercriminales patrocinados por el estado podrían llevar adelante estos ataques por razones económicas y militares como por ejemplo en el caso de interrupción de la operación de un sitio web operado por el gobierno de otro país.

El impacto de los ataques DDoS en cuanto a reputación y pérdida de ingresos en organizaciones privadas y públicas varía mucho dependiendo del tipo de sitio web blanco del ataque, la duración del ataque y el número de individuos y clientes afectados. El impacto al negocio de los ataques DDoS puede ser estimado como función de la pérdida de ingresos causado por la detención del servicio a los clientes e individuos cuando el sitio web ha sido derribado. De acuerdo al "Segundo Estudio Anual de 2011 del *Ponemon Institute* sobre Costo del Cibercrimen" que involucró 50 organizaciones y compañías de EE.UU., el impacto de DDoS se estima en un costo anual promedio de U$D 187.506. Este costo es ponderado por la frecuencia de los incidentes de ataque de todas las compañías evaluadas. Otra encuesta realizada por CA Technologies, que incluye 200 compañías de Norteamérica y Europa, estimó que el costo del tiempo de inactividad provocado por la Denegación de Servicio es alrededor de U$D 150.000 al año. Estas estimaciones de costos son simplemente órdenes de magnitud dado que los impactos al negocio varían mucho dependiendo del tipo de servicios online afectados y del volumen del negocio online comprometido por los ataques DDoS. Para una compañía de negocios de gran escala, como Amazon, por ejemplo, cuyos negocios generaron U$S 48 mil millones en ingresos en el año 2011, asumiendo que la mayoría de los ingresos de Amazon se generan online, una denegación de servicio de sólo una hora por un ataque DDoS podría provocar pérdidas en los ingresos de millones de dólares. Los CISOs de compañías que generan una parte significativa de sus ganancias a través de sitios online como en el caso del *e-commerce* y los sitios web financieros, necesitan considerar la amenaza de la denegación de servicio de los ataques DDoS como máxima prioridad para la mitigación de riesgo y pensar en la inversión en medidas de seguridad para mitigar el riesgo de estos ataques.

Hoy en día los ataques DDoS se encuentran ampliamente extendidos. La razón por la que estos ataques son tan extendidos se debe a la disponibilidad de herramientas para DDoS y de botnets que se alquilan para llevar adelante estos ataques, a un costo relativamente bajo para el atacante. De acuerdo al "Modelado de los incentivos económicos de los ataques DDoS: Caso de Estudio Femtocell, Vicente Segura y Javier Lahuerta, Departamento de Redes y Seguridad de Servicios de Telefónica" por ejemplo, el costo de alquilar una botnet para ataques DDoS es de aproximadamente U$S 100 por día por 1 Gbps de ancho de banda. Los CISOs también necesitan ser conscientes de la escalada de la amenaza DDoS a partir de que la severidad y sofisticación de los ataques DDoS también están creciendo. De acuerdo al "Sexto Informe Anual de Seguridad en Infraestructura Mundial, de *Arbor Networks*, 2011", comparando con DDoS de 6 años antes, el poder de los ataques DDoS creció 10 veces alcanzando anchos de banda de 100 Gbps. Esta escalada del poder de DDoS no puede explicarse solamente por la sofisticación de las herramientas DDoS, sino también por las nuevas técnicas de ataque que buscan amplificar el ancho de banda de los ataques.

Estas nuevas técnicas de ataques DDoS consisten en Ataques de Denegación de Servicio por Reflectores Distribuidos *(DRDoS - Distributed Reflector Denial of Service Attacks).* Los ataques DRDoS simulan la dirección IP de origen de la víctima y realizan consultas DNS enviadas hacia *DNS resolvers* abiertos, dado que los DNS abiertos responden al sistema de la víctima con paquetes de datos más grandes que la solicitud, pueden ser utilizados para amplificar aún más el ancho de banda cuando miles de *bots* están realizando consultas a miles de servidores DNS.

Las medidas tradicionales de capa de red para protección de ataques DDoS incluyen configurar *routers* para examinar y descartar paquetes, filtrar direcciones IP, configurar límites de velocidad y aplicar filtrado

de red de ingreso y egreso. Desafortunadamente hoy en día la mayoría de estas contramedidas no son suficientes para protegerse de ataques DDoS y DRDoS con anchos de banda de 100 Gbps. Para protegerse de los ataques más poderosos de DDoS y DRDoS, los CISOs de organizaciones cuyos servidores de alta disponibilidad se encuentran bajo la amenaza de ataques DDoS y DRDoS de gran ancho de banda, necesitan considerar invertir en segmentación de red, *hostear* parte del contenido estático del sitio web en Redes de Entrega de Contenido *(CDN - Content Delivery Networks)* y utilizar servicios de terceros, basados en la nube, para protección de DDoS, con acuerdos sobre el nivel de servicio para incrementar el ancho de banda del tráfico en caso que el mismo se esté consumiendo durante un ataque DDoS.

II-6 Mitigando los riesgos inherentes a las nuevas tecnologías de aplicación

El objetivo de este capítulo es guiar al CISO en la consideración de los riesgos de seguridad que se le plantean a la organización en la adopción de nuevas tecnologías. El término "Tecnologías" se utiliza aquí para incluir ejemplos de tecnologías que impactan en las aplicaciones, tales como tecnologías móviles, tecnologías Web 2.0, y software de *Cloud Computing* como servicio (SaaS - Software as a Service).

Dado que las tecnologías evolucionan, es importante para el CISO entender los riesgos de seguridad introducidos al adoptar estas nuevas tecnologías, y que las mismas pueden representar nuevas oportunidades para los atacantes de atacar tanto las aplicaciones como los datos. El incremento del riesgo para las aplicaciones a causa de la adopción de nuevas tecnologías incluye el incremento de la superficie de exposición/ataque tales como el caso de la extensión de las aplicaciones para dispositivos móviles, la introducción de un nuevo tipo de vulnerabilidad de cliente y servidor, como es el caso de la Web 2.0 y el incremento del riesgo de pérdida de datos e integridad de transacciones debidos al uso de Cloud Computing. A fin de apuntar a la mitigación de los riesgos debidos a la adopción de dichas tecnologías, el CISO necesita tener una imagen clara de los riesgos que son introducidos y decidir invertir en un nuevo tipo de evaluación de seguridad de aplicaciones, herramientas y medidas de seguridad para mitigar los riesgos.

Gestionando el riesgo de aplicaciones móviles

La seguridad de las aplicaciones móviles es una preocupación particular actual para la mayoría de las organizaciones: sobre todo debido al crecimiento exponencial de la adopción de teléfonos inteligentes y tabletas, tanto para uso personal como profesional. Desde la perspectiva de la seguridad en aplicaciones, el acceso a las aplicaciones empresariales desde dispositivos móviles aumenta la posibilidad que los agentes de amenaza ataquen a las aplicaciones y los datos que se pueden almacenar en los teléfonos móviles. Aquellos comprometidos con *malware*, por ejemplo, que exponen tanto la aplicación cliente instalada en el dispositivo, así como el servidor de aplicación al que se puede acceder a través del dispositivo móvil. Diferentes canales de comunicación móviles también se pueden atacar incluyendo canales de Internet para acceder a redes Wifi, MMS, mensajería SMS y GSM 2G, 3G, redes inalámbricas 4G. Empresas cuyas aplicaciones se puede acceder a través de dispositivos móviles deben tener en cuenta la exposición que los ataques incrementada por la adopción de esta tecnología. Una medida de seguridad importante es la exigencia de una evaluación de vulnerabilidades específica para comprobar la seguridad de las aplicaciones móviles y la protección de los datos confidenciales que se almacenan en el dispositivo móvil. El requisito para cifrar todos los datos confidenciales y de autenticación que se almacena el

dispositivo, por ejemplo, podría ser requerido para el cumplimiento de normas y políticas de seguridad móvil internas. La exposición de los servicios web que se puede acceder a través de una aplicación móvil también necesita de una prueba de vulnerabilidades. A menudo, la organización podría decidir evitar el riesgo de que las aplicaciones móviles tomen el riesgo de efectuar operaciones financieras, tales como transferencias de dinero y pago cuando la autenticación en el dispositivo no se considera tan fuerte como la que está disponible para aplicaciones basadas en PC. En algunos casos, los controles de seguridad de los dispositivos podrían considerarse no lo suficiente seguros, como cuando se utiliza el cifrado del basada en dispositivo (por ejemplo llavero iOS), ya que este puede ser quebrado por fuerza bruta cuando el usuario no está en posesión del dispositivo móvil. Estas son consideraciones importantes de riesgo y pueden ser aplicadas al requerir a la organización de desarrollo seguir las normas de seguridad para el diseño de aplicaciones móviles.

Además del compromiso de un dispositivo debido a una pérdida o robo, otro riesgo a tener en cuenta es el compromiso del dispositivo móvil por *malware* diseñado para instalar *keyloggers*, robar las credenciales del usuario y redireccionar estas credenciales al servidor del atacante. Hoy en día las aplicaciones móviles representan una oportunidad para atacar a las aplicaciones instaladas en los dispositivos móviles a través de diferentes canales de comunicación como correos electrónicos, redes sociales, *streaming* de audio y vídeo, mensajería instantánea y la web. Ejemplos de oportunidades para que un atacante comprometa dispositivos móviles con *malware*, incluye la ingeniería social a los usuarios para hacer clic en enlaces maliciosos en correos electrónicos y mensajes que transportan una carga *(payload)* con *malware* para instalar software espía (*spyware*) y herramientas de acceso remoto (RAT). La sofisticación del *malware* móvil actual es tal que algunos están diseñados específicamente para atacar los *tokens* temporales enviados al teléfono del usuario para autenticar sitios web de banca online. Este tipo de *malware* tiene la capacidad de realizar ataques *Man in the Mobile (MitMo)* y redirigir los *tokens* de autenticación de un solo uso al teléfono móvil del autor del fraude y que éste lo utilice para autenticarse en el sitio de banca online, con el nombre de usuario y contraseña correspondiente. Otra vía de ataque para aplicaciones móviles es subir aplicaciones maliciosas en los almacenes de aplicaciones móviles (por ejemplo Google Play y Apple Store) y atraer a usuarios móviles a descargar aplicaciones falsas de dichas tiendas. Dado que las aplicaciones para Android y iOS componen casi el 90% de las aplicaciones a nivel mundial, atacar estas tiendas representa la mejor oportunidad para que un atacante propague *malware* móvil a un gran número de usuarios. Normalmente los controles de seguridad que se realizan en estas tiendas, especialmente en el caso de Apple, mitigan estos riesgos pero la descarga de aplicaciones de sitios cuyo origen no siempre puedan ser validados por los usuarios debe considerarse un riesgo.

Sin embargo, se puede lograr una mayor seguridad con sólo seguir las medidas de seguridad básicas. En algunos casos, la falta de medidas básicas de seguridad por defecto en las aplicaciones, tales como el uso de PINs para evitar el acceso no autorizado y permitir la instalación de aplicaciones que requieran de *"Jail Break"* el teléfono, representa un mayor riesgo tanto para los datos como para las aplicaciones móviles que residen en el dispositivo. Una buena medida preventiva es mantener informados a los usuarios de las amenazas dirigidas, y recomendarles seguir las medidas de seguridad básicas. Un buen recurso de concientización sobre seguridad en teléfonos móviles y protección contra amenazas dirigidas a dispositivos móviles es Ciberamenazas para teléfonos móviles del US CERT.

Más información: http://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf

Para los CISOs cuya responsabilidad es la gestión de la seguridad de aplicaciones móviles, es importante tener en cuenta la adopción de procesos y normas de seguridad específicas para la seguridad de las mismas. Estas medidas podrían incluir la adopción y documentación de estándares de seguridad de tecnología móvil, la adopción de evaluaciones de vulnerabilidades para pruebas específicas de seguridad en aplicaciones móviles y normas para el aprovisionamiento seguro de estas aplicaciones y de los datos de la aplicación en los dispositivos personales. Desde la perspectiva de la adopción del proceso específico de pruebas de seguridad contra vulnerabilidades de aplicaciones móviles, el **Proyecto de Seguridad Móvil de OWASP** tiene un número de recursos tales como documentación sobre riesgos de seguridad móvil, herramientas gratuitas de evaluación de vulnerabilidades, hojas de trucos *(Cheat Sheets)* y directrices para el diseño seguro de aplicaciones móviles.

Más información: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

Un aspecto importante de la seguridad móvil y de preocupación especial para los CISOs es asegurar los dispositivos móviles facilitados por la organización, así como los dispositivos personales que se lleven a la organización. Por ejemplo, el principio "Trae tu Propio Dispositivo (*BYOD - Bring Your Own Device*) es la práctica de llevar dispositivos personales al entorno empresarial y actualmente está muy extendido. Los CISOs necesitarán aceptar los riesgos potenciales y determinar el grado de acceso que le conceden a estos dispositivos potencialmente peligrosos. Hoy en día algunas organizaciones pueden permitir que los dispositivos de los empleados accedan directamente a la red de la organización sólo a través de una conexión segura como una VPN, virtualización segura, servidores terminales o servicios públicos de acceso remoto, como computación en red virtual (VNC). En todos estos casos, es importante que los CISOs hayan desplegado políticas específicas para el acceso remoto de los dispositivos de los empleados que aplican estrictamente a través de tecnologías y servicios de acceso seguro controlados y gestionados de forma centralizada. Un buen recurso que puede ayudar a los CISOs a establecer directrices de BYOD para una gestión centralizada y asegurar dispositivos móviles, como teléfonos inteligentes y tabletas es el NIST SP 800-124, Directrices para la gestión y seguridad de dispositivos móviles en empresas (borrador) y Directrices para la seguridad teléfonos celulares y PDA.

Más información: http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf

Gestión de riesgos de tecnologías de la Web 2.0

Las nuevas tecnologías introducen nuevos riesgos y se deben poner en marcha nuevas medidas en la organización para mitigar estos riesgos. Una posible forma de prepararse al impacto de las nuevas tecnologías es planificar con antelación la adopción de medidas y procesos de seguridad para reducir los riesgos al conocer que tales tecnologías se convertirán en "dominantes" y que serán ampliamente adoptadas por las empresas. De acuerdo con algunos analistas como Gartner, la adopción de nuevas tecnologías por el mercado sigue un ciclo también conocido como "exageración" que se compone de cinco fases que son (1) "el disparador de la tecnología", (2) "el auge de expectativas excesivas", (3) "el valle de la desilusión", (4) "la caída de la cultura", y (5) "la meseta de la productividad". En el ciclo de la exageración que Gartner publicó en 2009 abarca las tecnologías emergentes, la Web 2.0 mostró una adopción

generalizada de dos años o menos. Esta predicción se valida hoy (2012) al considerar que varias aplicaciones de hoy en día han adoptado e integrado las tecnologías 2.0 en sus aplicaciones web. Ya que la alta dirección y el personal directivo típicamente ponen atención específica en el mercado y las investigaciones de analistas sobre tecnologías de seguridad (por ejemplo, Gartner y Forrester) y es importante para el CISO ver estas investigaciones, desde la perspectiva de decidir si adoptar un determinado tipo de tecnología, y de la preparación de los impactos sobre la seguridad de este tipo de tecnologías. En primer lugar, es importante entender la terminología utilizada. Las tecnologías web 2.0 se pueden definir como *"aplicaciones web que facilitan el intercambio interactivo de información y la colaboración, interoperabilidad y diseño centrado en el usuario en la WWW"*. Las características principales de las tecnologías web 2.0 son:

- Fomentar la participación y la colaboración de los usuarios a través de una comunidad virtual de redes sociales/sitios. Los usuarios pueden añadir y actualizar su propio contenido, los ejemplos incluyen Twitter y redes sociales como *Facebook, MySpace, LinkedIn, YouTube*.
- Trascender a partir de las tecnologías/*frameworks* utilizados. Los ejemplos incluyen *AJAX, Adobe AIR, Flash, Flex, Dojo, Google Gears* y otros.
- Combinar y, agregar datos y funcionalidad de diferentes aplicaciones y sistemas, los ejemplos incluyen los *"mashups"* como agregados de funcionalidad del cliente que proporcionan los distintos desarrollos y/o servicios *in-house* de terceros (por ejemplo, servicios web, SaaS).

Un aspecto importante que los CISOs deben ser conscientes respecto de las tecnologías web 2.0 es cómo estas tecnologías afectan al panorama de las amenazas. En primer lugar, las amenazas de la web 1.0 son amplificadas por la naturaleza intrínseca de la Web 2.0, debido al amplio volumen de interacciones entre usuarios: considerar, por ejemplo, los cientos de millones de usuarios de redes sociales y el aumento de la superficie de ataque a las aplicaciones web que ofrecen enlaces a Facebook y cuentas de Twitter que actualmente se prescribe a un agente de amenaza para atacar al usuario con *phishing*, *malware*, y *exploits* contra vulnerabilidades tradicionales de la web 1.0 tales como fallas de inyección, XSS y CSRF. Las redes sociales facilitan específicamente el compartir información confidencial y privada con el cliente ya que los límites entre la información privada y personal a menudo se cruzan al compartir voluntariamente dicha información con la empresa, incluso si no se solicita explícitamente.

Otro de los elementos de mayor riesgo está representado por el aumento de la complejidad de las funciones debido a la integración de diferentes tecnologías y servicios web 2.0 tanto para el cliente (*front-end*), como para el servidor (*back-end*). Ricas interfaces de cliente como los widgets por ejemplo, aumentan la probabilidad de ataques a la lógica de negocio, mientras que la exposición de nuevos *web services* aumenta la exposición de ataques a los servidores.

Las vulnerabilidades de la web 2.0 explotadas por atacantes

Debido al aumento de los riesgos en las aplicaciones web debido a la introducción de tecnologías de la web 2.0, es importante que los CISOs se aseguren que las aplicaciones web están específicamente diseñadas, implementadas y probadas para mitigar los riesgos. Desde una perspectiva de análisis de las amenazas y vulnerabilidades web 2.0 de las aplicaciones, se pueden analizar utilizando el Top 10 de OWASP y el Top 50 de amenazas de WASC.

El Top 10 de vulnerabilidades de OWASP 2013 que las aplicaciones web 2.0 que necesitan ser probadas incluyen A1-Inyección, A2-Autenticación defectuosa, A3-XSS y A8-CSRF. Ejemplos de vulnerabilidades 2.0 incluyen inyecciones XML, como cuando un atacante proporciona información suministrada por el usuario insertado en XML sin una validación suficiente que afecta la estructura del registro XML y las etiquetas (no sólo el contenido). Un tipo particular de inyección XML es la inyección XPATH. Este es un ataque dirigido a modificar una consulta XML para lograr el objetivo del atacante y realizar consultas no autorizadas para poder recuperar datos confidenciales. Otra de las vulnerabilidades de inyección web 2.0 incluyen inyecciones JSON *(JavaScript Object Notation structure)* para ejecutar código no autorizado, potencialmente dañino mediante la inyección de código JavaScript malicioso en el JSON del cliente.

Entre las vulnerabilidades de inyección Web 2.0, las inyecciones RSS se pueden utilizar para consumir fuentes no confiables de canales RSS como enlaces maliciosos para descargar *malware* en el ordenador de la víctima. Los *exploits* XSS de la web 2.0 se ven facilitados por el hecho que una gran cantidad de sitios permiten añadir HTML al contenido de texto normal, por ejemplo, cuando se publica en blogs y la retroalimentación con las empresas de productos/servicios. Cuando los datos HTML no son filtrados de entradas maliciosas que podría permitir que el atacante ingrese etiquetas HTML no confiables que pueden ser utilizadas indebidamente para realizar ataques XSS a las víctimas que leen publicaciones en blogs o comentarios para que presionen sobre enlaces maliciosos. Un vector de ataque adicional al XSS también está representado por XSS DOM desde las APIs de la web 2.0 que usan DOM en Aplicaciones de Internet Enriquecidas *(RIA - Rich Internet Applications)* escritas en Flash, Silverlight, como *mashups* y *widgets*. El uso de AJAX *(Asynchronous JavaScript)* en el cliente también aumenta los posibles puntos de entrada para atacar varias peticiones HTTP al sitio web con ataques XSS. Un ejemplo que aprovecha vulnerabilidades de inyección están incluidos en el *Web Hacking Incident Database WHID 2008-32: "Yahoo HotJobs"* que permitía a los agentes de amenaza explotar una vulnerabilidad XSS para robar cookies de sesión de las víctimas y hacerse con el control de todos los servicios al alcance de la víctima dentro de Yahoo, incluyendo Yahoo! Mail.

Más información: http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database

Ejemplos de *exploits* de la web 2.0 para vulnerabilidades del Top OWASP 2013 10-A2:Autenticación rota y gestión de sesiones, incluyen el uso de contraseñas débiles, contraseñas almacenadas en *widgets/mashup* AJAX que se envían y almacenan en texto claro fuera del control del host, contraseñas almacenadas en el cliente como "función de inicio de sesión automático" o en la nube para SSO *(Single Sing-on)* desde el escritorio y controles de recuperación contraseñas que no están protegidas contra ataques de fuerza bruta ya que no bloquea las cuentas cuando se realizan varios intentos fallidos para adivinar contraseñas. Un ejemplo de este tipo de vulnerabilidad es explotar también parte del catálogo *WHID catalogue as 2008-47: "The Federal Suppliers Guide"* que validaba credenciales de inicio de sesión en JavaScript.

Un tipo de vulnerabilidad que se ve facilitado por la web 2.0 es el CSRF tal como cuando los clientes usan AJAX para realizar llamadas XHR que permiten realizar consultas invisibles de una aplicación web y el usuario no puede validarlas visualmente por la falsificación. CSRF también se ve facilitado por la insuficiencia del navegador para ejecutar la Política del Mismo Origen *(SOP - Same Origin Policy)* para

widgets de escritorio y una gestión de sesiones débil cuando el tiempo de expiración de la sesión se fija bastante alto, lo que aumenta el riesgo de ataques de sesión como CSRF.

Más información: https://www.w3.org/Security/wiki/Same_Origin_Policy

Las *cookies* de sesión persistentes que son compartidas por los *widgets* también aumentan las posibilidades de ataques CSRF. Un conocido incidente de seguridad web 2.0 se encuentra en el catálogo *WHID catalogue as 2009-4: "Twitter Personal info CSRF"* que permitía a un atacante explotar un *bug* CSRF para obtener perfiles de Twitter de los visitantes.

Un tipo de vulnerabilidad que también es explotada y utilizada contra aplicaciones web 2.0, pero también general contra los sitios web es la falta de defensas anti-automatización. Esta vulnerabilidad no está dentro del OWASP Top 10 pero sí en WASC como el Top 21 dentro del TOP 50. Los ataques automatizados contra aplicaciones web 2.0 que están autorizados a publicar información, como formularios de comentarios, *blogs* y *wikis*, por ejemplo, plantan comentarios tipo spam con información comercial publican enlaces a sitios maliciosos para propagar *malware* a través de la técnica de *Drive by Download* o *Phishing*.

Más información: http://projects.webappsec.org/w/page/13246938/Insufficient%20Anti-automation

Ejemplo: insuficiente defensa anti-automatización para Facebook

En 2007, Facebook fue accedido a través de un ataque automatizado en un intento por recolectar información de usuarios. Vea WHID 2007-65: "Botnet para manipular Facebook".

Medidas de seguridad para mitigar riesgos

Para el análisis de vulnerabilidades de aplicaciones web 2.0 es crítica la determinación de las causas de raíz de las mismas. Sólo a través de la identificación de vulnerabilidades de las causas de raíz, se las pueden erradicar. Por ejemplo, si estas vulnerabilidades se originan a partir de la falta de requisitos de seguridad para la web 2.0 que los desarrolladores de software necesitan para seguir, deben ser documentados. En el caso que los problemas sean causados por errores en el diseño, estas necesidades deben evitarse asegurándose que el diseño de las aplicaciones web 2.0 es revisado por un arquitecto de seguridad que cuente con experiencia en tecnologías web 2.0. Para las vulnerabilidades de la web 2.0 introducidas por los desarrolladores de software, como errores de programación o debido a la integración con software y bibliotecas de terceros que están expuestas a vulnerabilidades de la web 2.0, es importante que los mismos estén entrenados en programación defensiva de aplicaciones 2.0 y que los auditores de seguridad sepan cómo identificar y probar las vulnerabilidades de la web 2.0.

Un conjunto prescriptivo de medidas de seguridad web 2.0 que los CISOs pueden llevar a cabo para mitigar riesgos incluyen:

- Documentación de normas de seguridad para tecnologías web 2.0, como requisitos de seguridad para el diseño, desarrollo y pruebas específicas para tecnologías web 2.0 como AJAX, FLASH y la aplicación de estos al comienzo del SDLC.
- Instituir una actividad de seguridad durante el diseño para revisar las amenazas contra las aplicaciones web 2.0 e identificar contramedidas tales como el modelado de amenazas de la misma. Parte de esta actividad también incluye la revisión de seguridad de la arquitectura de la

aplicación y los controles de seguridad que son explotados por ataques contra dichas aplicaciones, como la validación de entrada, autenticación, gestión de sesiones y controles anti-automatización como el CAPTCHA.

- Exigir a las aplicaciones 2.0 a someterse a una revisión de código seguro para garantizar el cumplimiento de los estándares de seguridad de codificación del código fuente y el análisis estático para identificar los problemas, tanto en el código fuente del cliente que utiliza widgets, RIA, componentes AJAX, así como el código del lado del servidor que se utiliza en los servicios web y Arquitecturas Orientadas a Servicios *(SOA - Service Oriented Architectures)*. Los requisitos específicos de seguridad del código se pueden documentar para AJAX, estos pueden ser socializados con los arquitectos y desarrolladores de software, y validados durante el diseño y revisión de código fuente.
- Exigir pruebas de seguridad para incluir casos de prueba específicos para probar vulnerabilidades de los componentes de la web 2.0 y para *web services*. Consulte la guía de casos de prueba de OWASP como por ejemplo las pruebas de AJAX y *web services*.
- Asegúrese que los riesgos técnicos de la web 2.0 son gestionados tal como riesgos de negocio por fallas de diseño de la web 2.0 y errores que podrían perjudicar al negocio. La metodología de riesgos de OWASP puede ser utilizada para gestionar los riesgos de seguridad 2.0. Un ejemplo del *framework* de riesgos de OWASP aplicado a las tecnologías web 2.0 está incluido en la siguiente tabla.

Agentes de amenaza	Vectores de ataques y abuso	Debilidades de seguridad	Controles de seguridad/ Contramedidas	Impactos técnicos	Impactos al negocio
Usuarios Web 2.0	Usuarios comparten información privada/confidencial, agentes publican información confidencial	Debilidades Inherentes al control de la contribuciones de contenido hechas por el usuario en redes sociales, blogs, chat, correos privados	Políticas de seguridad 2.0 en redes sociales, monitoreo de cumplimiento, filtrado, archivado, flujo de trabajo de aprobación para publicar en sitios sociales	Pérdida de datos sensibles/ confidenciales	Daño a la reputación, multas por incumplimiento
Usuarios maliciosos y fraudulentos	La víctima es atacada con *phishing*, descarga de widgets maliciosos, *posts* maliciosos	Ingeniería social, vulnerabilidades 2.0: XSS	Educación a usuarios, filtrado de datos, escape/*encoding* de datos no confiables	Ejecución de JavaScript en el cliente, instalación de *malware*	Fraudes, pérdidas financieras, *defacements*, daño a la reputación
	El atacante envía datos maliciosos a las interfaces de la aplicación	Vulnerabilidades de la web 2.0: inyección XPATH, inyección XML, inyección JSON	Filtrado, APIs parametrizadas, métodos de filtrado con ESAPI, validación a través de listas blancas	Pérdida de datos, alteración de datos, denegación de servicio/acceso	Revelación pública, daño a la reputación
	Los atacantes utilizan fugas o fallas en la autenticación o en las funciones de gestión de sesión	Pérdida de autenticación y vulnerabilidades de gestión sesión	Requerimientos de seguridad para la política de contraseñas seguras, bloqueo de cuenta, deshabilitar el *login* automático	Acceso a datos y funciones no autorizado	Pérdida de CID, implicaciones legales y financieras
Usuarios fraudulentos	Los atacantes crean peticiones HTTP manipuladas y engañan a las víctimas para que las usen	Vulnerabilidades CSRF de la web 2.0	Incluir el *token* único en un campo oculto	Puede cambiar datos y realizar funciones en nombre del usuario	Pérdida de CID, fraude, denegación de acceso

Scripts automatizados / Robots spam	Publicar enlaces de aplicaciones, crear cuentas, aplicaciones de juegos, arrastre de datos	Anti-automatización insuficiente	Monitoreo de comportamiento, detección de ataques AppSensor, incluir CAPTCHA, incluir las API de intrusión ESAPI	Puede desbordar procesos con spam, enumeraciones	Falta de disponibilidad/pérdida del negocio, daño a la reputación

Gestionar los riesgos de los servicios de computación en la nube

El concepto de computación en la nube no es nuevo. Muchas organizaciones utilizaron centros de datos de terceras partes para tener sus centros de datos, un concepto que en computación en la nube es considerado una implementación de una Infraestructura como Servicio *(IaaS - Infrastructure as a Service)*. El término computación en la nube abarca infraestructuras externas tales como el caso de Infraestructuras como Servicios, plataformas tercerizadas como es el caso de Plataformas como Servicios *(PaaS - Platform As a Service)* y a través de software externo, un término conocido como Software como Servicio *(SaaS - Software As a Service)*.

Los CISOs de hoy en día enfrentan el desafío de evaluar y garantizar la seguridad de las implementaciones de computación en la nube dentro de su red (por ejemplo: en las instalaciones o en nubes privadas) o fuera de la organización (ejemplo: instalaciones propias fuera de la organización o en una nube pública). La información y la seguridad de aplicaciones es una preocupación primordial para las organizaciones que tercerizan sus componentes de infraestructura y plataformas o software y datos a proveedores de nube. Los CISOs necesitan considerar los riesgos potenciales y evaluarlos antes de decidir externalizar sus servicios a terceros. Los CISOs deberían considerar por ejemplo, el riesgo potencial que los datos de la compañía estén alojados en un proveedor de computación en la nube que puede ser comprometido debido a la ocurrencia de un incidente de seguridad. También deberían considerar por ejemplo, el riesgo que una organización podría enfrentar cuando el servicio de datos que es proporcionado a sus clientes sea tercerizado a un software de terceros y no esté disponible debido a que el proveedor de dicho servicio en la nube haya sido el objetivo de un ataque de denegación de servicios.

Por lo tanto, es importante que los CISOs consideren todo el espectro de riesgos de seguridad de la información antes que la organización decida migrar sus servicios o sus datos a un proveedor de computación en la nube. A alto nivel, estos riesgos pueden ser evaluados mediante una evaluación de seguridad de la información de terceros sobre el proveedor del servicio. Este tipo de evaluaciones buscan afirmar la postura de seguridad del proveedor contra las políticas y normas de seguridad de la información de la compañía, así como también con la auditoría de normas relevantes de TI y de seguridad de la información tales como SAS70, SOC, FISMA, PCI-DSS, ISO, FIPS-140, ISO/IEC 27001-2005, etc.; y otros como esos que son relevantes para las operaciones de negocio regulados por la organización tales como HIPPA, FFIEC, MPAA, etc.

El caso de la evaluación de computación en la nube, riesgos de seguridad y auditoría de cumplimiento son actualmente algunos de los dominios que necesariamente deben ser evaluados junto a otros tales como la arquitectura de la nube, gobierno, implicaciones legales y leyes, privacidad, continuidad de negocio y recuperación ante desastres, respuesta a incidentes, seguridad en aplicaciones, cifrado y gestión de claves e identidades, gestión de accesos y derechos, virtualización y seguridad como servicio.

Una guía exhaustiva sobre cómo llevar a cabo la supervisión en todos estos dominios de computación en la nube es la Alianza de Seguridad en la Nube *(CSA - Cloud Security Alliance)*. CSA proporciona una guía con el nivel de seguridad más alto para áreas críticas en computación en la nube. También provee un conjunto de herramientas que pueden ser utilizadas por las organizaciones para evaluar riesgos de seguridad de servicios en computación en la nube en estos dominios, incluyendo una matriz de control para evaluar controles de seguridad de la información en SaaS, PaaS y IaaS, leyes, políticas de la organización, gestión de riesgos, resiliencia, arquitectura de seguridad contra normas tales como COBIT 4.1, ISO 27001, NIST SP 800-53, PCI-DSS v2.0, entre otros.

El Cuestionario de la Iniciativa del Consenso de Evaluación de CSA *(CSA Consensus Assessments Initiative Questionnaire v1.1)*, le permite a los CISOs evaluar al proveedor de servicio de computación en la nube con respecto a la seguridad de la información así como también con su cumplimiento, el gobierno de datos, instalaciones de seguridad, recursos humanos de seguridad, legales, gestión de operaciones, gestión de riesgos, gestión de liberaciones/parches, resiliencia y arquitectura de seguridad. La CSA en 2013 también publicó un documento con la guía sobre la adopción de controles en la nube para mitigar el riesgo de las principales amenazas.

Más información: https://cloudsecurityalliance.org/

Top 9 de amenazas en Computación en la Nube	
1.	Filtración de datos
2.	Pérdida de datos
3.	Secuestro de cuentas
4.	APIs inseguras
5.	Denegación de servicio
6.	Personal interno malicioso
7.	Abuso de servicios en la nube
8.	Debida diligencia insuficiente
9.	Problemas con tecnologías compartidas

OWASP recomienda que los CISOs tomen como referencia las guías de documentación de la CSA, cuestionarios y análisis de amenazas a las que refiere el presente documento y los usen para construir un proceso de evaluación de seguridad de computación en la nube *ad-hoc* que pueda ser utilizado por los equipos de seguridad de la información de la organización para realizar una debida diligencia en seguridad, una evaluación de cumplimiento/auditoría y riesgos sobre los proveedores de computación en la nube. Tales evaluaciones de seguridad *ad-hoc* podrían considerarse para crear políticas de seguridad de la información, normas y regulaciones ya que son el punto de partida para confirmar la seguridad de los proveedores de nube ya que son las mismas que son aplicables y relevantes a los requerimientos de la organización para proteger la confidencialidad, integridad y disponibilidad de los datos. Una evaluación de seguridad ad-hoc de computación en la nube debería, como mínimo, incluir un proceso estándar que pueda ser seguido incluyendo un conjunto de herramientas, cuestionarios “sí/no” pueden ser usados para capturar y confirmar la seguridad, de cumplimento y gestión de riesgos de la seguridad del proveedor de computación en la nube antes de tomar una decisión de negocio si tercerizar servicios tales como infraestructuras, redes, plataformas y datos de software a proveedores de servicios de terceros.

El objetivo principal de esta evaluación es identificar brechas de control y áreas potenciales de riesgos para la organización. Ejemplos de riesgos de seguridad en aplicaciones que pueden ser identificadas con estas evaluaciones podrían incluir la identificación de una falta de cifrado de inicio a fin de los datos, otorgando control total y garantía de confidencialidad de los datos en tránsito o almacenados al proveedor, falta de segregación de datos desde otros negocios en un entorno de computación en la nube virtualizado y, la falta de auditoría y registros para eventos e incidentes específicos de seguridad. Ejemplos de controles de seguridad para mitigar estos riesgos podrían incluir el requerimiento de uso de cifrado de inicio a fin para datos confidenciales en tránsito y almacenados en el proveedor de nube, el uso de arquitecturas hipervisor seguras y firewall virtual para asegurar a los clientes de hosting de entornos de nube virtualizados en SaaS, y la adopción de instalaciones de registro y auditoría específicas que puedan ser utilizadas para alertar a ambos, proveedor de nube y la organización que contrata el servicio, en el caso que ocurra un incidente de seguridad, por dar algunos ejemplos.

Una vez que estas brechas de controles han sido identificadas es importante asignar el nivel de riesgo/severidad y determinar si los controles compensatorios podrían ser implementados antes que el despliegue de la solución de computación en la nube. Un aspecto importante para la gestión de estos riesgos, también es garantizar que un Acuerdo del Nivel de Servicio *(SLA - Service Level Agreement)* captura estos riesgos y proporciona un acuerdo contractual obligatorio con el proveedor de servicio en la nube, y cláusulas de responsabilidad e indemnizaciones para la organización en caso de incumplimiento de dichos acuerdos.

Parte III: Programa de Seguridad de Aplicaciones

III-1 Resumen Ejecutivo

Desde el punto de vista estratégico de la gestión de riesgo, la mitigación de riesgos de seguridad de aplicaciones no es un ejercicio de una vez, más bien es una actividad continua que requiere prestar especial atención a las amenazas emergentes y planificar a futuro el despliegue de nuevas medidas de seguridad para mitigar estas nuevas amenazas.

Esto incluye la planificación para la adopción de nuevas actividades de seguridad de aplicaciones, procesos, controles y entrenamiento. Cuando planifican nuevos procesos de seguridad de la aplicación y controles, es importante que los CISOs sepan en qué dominios de seguridad de aplicaciones invertir para que el negocio cumpla con sus misiones.

Para construir y hacer crecer un programa se seguridad de aplicaciones, los CISOs deben:

- Trazar las prioridades de negocio con las prioridades de seguridad
- Evaluar el estado actual usando un modelo de madurez del programa de seguridad
- Establecer el objetivo deseado usando un modelo de madurez del programa de seguridad

Trazar las prioridades de negocio con las prioridades de seguridad

Todas las prioridades de seguridad deben poder trazarse a prioridades de negocio. Este es el primer paso hacia el establecimiento de la relevancia de cada iniciativa de seguridad y muestra a la dirección del negocio como la seguridad soporta la misión. Esto también demuestra al personal de seguridad como personal soporta la misión.

Evaluar el estado actual usando un modelo de madurez del programa de seguridad

La evaluación de la madurez de los procesos es un prerrequisito para la adopción de la seguridad de las aplicaciones y los procesos de seguridad de software. Un criterio que es usualmente adoptado por las organizaciones es considerar las capacidades de la organización en dominios de seguridad y la madurez de la organización en operar esos dominios. Ejemplos de esos dominios de seguridad incluyen gobierno de seguridad de aplicaciones, gestión de riesgos de vulnerabilidades, cumplimiento regulatorio e ingeniería de seguridad de aplicaciones como por ejemplo diseñar e implementar aplicaciones seguras. Específicamente en el caso de ingeniería de seguridad de aplicaciones, adoptar una garantía de seguridad de software es a menudo necesario cuando no hay un control directo de la implementación de la seguridad de ese software debido a que es producido por un proveedor tercero. Un factor a considerar en este caso es medir la garantía de seguridad de software usando un modelo de madurez. Un prerrequisito para medir la garantía de la seguridad de software es la adopción de un Ciclo de Vida de Desarrollo Seguro (S-SDLC). A alto nivel, S-SDLC consiste en incorporar las actividades de seguridad embebidas, entrenamiento y herramientas de seguridad en el SDLC. Ejemplos de esas actividades pueden incluir procesos/herramientas de seguridad de software como análisis de riesgos de arquitectura/modelado de amenazas, revisión de código/análisis estático de código, pruebas de seguridad de aplicaciones/escaneo de vulnerabilidades de aplicación y programación segura para desarrolladores de software. Una referencia al modelo de madurez

de garantía de software de OWASP como así también varios proyectos de OWASP dedicados a seguridad de software y S-SDLC se proporcionan también en esta guía.

Establecer el objetivo deseado usando un modelo de madurez del programa de seguridad

No todas las organizaciones tienen que estar en la más alta madurez. La madurez debería estar al nivel que ésta pueda manejar los riesgos de seguridad que afectan al negocio. Obviamente, esto varía entre las organizaciones y está impulsado por el negocio y como ésta acepta el riesgo como parte de la colaboración continua y la transparencia de la organización de seguridad.

Una vez que el objetivo deseado está definido, CISOs deberían construir una hoja de ruta que identifique la estrategia por para hacer frente a los problemas conocidos, así como la detección y mitigación de riesgos nuevos.

OWASP provee varios proyectos y guías para CISOs para ayudarle a desarrollar e implementar un programa de seguridad de aplicaciones. Además de leer esta sección de la guía, consulte el Apéndice B para obtener más información sobre el tipo actividades de los dominios de ingeniería de seguridad que pueden ser incorporados dentro de un programa de seguridad de la aplicación.

III-2 Introducción

Mitigar el riesgo de los ataques que tratan de explotar vulnerabilidades de las aplicaciones, así como posibles brechas en los controles de protección y de detección es una de las principales preocupaciones de los CISOs. En el caso de que las vulnerabilidades se encuentren sólo después de un incidente de seguridad, el siguiente paso es arreglar las vulnerabilidades identificadas y limitar impacto adicional. Típicamente, esto implica la reproducción de las vulnerabilidades y volver a probar las vulnerabilidades una vez implementados los arreglos para asegurar que las vulnerabilidades ya no pueden ser explotadas. Si el incidente se debe a una deficiencia de un control de seguridad, como una falla para filtrar entradas maliciosas o para detectar el evento de ataque, el siguiente paso es poner en práctica contramedidas para mitigar el riesgo. Las contramedidas pueden ser una combinación de controles de seguridad disuasorios, preventivos, detectivos, correctivos, y compensatorios. Para tomar este tipo de decisiones, el CISO debe tener en cuenta tanto los riesgos de vulnerabilidades, así como las debilidades de las medidas de control de seguridad para tomar una decisión sobre la forma de mitigar los riesgos. Típicamente arreglar una vulnerabilidad implica un ciclo de gestión de vulnerabilidad que incluye la identificación de la vulnerabilidad, corrección y vuelta a probarlo para determinar que ya no está presente.

Para contramedidas, la evidencia de que éstas son efectivas en prevenir y detectar un vector de ataque puede también ser demostrada con una prueba de seguridad funcional después de que las medidas son desplegadas. La decisión en cuanto a qué contramedida desplegar podría depender de diferentes factores como el costo de la medida vs el impacto del negocio del incidente como también en cómo es de efectiva la contramedida en la mitigación del riesgo en comparación con otras. El próximo paso para el CISO después de que el incidente de seguridad está bajo control es asegurar que todas las vulnerabilidades son arregladas y las contramedidas son desplegadas para mitigar el riesgo.

En esta sección de la guía nosotros nos enfocamos en las medidas de seguridad de aplicaciones que son más rentables para alcanzar a los problemas identificados en la **Parte II**. Por ejemplo como dividir presupuestos entre actividades de seguridad en software como entrenamiento en programación segura, revisión de código seguro, verificación y pruebas de seguridad, problemas y gestión de riesgos.

En la Encuesta a CISOs de 2013, los CISOs identificaron sus más altas prioridades y también los riesgos que enfrentan sus programas. Aquí usted encontrará una guía para herramientas y procesos no sólo para cumplir esas prioridades, sino también para gestionar los riesgos que posiblemente impacten en sus prioridades.

Encuesta a CISOs 2013: Top 5 de Prioridades para CISOs

1. Concientización y entrenamiento a desarrolladores
2. Procesos del ciclo de vida de desarrollo seguro (ej., programación segura, proceso de aseguramiento de la calidad)
3. Pruebas de seguridad de las aplicaciones (análisis dinámico, observación de tiempo de ejecución)
4. Tecnologías y procesos de gestión de vulnerabilidades de la capa de aplicación
5. Revisión de código (análisis estático de código fuente para encontrar defectos de seguridad)

Estas prioridades pueden ser inhibidas el TOP de riesgos de los programas identificados por CISOs en la misma Encuesta CISO 2013.

Encuesta a CISOs 2013: Top 5 de Riesgos para CISOs

1. Falta de conciencia de los problemas de seguridad de aplicaciones dentro de la organización
2. Desarrollo de código fuente inseguro
3. Metodologías de prueba pobres/inadecuadas
4. Falta de presupuesto para soportar las iniciativas de seguridad de aplicaciones
5. Personal (por ejemplo, la falta de habilidades de seguridad en el equipo)

III-3 Abordando las Funciones de seguridad de aplicaciones del CISO

Gobierno, riesgos y cumplimiento de la seguridad de aplicaciones

Gobierno es el proceso que introduce políticas, normas, procesos y establece la estrategia, objetivos y estructura organizativa para apoyarlos. A nivel operativo, el gobierno, el cumplimiento y la gestión de riesgos están relacionados entre sí. Como parte de las responsabilidades de gobierno, CISOs influyen en los objetivos de seguridad de aplicaciones y trabajan con la dirección ejecutiva para establecer las normas de seguridad de aplicaciones, procesos y estructura organizacional para apoyar estos objetivos. Como parte de las responsabilidades de cumplimiento, CISOs trabajan con los auditores y los asesores legales para obtener las políticas de seguridad de la información y establecer los requisitos para el cumplimiento, medir y monitorear estos requisitos, incluyendo los requisitos de seguridad de la aplicación. Como parte de las responsabilidades de gestión de riesgos, los CISOs identifican, cuantifican y hacen evaluaciones de riesgo para determinar la forma de mitigar los riesgos de seguridad de aplicaciones que incluyen la introducción de nuevas normas de seguridad de aplicaciones y procesos (de gobierno), nuevos requisitos de seguridad de las aplicaciones (de cumplimiento) y nuevas medidas de seguridad de aplicaciones (riesgos y controles). Desde la perspectiva de la gobierno, la adopción de procesos de seguridad de aplicaciones y software, la creación de equipos de seguridad de aplicaciones y normas de seguridad de aplicaciones dentro de una organización determinada varía mucho en función del tipo de industria de la organización, el tamaño de la organización y los diferentes roles y responsabilidades que el CISO tiene en esa organización. OWASP proporciona varios proyectos y guías para los CISOs para ayudar a desarrollar, implementar y administrar el gobierno de seguridad de aplicaciones. Consulte el Apéndice B para más información sobre los proyectos de OWASP y guías en el ámbito del gobierno.

Típicamente, la fuente de las inversiones de seguridad de aplicación también varía dependiendo del tamaño y el tipo de la organización. Para los CISOs que informan al jefe de seguridad de la información operativa y de gestión de riesgos de la organización, por lo general el presupuesto para seguridad de las aplicaciones es parte del presupuesto total asignado por la seguridad de la información y los departamentos de riesgo operacional. Para estos CISOs, una de las principales razones para la adopción de las nuevas actividades de seguridad de aplicaciones, guías y herramientas como las que OWASP provee, es, ante todo para satisfacer el cumplimiento y reducir los riesgos de los activos de la organización, tales como aplicaciones y software. El cumplimiento varía mucho en función del tipo de industria y los clientes atendidos por la organización. Por ejemplo, las organizaciones que producen software que implementan cifrado para su uso por los gobiernos, como el departamento y las agencias del gobierno federal de los Estados Unidos tiene que cumplir con las Normas de Procesamiento de Información Federal (FIPS) 140. Las organizaciones que producen software y aplicaciones que manejan datos como los de titulares de tarjetas de crédito y datos de la tarjeta de débito para los pagos tienen que cumplir con la Norma de Seguridad de la Industria de Tarjetas de Pago (PCI DSS). CISOs que reportan al jefe de tecnología de información de la organización, por lo general tienen la responsabilidad tanto en funciones de seguridad y tecnología de la información que también pueden incluir el cumplimiento de las normas de seguridad de tecnología de las aplicaciones y software como FIPS 140 y PCI-DSS. El cumplimiento de las normas de seguridad de tecnología representa una oportunidad para promover el desarrollo seguro y pruebas dentro de la organización, como el uso de las guías de pruebas de seguridad de OWASP para lograr certificaciones de seguridad para

aplicaciones y productos de software. El cumplimiento de los requisitos de PCI-DSS, por ejemplo, ya puede requerir a la organización probar las aplicaciones para un conjunto mínimo de vulnerabilidades comunes, tales como el OWASP Top 10. El presupuesto asignado por el departamento de TI para lograr las certificaciones con las normas de seguridad de tecnología como FIPS-140 y PCI-DSS también se puede utilizar para la promoción de las guías de programación segura, como la guía de programación segura OWASP e invertir en herramientas de análisis de código estático. Por ejemplo, en el caso de cumplimiento con PCI-DSS, CISOs podrían optar por el análisis de código estático para satisfacer el requisito 6.6 de PCI-DSS. OWASP proporciona varios proyectos y guías para CISOs para ayudar a desarrollar y poner en práctica las políticas, normas y guías para seguridad de las aplicaciones, así como para ayudar a definir los requisitos de seguridad de las aplicaciones que pueden ser verificados y auditados. Consulte el Apéndice B sobre los proyectos de OWASP en las normas y las políticas y los dominios de Auditoría y Cumplimiento.

CISOs de las organizaciones pequeñas también pueden utilizar métricas de gestión de vulnerabilidades para hacer el caso de negocio en aquellas fases del SDLC en las que invertir en seguridad y mejorar, tanto la calidad del software, así como la seguridad. Por ejemplo, ya que la mayoría de los errores de la calidad y seguridad se deben a errores de programación, es importante para CISOs enfatizar al departamento de TI de la necesidad de procesos de programación segura, estándares y entrenamiento para los desarrolladores ya que enfocándose en las actividades de seguridad de software también conduce al ahorro de costos para la organización. Un estudio del NIST sobre el costo de arreglar los problemas de seguridad, por ejemplo, ha demostrado que el costo de arreglar de un problema de programación en producción es seis veces más caro que su arreglo durante el desarrollo. La Parte IV de la Guía CISO proporciona orientación sobre la configuración de las métricas para la gestión de riesgos de seguridad de la aplicación y para decidir sobre las inversiones en seguridad de aplicaciones.

Entre las responsabilidades del CISO, la Continuidad del Negocio (CdN) es de vital importancia especialmente para aplicaciones web que ofrecen funciones críticas del negocio a los clientes. CISOs son responsables de desplegar planes CdN para garantizar que la empresa podría seguir funcionando a pesar de las circunstancias o los eventos adversos. Un plan de CdN incluye procedimientos para restaurar los servicios que se han perdido a causa de un evento negativo, como un corte de energía del centro de datos donde se aloja una aplicación web. Un elemento fundamental de la planificación del CdN es la identificación de las aplicaciones web que se consideran críticas para el negocio y asignar un nivel de criticidad y los requisitos específicos para las pruebas del CdN como el tiempo máximo para recuperarse de una pérdida de servicio. Igual que en CdN, tener un plan de recuperación de desastres es también una de las responsabilidades CISO: esto incluye los procesos, las políticas y los procedimientos para la recuperación o el continuidad de la infraestructura de la tecnología en el caso de desastres naturales o provocados por el hombre.

Una de las principales responsabilidades CISOs es aumentar la conciencia de seguridad de aplicaciones, entre las partes interesadas en seguridad de aplicaciones. Una encuesta de 2012 por el *Ponemon Institute* y *Security Innovation* que incluyó a más de 800 ejecutivos de TI encontró que *"las diferencias en las percepciones entre los profesionales de la seguridad y los desarrolladores acerca de la madurez de seguridad de aplicaciones, la disponibilidad y la rendición de cuentas indican por qué las aplicaciones críticas de muchas organizaciones están en riesgo"*. Casi el 80% de los desarrolladores y el 64%

de los directores de seguridad que participaron en esa encuesta, respondió que su organización no tiene un proceso para la construcción de controles de seguridad en sus aplicaciones, y más del 50% de los desarrolladores y los oficiales de seguridad informaron que no recibieron capacitación en seguridad de software y aplicaciones, sólo el 15% de los desarrolladores y el 12% de los oficiales de seguridad informaron de que las aplicaciones cumplen las normas de seguridad y el 68% de los desarrolladores versus el 47% de los oficiales de seguridad informaron ser conscientes de los errores de seguridad que afectan a las aplicaciones que ocurrieron en los últimos 2 años.

Está claro que existe una oportunidad para obtener ganancias de eficiencia mediante la construcción de seguridad en el SDLC a través de la formación en seguridad. OWASP cuenta con diversos recursos de capacitación y concientización que se pueden utilizar para el entrenamiento de equipos de desarrollo seguro, operacionales y de seguridad de la información.

Para CISOs cuyo principal objetivo es la seguridad de la información y la gestión de riesgos, uno de los principales requisitos, además del cumplimiento es introducir eficiencia y ahorrar dinero gastado en los procesos de seguridad existentes, incluyendo la seguridad de aplicaciones. Dado que el departamento de seguridad de la información asigna el presupuesto, cualquier solicitud de presupuesto de seguridad de la aplicación deberá justificarse mediante la mejora de la seguridad y la reducción de los riesgos. Objetivos de seguridad y reducción de riesgos están alineados mejorando los procesos de prueba de seguridad con el uso de mejores herramientas y capacitación para los desarrolladores. Para CISOs de las grandes organizaciones, promover una iniciativa de seguridad de software se justifica también por los beneficios de evitar costos de arreglo de las vulnerabilidades como resultado de las normas de programación segura, revisiones de código de seguridad y pruebas de seguridad en las primeras fases del SDLC, cuando correcciones de errores son menos costosas. Vea el Apéndice B para obtener información sobre las guías y proyectos que ayudan a CISOs en la implementación de un programa de seguridad de aplicaciones, incluidos los procesos de pruebas de seguridad de desarrollo de software de seguridad y de OWASP.

A menudo, CISOs deben justificar el presupuesto para seguridad de las aplicaciones teniendo en cuenta las diferentes necesidades de los departamentos de seguridad y de negocios. Para CISOs que sirven en los organismos financieros, por ejemplo, la seguridad es a menudo un compromiso con los objetivos de seguridad y empresariales. En este caso, es importante para los CISOs poder alinear los programas de seguridad de las aplicaciones con los objetivos de negocio y cuando estos objetivos no se alinean, se concentre en los que lo hacen. Por ejemplo, al enfocarse en mejorar de la calidad y la seguridad del software y por alcanzar un acuerdo en caso de que la seguridad impacte negativamente en la experiencia del cliente, por lo que diferentes opciones de seguridad deben tenerse en cuenta. En el caso de que la empresa está patrocinando un nuevo proyecto de desarrollo de aplicaciones, CISOs pueden utilizar esto como una oportunidad para promover las nuevas características de seguridad de aplicaciones para la aplicación y trabajar conjuntamente con los gerentes de proyecto para alanzar el cumplimiento de normas de seguridad, la mejora de la seguridad por diseño y programación y sin embargo lograr un ahorro global de costos para el proyecto en general.

La importancia de métricas de seguridad

Para CISOs cuya responsabilidad es gestionar los riesgos de vulnerabilidades de aplicaciones, las métricas de seguridad tales como métricas de vulnerabilidades de aplicaciones constituyen un factor importante para hacer casos de negocio para invertir en medidas de seguridad de aplicaciones para controlar y reducir los riesgos. Métricas de seguridad, como las mediciones de las vulnerabilidades encontradas en las mismas aplicaciones durante el despliegue de las actividades de seguridad de aplicaciones orientadas a reducir el número y el riesgo de vulnerabilidades, por ejemplo, pueden demostrar a los altos directivos y ejecutivos de la empresa que la adopción de procesos de seguridad de aplicaciones, capacitación y herramientas, ayudan en última instancia a la organización para ofrecer aplicaciones y productos de software que tienen un menor número de vulnerabilidades y suponen un menor riesgo para la organización y los clientes.

III-4 Enfocando las actividades de Seguridad en Software y procesos del S-SDLC

OWASP proporciona varios proyectos y guías para CISOs para ayudarlos en el desarrollo y ejecución de las actividades de seguridad de software y seguridad en el Ciclo de Vida del Software (S-SDLC). Para saber más, además de la lectura de esta sección de la guía, por favor consulte el Apéndice B para más información

Reconociendo la importancia y criticidad de la seguridad en software

Puesto que la programación insegura provoca un gran número de vulnerabilidades en aplicaciones, es importante que el CISO reconozca la importancia que tiene el software seguro en la mejora de la seguridad de la aplicación. Las causas de software inseguro pueden depender de diferentes factores, tales como errores de programación, no seguir las normas de programación segura y requisitos de seguridad, la integración con las bibliotecas de software vulnerables, falta procesos de revisión de seguridad de código y las pruebas de seguridad y capacitación formal y concientización en programación segura para los desarrolladores de software. Desde la perspectiva del CISO, es importante entender que la seguridad del software es una disciplina compleja y requiere un enfoque especial en los procesos de seguridad, herramientas, así como habilidades de la gente. También es importante reconocer que la inversión en seguridad de software ayuda a la organización para ahorrar el dinero gastado en los costos de reparación de vulnerabilidades de aplicaciones en el futuro. Al invertir en iniciativas de seguridad de software, las empresas pueden centrarse en el arreglo de las vulnerabilidades tan pronto como durante la fase de programación del ciclo de vida de desarrollo de software (SDLC), donde es más barato para identificar, probar y solucionar ellos que durante la fase de validación.

Hoy en día, también gracias a OWASP, la seguridad del software ha madurado y evolucionado como disciplina. Por ejemplo, varias organizaciones ya adoptaron las mejores prácticas de seguridad de software dentro de sus procesos de desarrollo de software, tales como la documentación de los requisitos de seguridad, siguiendo las normas de programación segura y el uso de herramientas de pruebas de seguridad de software, tales como las herramientas de análisis estático de código fuente para identificar vulnerabilidades en el mismo antes de liberarlo para que se va construido e integrado para pruebas de integración y de aceptación de usuario final. Mediante la integración de las actividades de seguridad de software en el SDLC, las organizaciones pueden producir software y aplicaciones con un menor número de vulnerabilidades y riesgos más bajos que los programas y aplicaciones que no lo hacen.

Integrando la gestión de riesgos como parte del SDLC

CISOs determinan cómo las actividades de seguridad de software se pueden integrar como parte del SDLC. Según la Publicación Especial del Instituto Nacional de Estándares de Tecnología (NIST-SP) 800-30, “La gestión eficaz de riesgos debe estar totalmente integrada en el SDLC, la que tiene cinco fases: inicio, desarrollo o adquisición, implementación, operación o mantenimiento y eliminación”. La integración de la seguridad en el proceso de SDLC comienza por identificar los activos de información que el software estará procesando y especificando los requisitos de confidencialidad, integridad y disponibilidad. Los próximos pasos consisten en la determinación del valor los activos de información, la identificación de las posibles

amenazas y la identificación de las medidas de seguridad de aplicaciones necesarias, tales como la autenticación, autorización y cifrado.

Un amplio conjunto de requisitos de seguridad necesitan también incluir los requerimientos para implementar el software seguro siguiendo ciertos estándares de seguridad y tecnología, tecnologías y plataformas de seguridad aprobados, así como los controles de seguridad antes de la integración de software con otros componentes/librerías de software de otros proveedores.

Evaluar riesgos antes de la adquisición de componentes/servicios de terceros

Cuando el software es adquirido, ya sea como software comercial directamente del estante de un comercio *(COTS - Commercial Off The Shelf)* o como código abierto/software libre *(FOSS - Free and Open-Source Software)* por ejemplo, es importante que los CISO tengan un proceso para validar este tipo de bibliotecas de software contra los requisitos de seguridad específicos antes de adquirirlos. Esto podría proporcionar al CISO de la organización de un cierto nivel de garantía de que el software adquirido es seguro y puede ser integrado con la aplicación. En ese sentido, OWASP ha desarrollado un proyecto legal y un anexo de contrato de un modelo de contrato que incluye requisitos de seguridad para el ciclo de vida para que los productos COTS sean más seguros. Por favor, consulte el Apéndice B para más información sobre los proyectos de OWASP que pueden ayudar a los CISO para evaluar la adquisición de nuevos procesos de aplicaciones, servicios, tecnologías y herramientas de seguridad.

Seguridad en las Metodologías del SDLC (S-SDLC)

En casos en que el CISO de la organización tiene también la responsabilidad sobre promover un proceso de seguridad de software dentro de la organización, es importante no tomarlo a la ligera ya que este objetivo por lo general requiere una cuidadosa planificación de los recursos y el desarrollo de nuevos procesos y actividades. Afortunadamente hoy en día, varias metodologías de "Seguridad en SDLC" (S-SDLC) pueden ser adoptadas por los CISO para incorporar la seguridad en el SDLC. Las metodologías de S-SDLC más populares utilizadas en la actualidad son *Touch Points de Cigital*, Microsoft SDL, OWASP CLASP y la *BITS Software Assurance Framework*. A alto nivel, estas metodologías S-SDLC son muy similares y consisten en la integración de las actividades de seguridad, tales como los requisitos de seguridad, revisión de arquitectura segura, la arquitectura de modelado de análisis de riesgos, amenazas, análisis estático, revisión de código fuente, las actividades de pruebas de seguridad, penetración dentro de las actividades existentes SDLCs utilizadas por la organización.

El reto para la integración de la seguridad en el SDLC desde la perspectiva CISO es asegurarse de que estas actividades de seguridad de software están alineadas con los procesos de ingeniería de software utilizados por la organización. Esto significa, por ejemplo, la integración de los diferentes tipos de S-SDLC s como Agile, RUP y Cascada, que podrían ya estar siendo seguidos por los diferentes equipos de desarrollo de software dentro de la organización.

Un ejemplo de cómo estos pueden ser integrados dentro de un SDLC en cascada, así como iterados en diferentes iteraciones de un proceso de SDLC se muestra a continuación.

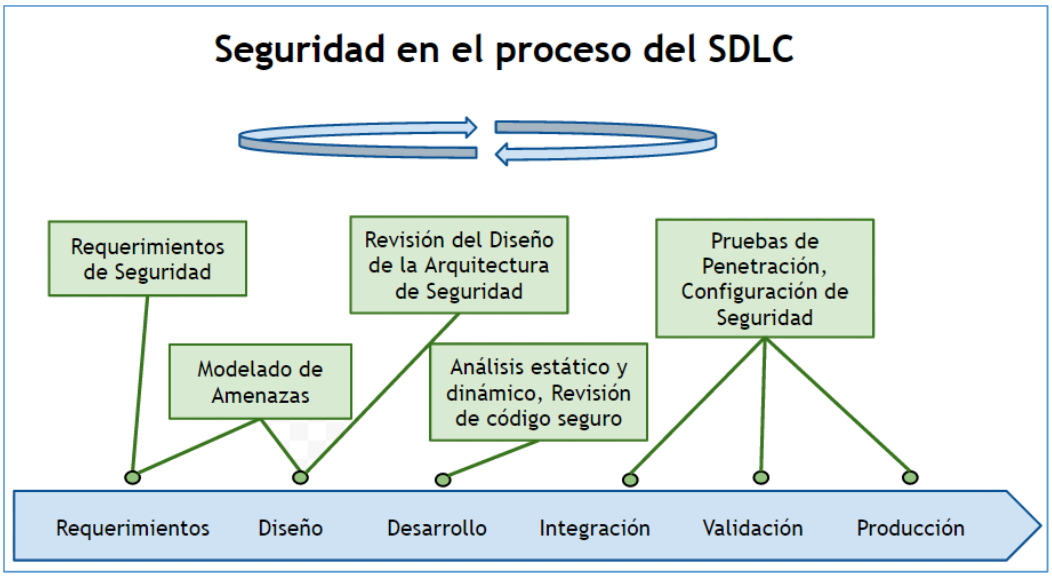

Figura 7 – Ejemplo del proceso de seguridad construido sobre el SDLC en cascada

La adopción de un enfoque holístico hacia la seguridad de aplicación y software conduce a mejores resultados ya que puede alinearse con la seguridad de la información y la gestión de riesgos ya adoptadas por la organización. De la perspectiva de seguridad de la información, el enfoque holístico hacia la seguridad de la aplicación debe incluir, por ejemplo, capacitación en seguridad para los desarrolladores de software, así como para los oficiales de seguridad y gerentes, la integración con la seguridad de la información y la gestión de riesgos, el alineamiento con las políticas de seguridad de la información y estándares de tecnología y el aprovechamiento de las herramientas de seguridad de la información y tecnologías utilizadas por la organización.

Modelos de madurez de garantía del software

Además de seguir un enfoque holístico hacia la seguridad de las aplicaciones que tenga en cuenta otros dominios es también importante para el CISO considerar cuáles son las capacidades de organización desde el primer momento, en la construcción de seguridad de software y planear sobre cómo integrar nuevas actividades en el futuro. Medir las capacidades en las organizaciones de seguridad de software es posible hoy en día con los modelos de madurez de seguridad de software, tales como *Build Security In Maturity Model (BSIMM)* y *Open Software Assurance Maturity Model (SAMM)*. Estos modelos también pueden ayudar al CISO en la evaluación, la planificación y la implementación de una iniciativa de seguridad de software para la organización. Estos modelos de madurez están diseñados explícitamente para la garantía de seguridad de software. Aunque se basan en mediciones empíricas, se alimentan a partir de datos reales (encuestas de seguridad de software, por ejemplo), por tanto, permiten medir las organizaciones contra pares que ya habían implementado iniciativas de seguridad de software. Al permitir que las prácticas seguras de desarrollo de software de su organización sean medidas usando estos modelos, los CISOs pueden comparar sus capacidades de desarrollo de software seguro de la organización

contra otras organizaciones de desarrollo de software para determinar en que las actividades de seguridad de software de la organización están adelantada o atrasada.

Para las actividades de seguridad de software para las que la organización se está retrasando, las mediciones BSIMM y SAMM permiten al CISO construir un plan de actividades de seguridad de software para cerrar estas diferencias en el futuro. Es importante notar que estos modelos no son prescriptivos, es decir, no le están diciendo las organizaciones de qué hacer, sino más bien medir las actividades de seguridad en comparación con organizaciones similares en el ámbito. Se organizaron los modelos a lo largo de los dominios similares, gobierno, la inteligencia, los puntos de contacto SSDL, despliegue y gobierno para BSIMM; y construcción, verificación, despliegue para SAMM. Las mediciones de SAMM se hacen en tres mejores prácticas y tres niveles de madurez para cada función de negocio.

Figura 8 - Funciones de negocio y las prácticas de seguridad para cada función de negocio
Fuente: www.opensamm.org

Las mediciones BSIMM cubren 12 mejores prácticas y 110 actividades seguridad del software. Los niveles de madurez ayudan al CISO a planificar las mejoras organizativas en los procesos de seguridad de software. Las mejoras de seguridad de software se pueden medir mediante la asignación de metas y objetivos a alcanzar para cada actividad. Para CISOs que, o bien ya han comenzado a implementar una iniciativa de seguridad de software, tales como S-SDLC dentro de su organización o que acaban de planear en el futuro, las medidas que un modelo como BSIMM y SAMM proporcionan son criterios de medición importantes para determinar en qué actividades de seguridad de aplicaciones enfocar el gasto. Si todavía no están familiarizados con BSIMM y SAMM, CISOs también puede referirse a *Capability Maturity Model (CMM)* y los diversos niveles de madurez para planear las capacidades de la organización del proceso de desarrollo seguro de software.

Como BSIMM y SAMM, CMM es también un modelo empírico cuyo objetivo es mejorar la previsibilidad, la eficacia y el control de los procesos de software de una organización. En CMM, por ejemplo, se trata de cinco niveles que pueden ser utilizados para medir cómo la organización se mueve hacia arriba a los diferentes niveles de madurez del proceso de ingeniería de software: inicial, repetible, definido, administrado, optimizado. En el primer nivel (inicial), el proceso de ingeniería de software es ad-hoc y utilizado por la organización en forma descontrolada y reactiva. A medida que la organización de desarrollo de software alcanza el nivel 2, los procesos de desarrollo de software son repetibles y es posible proporcionar resultados consistentes. Cuando una organización alcanza el nivel 3, significa que ha adoptado un conjunto de procesos de desarrollo de software estándar definido y documentado y éstos

son seguidos consistentemente a través de la organización. A nivel 4, que es administrado, una organización de desarrollo de software ha adoptado las métricas y mediciones para que el desarrollo de software pueda ser administrado y controlado. Cuando una organización de desarrollo de software está en el nivel 5, optimizado, la atención se centra en la mejora continua del desempeño de los procesos a través tanto de cambio tecnológico incremental e innovador y en mejoras en el desarrollo de software.

En referencia a los procesos de seguridad de software, en el Nivel CMM 1 (Inicial) CISOs tienen un proceso *ad-hoc* para "atrapar" y "remendar" vulnerabilidades de las aplicaciones. En este nivel, la madurez organización en la práctica de seguridad de software consiste en correr herramientas de análisis de vulnerabilidades de aplicaciones web en reacción a los acontecimientos, como para validar las solicitudes de cumplimiento de PCI-DSS y OWASP Top 10. En CMM Nivel 2, la organización ya ha adoptado procesos estándar para las pruebas de seguridad de aplicaciones para las vulnerabilidades, incluidas las revisiones de código seguro de las bibliotecas y componentes de software existentes. En este nivel, el proceso de pruebas de seguridad puede repetirse para producir resultados consistentes (por ejemplo, conseguir mismos problemas de seguridad si se ejecuta por diferentes *testers*), pero no se ha adoptado en todos los grupos de desarrollo de software dentro de la misma organización. En el Nivel CMM 2, los procesos de seguridad de aplicación también son reactivos, es decir, no se ejecutan como exigen los estándares de prueba de seguridad. En el nivel 3 de CMM, los procesos de seguridad de las aplicaciones se ejecutan siguiendo los procesos estándares definidos y estos son seguidos por todos los equipos de seguridad dentro de la misma organización. En este nivel, los procesos de seguridad de aplicaciones también son proactivos, lo que significa que se ejecutan las pruebas de seguridad de aplicaciones como parte de los requisitos de gobierno, riesgo y cumplimiento antes de su liberación en producción. En CMM nivel 4 (administrado) los riesgos de seguridad de aplicaciones son identificados y gestionados en diferentes fases del SDLC. En este nivel, el enfoque de la seguridad es la reducción de los riesgos para todas las aplicaciones antes de que aparezcan en producción. En el nivel 5 de CMM (optimizado), los procesos de seguridad de aplicaciones están optimizados para una mayor cobertura de la aplicación y del mayor retorno de las inversiones en las actividades de seguridad de la aplicación.

Estrategia de seguridad

Estrategia

La estrategia (del griego "στρατηγία" – Strategia: "*arte del general, comando, generalato"*) es un plan de alto nivel para lograr uno o más objetivos en condiciones de incertidumbre. El arte y la ciencia de planificar y de maniobrar recursos para su uso más eficiente y eficaz. La estrategia es importante porque los recursos disponibles para lograr estos objetivos suelen ser limitados. Estrategia también se trata de conseguir y mantener una posición de ventaja frente a los adversarios a través de la explotación sucesiva de posibilidades conocidas o emergentes en lugar de comprometerse a cualquier plan fijo específico diseñado desde el principio ". Al igual que con una estrategia de TI general la mayoría de las organizaciones deben tener una estrategia de seguridad. Permite a una organización a mirar más allá decisiones tácticas a corto plazo y desarrollar planificación estratégica y de largo plazo. Debido a la evolución del panorama de amenazas cibernéticas, es importante para los CISOs proteger los activos de seguridad de la información de las amenazas del mañana. Esta estrategia puede guiar las decisiones operacionales, planes y prioridades

establecidas para el nivel adecuado de inversión de los recursos para lograr los objetivos de su organización.

Tener un plan y estar listo para cambiarlo

Una estrategia de seguridad no va a cubrir todas las eventualidades, sino que le proporcionará un buen marco estratégico. Además, con el tiempo su medio ambiente o los supuestos subyacentes cambiarán y su estrategia tendrá que evolucionar constantemente y adaptarse en consecuencia. Es mejor definir una estrategia y revisarla con frecuencia, adaptándola a las nuevas circunstancias, que frenar el desarrollo de su estrategia de seguridad por tiempo indefinido, a la espera de toda la información esté disponible.

Para definir los fundamentos de la estrategia de seguridad, usted debe considerar las siguientes tres preguntas generales:

- Las partes interesadas: ¿Quiénes son sus principales partes interesadas y agentes de amenaza potenciales?
- Activos: ¿Cuáles son sus activos de información y cómo éstos (y su protección) generan valor para sus clientes dentro y fuera de la organización?
- Capacidades: ¿Cuáles son las capacidades de seguridad y de protección esenciales que la organización y sus partes interesadas deben entregar a esa propuesta de valor?

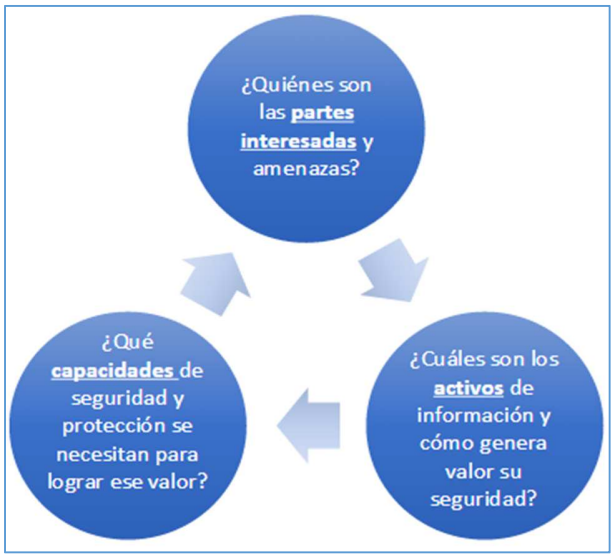

Figura 9 – Tres preguntas claves para construir una estrategia de seguridad

Cómo definir la estrategia de seguridad de su organización

Al igual que con todos los documentos estratégicos, usted analizará el impacto de suposiciones y objetivos subyacentes y derivará su estrategia de seguridad en cómo alcanzar estos objetivos.

Recopilando entradas para el desarrollo de su estrategia de seguridad

En general, las siguientes entradas son útiles en el proceso de definición de su estrategia de seguridad. A menudo, las organizaciones no tienen todas estas, o tal vez las tienen en forma informal menos accesible

(por ejemplo, en la mente de algunos de sus empleados clave de la organización). O pueden ser obsoletas o no coinciden exactamente con lo que se esperaba. Idear una estrategia de seguridad basada en la claridad limitada de la estrategia general de una organización o piezas de información que faltan puede ser un reto. Sin embargo, todavía es mejor desarrollar una estrategia y evolucionar con el tiempo a medida que más y más información relacionada esté disponible.

Figura 10 - Entradas necesarias para desarrollar una estrategia de seguridad

1. Estrategia de negocio

Los CISOs deben mirar primero la estrategia de negocio de la organización, tales como la declaración de la misión, los objetivos de negocio, así como los otros componentes de la estrategia (ver los siguientes puntos) en apoyo de estos objetivos. Por ejemplo, ¿qué partes de su operación son críticamente dependientes de la confidencialidad, disponibilidad e integridad de la información proporcionada por las funciones de TI? ¿Cuál sería el impacto en sus ventas y marketing en el caso de fallos del sistema o pérdida de información de precios, cuán dependiente es la cadena de suministro en el funcionamiento de TI troncal, pueden las entregas hacerse en caso de fallo, podría el fraude ser detectado en caso de problemas de seguridad? ¿Qué partes de la cadena de valor son susceptibles a ataques potenciales? ¿Qué oportunidades pueden ofrecer ciertas posturas de seguridad como una ventaja competitiva para el negocio? Por ejemplo, ¿puede un entorno de seguridad más robusto permitir más comercio electrónico, una mayor dependencia de los procesos de TI y más eficiencia? ¿Pueden los procesos de adquisiciones cambiar drásticamente, por ejemplo, al permitir una estrategia BYOD (trae tu propio dispositivo)? ¿Existen nuevos y potencialmente disruptivos casos de negocio posibles debido a aplicaciones seguras y confiables? ¿Hasta dónde puede permitir que algunos de los datos salgan del control inmediato de su organización (por ejemplo, en el caso de las aplicaciones basadas en la nube)? ¿Cómo se puede reducir al mínimo los riesgos, por los controles legales y técnicos? ¿Son los niveles de riesgo que resultan aceptables para el negocio?

2. Estrategia corporativa

¿Cómo se alinea su estrategia corporativa con su estrategia de TI y de seguridad? ¿Su organización pretende obtener una estructura organizativa descentralizada o centralizada? ¿Cómo afecta esto su

capacidad de hacer cumplir las políticas centrales y locales de seguridad? ¿Son frecuentes las adquisiciones corporativas y su integración una parte importante de su estrategia corporativa y cómo integra usted con eficacia nuevas entidades y gestiona la seguridad de estas entidades corporativas recién adquiridas a través de toda la organización?

3. Estrategia de TI & Revisión de la arquitectura de TI

Un aspecto importante de la estrategia de seguridad es la alineación con la estrategia de TI, por ejemplo, en función de si los sistemas son descentralizados o centralizados, determinará cómo y hasta donde la organización puede reforzar las políticas centrales y locales de seguridad. Otros aspectos son visión global de la arquitectura del sistema, los límites de confianza, los flujos de datos, datos en movimiento y datos en reposo. ¿Cómo impulsa su estrategia de negocios de su estrategia de TI? ¿Qué clase de activos de TI y capacidades tiene su organización y planea desarrollar en el futuro?

4. Requerimientos de cumplimiento y legales

5. Analice sus amenazas y riesgos

Necesita comprender cómo estos riesgos afectan su operación de negocios y posiblemente podrían afectar su negocio y estrategia de negocio. (Véase también la Parte II de esta guía)

6. Revise de su estado de seguridad actual

Otro factor importante a tener en cuenta antes de establecer la estrategia de seguridad es la madurez de la organización y las capacidades de los diferentes dominios de seguridad y, específicamente, del dominio de seguridad de las aplicaciones. Un modelo de madurez, como OWASP OpenSAMM y las diversas actividades en la Estrategia y Métricas también pueden ser utilizados por los CISO para revisar el estado de seguridad actual y fijar objetivos. En concreto, siguiendo el modelo OpenSAMM los CISOs pueden empezar con actividades (básicas) del nivel 1 SAMM como “estimar el perfil global de riesgo del negocio” y “construir y mantener la de hoja de ruta del programa de aseguramiento/garantía”. A medida que la madurez de la organización crece, CISOs pueden incorporar actividades de nivel 2 de OpenSAMM como “clasificar los datos y las aplicaciones basadas en el riesgo del negocio”, y “establecer y medir objetivos de seguridad por la clasificación”. Comprender la situación actual de la seguridad de la organización va a permitir desarrollar una hoja de ruta clara como uno de los componentes clave de una buena estrategia de seguridad en el futuro.

Más información: http://www.opensamm.org/download/

Componentes de su estrategia de seguridad

Una estrategia de seguridad debe contener o habilitar los siguientes componentes:

1. Principios rectores generales y prioridades

¿Qué inversiones de seguridad hará la organización en los próximos x meses? En general la mayoría de las compañías utilizan un periodo de tiempo de 12 - 24 meses para sus definiciones de estrategia. Sería conveniente contar con una estrategia principal de seguridad definida por 12 meses, con un segundo componente de planificación a largo plazo para entre 2 y 5 años, dependiendo del tipo de organización,

que esboza los planes de inversión para la seguridad a largo plazo. Por supuesto, en rápida evolución ámbito de la seguridad de hoy en día, las amenazas y los riesgos pueden cambiar muy rápidamente y el plan debe adaptarse siempre que exista una presunción de cambio y ser revisado por lo menos una vez al año.

2. Gestión de Riesgos, niveles de aceptación de riesgos

(ver Parte II)

3. Hoja de ruta de seguridad

Para definir su hoja de ruta de seguridad, una buena manera es mirar a las hojas de ruta general de la compañía y de TI y combinar esto con una hoja de ruta de seguridad derivada de las evaluaciones de riesgo utilizando modelos de madurez, como por ejemplo OpenSAMM.

4. Arquitectura de seguridad y Procesos

¿Qué propiedades de seguridad presenta la arquitectura de sistemas global? ¿Cuáles son y dónde están los límites y presuposiciones subyacentes de confianza para su organización? ¿Cuáles son los sistemas básicos de seguridad, como autenticación y la autorización? ¿Qué tan profunda es la dependencia de los sistemas centrales y heredados individuales, por ejemplo, si implementa *Single-sign-On* o equivalentes, qué tan confiable es el sistema central de gestión de todos los controles de autorización?

Además, la arquitectura de seguridad debe tener en cuenta la superficie de ataque y la exposición a las amenazas informáticas, en concreto qué partes de la arquitectura de la aplicación y la funcionalidad son susceptibles a potenciales ataques cibernéticos. Y sobre la base de esa resiliencia por lo tanto, la cuestión es que arquitectura de seguridad es la más resistente en caso de ataques, como por ejemplo, DDoS, etc.

La adquisición de la tecnología y los servicios de la seguridad es un componente crítico de la estrategia de seguridad también. Preguntas que deben hacerse aquí es si el proceso de adquisición aborda los riesgos de seguridad introducidos por la adopción de la tecnología de terceros y lo que la organización puede hacer para mejorar la seguridad de los procesos y aplicaciones de terceros.

Y en los sistemas basados en la nube de hoy en día, los datos a menudo pueden dejar el perímetro de seguridad y el flujo a través de otras redes (por ejemplo, en la nube) y sistemas. Y la organización puede tener ninguno o sólo muy limitado el control sobre la forma como los datos están protegidos en dichas aplicaciones en la nube.

5. Continuidad de Negocio y Respuesta a Incidentes

Es importante que los CISOs también desarrollen un Plan de Continuidad de Negocios (PCN) como parte de la estrategia de seguridad que tenga en cuenta los posibles fallos del sistema y las dependencias de la cadena de suministro del funcionamiento la infraestructura de TI.

Una estrategia de seguridad debe tener en cuenta los peores escenarios y planificar las medidas de seguridad con antelación. Una estrategia de riesgos proactiva consiste en responder a preguntas sobre la

gestión de impacto en el negocio antes de que se produzca realmente un incidente. Para una empresa de prestación de servicios, por ejemplo, la pregunta podría ser si la aplicación puede seguir funcionando para garantizar la entrega y fallar de forma segura.

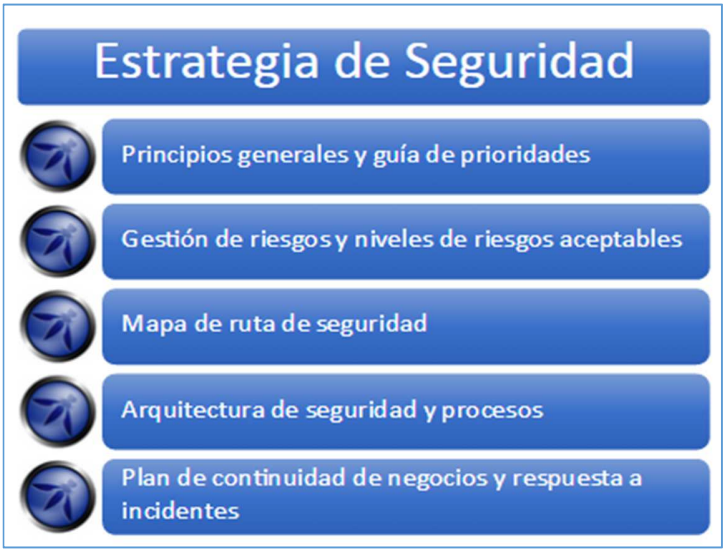

Figura 11 - Elementos de una estrategia de seguridad

Conclusión

El objetivo general de la estrategia de seguridad es minimizar los riesgos y maximizar los beneficios para el negocio de la organización. La pregunta clave que la estrategia debe responder es si los controles de seguridad son bastante suficientes y eficientes para reducir el riesgo para la organización y que los riesgos residuales son aceptables luego de que las medidas de seguridad son aplicadas.

Generalmente, la mayoría de las hojas de ruta tienen una duración de 1-2 años. La encuesta de OWASP de 2013 para CISO encontró que el 64% de las hojas de ruta son proyectadas para 1-2 años.

Duración	%
1 año	35.59%
2 años	28.81%
3 meses	10.17%
3 años	10.17%
5 años+	6.78%
6 meses	8.47%
Total	100.00%

Figura 12 – Análisis de hoja de ruta y su duración

III-5 Cómo elegir los proyectos de OWASP adecuados para su organización

Dependiendo del nivel de seguridad global y el perfil de riesgo de las unidades organizativas, diferentes herramientas y estándares pueden ser particularmente útiles para el CISO en el avance de su estrategia de seguridad.

Tenga en cuenta, después de las discusiones de riesgo en el capítulo anterior, en función del perfil de riesgo de las diferentes unidades de negocio, la estrategia de seguridad en realidad puede ser diferente en función de sus diferentes escenarios de riesgo individuales y diferentes requerimientos regulatorios. Por ejemplo, un departamento financiero puede requerir a una postura de seguridad mucho más fuerte, mientras que una página web interna que anuncia el menú de almuerzo de la cantina puede ser suficientemente protegida con medidas de seguridad básicas (aunque con el conocimiento de los autores en los entornos militares, incluso el menú del almuerzo se puede considerar información tan confidencial como obtener más información sobre la logística de suministro, etc. podría derivarse de eso).

Basado en estos diferentes perfiles de riesgo, diferentes herramientas y normas pueden ser más relevantes para el proyecto y la unidad organizativa en cuestión.

También tenga en cuenta que OWASP proporciona varios proyectos y una guía para CISOs para ayudarle en el desarrollo e implementación de los procesos de desarrollo de software de seguridad y pruebas de seguridad. Por favor, consulte el **Apéndice B** para una referencia rápida de las guías y los proyectos de OWASP.

En general herramientas se pueden clasificar en varias categorías (y así también los proyectos de OWASP).

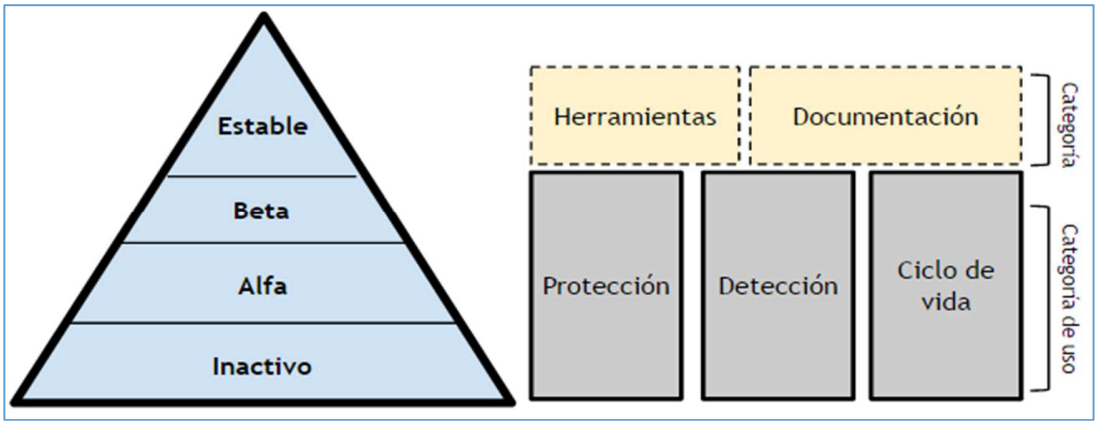

Figura 13 – Ilustración de proyectos OWASP

Madurez del proyecto

- Estable: un proyecto o herramienta que es madura y constantemente mantiene una buena calidad.
- Beta: relativamente probado, aunque no con la calidad óptima.
- Alpha: esto suele reflejar un buen primer prototipo, pero todavía mucha funcionalidad, puede estar fallando o no alcanza un estándar establecido.

- Inactivo: proyectos antiguos que se han retirado o menospreciado o que en algún momento han sido abandonados.

Obviamente para un CISO, los proyectos y las herramientas más interesantes serían las estables y fiables. Él puede confiar en una cierta calidad probada, y que estén disponibles y mantenidos hasta cierto punto en el futuro. Proyectos beta también pueden ser muy valiosos, ya que pueden representar a los proyectos que no han terminado su ciclo de revisión completa todavía, pero ya están disponibles para primeros adoptantes y que pueden ayudar a construir buenos cimientos para sus programas y herramientas de seguridad en el futuro.

Categorías de proyectos

Por lo general, los proyectos de OWASP se dividen ya sea en Herramientas o Documentación. Y por la categoría de uso: Constructores, Rompedores y Defensores. Estas categorías pueden ayudar al gerente a navegar rápidamente el amplio portafolio de herramientas de OWASP disponible y encontrar más fácilmente el proyecto adecuado para sus necesidades actuales.

Personas, procesos y tecnología

El CISO también puede optar por alcanzar sus objetivos de seguridad mediante tres elementos principales: Personas, Procesos y Tecnología. La gestión de la organización por lo general es importante para dar forma a los tres pilares para lograr el mejor impacto en toda la organización. Centrándose en sólo uno o dos de ellos puede dejar la organización vulnerable.

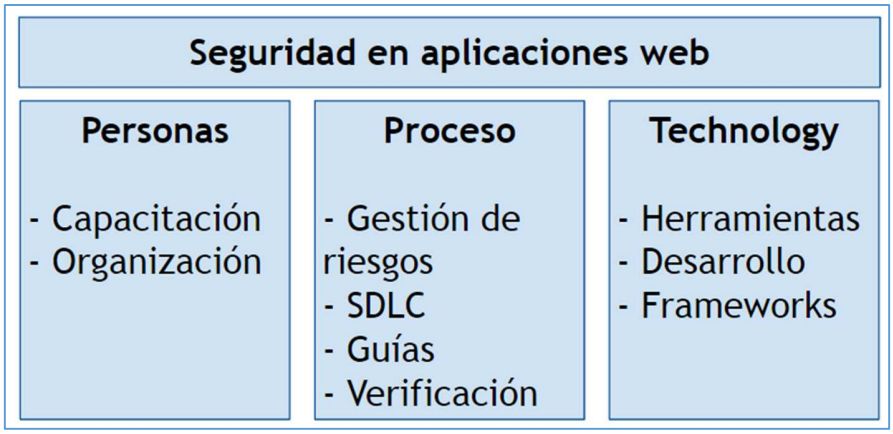

Figura 14 – Personas, Procesos y Tecnología

Personas

Este abordará la formación y motivación del personal, proveedores, clientes y socios. Si están bien educados y motivados, las posibilidades de comportamientos malintencionados o errores accidentales pueden reducirse drásticamente y muchas amenazas de seguridad básicas se pueden evitar.

Procesos

Si una organización se vuelve más madura, los procesos estarán bien definidos y permitirán a la fuerza de trabajo hacer las cosas de la manera “correcta”. Los procesos pueden asegurar que las acciones de la

organización se convirtieron confiables y repetibles. Por ejemplo, con los procedimientos operativos estándar bien definidos, el proceso de respuesta a incidentes será confiable y no dependerá de las decisiones ad hoc que antes hubieran variado con el decisor individual. En organizaciones muy maduras, los procesos de negocio y TI serán constantemente evaluados y mejorados. Si ocurre una falla, los procesos mejorados pueden permitir a una organización en su conjunto aprender de los errores del pasado y mejorar su funcionamiento a formas más eficientes y seguras.

Tecnología

La tecnología puede guiar y apoyar a las personas al proporcionar una buena formación y conocimiento por ser atractiva y motivadora para trabajar. La tecnología puede facilitar que una organización siga las prácticas de seguridad sólidas al proporcionar buenas herramientas, mientras que hace difícil para desviarse del camino correcto sin ser detectado. Por ejemplo, una buena tecnología sería automatizar los controles de acceso y autenticación y hacerlos muy simples para el usuario autorizado, al tiempo que niegan el acceso o privilegios a un atacante no autorizado. Por último, una serie de herramientas automatizadas pueden en segundo plano (*background*) y respaldar las personas y la organización en su trabajo de defender contra los riesgos de manera más eficaz y más eficiente. Muchas de las normas de seguridad y las herramientas (en OWASP y otros organismos) también pueden ser vistos como enfoques en las partes de este marco de trabajo. Por ejemplo, la capacitación del personal permitirá a la gente desarrollar su conocimiento de seguridad y hacer lo correcto, mientras que los diversos modelos SDLC pueden ayudar a una organización a establecer el nivel adecuado de procesos para sus mecanismos de desarrollo y de respuesta de incidentes.

Parte IV: Métricas para Gestionar Riesgos e Inversiones en Aplicaciones de Seguridad

IV-1 Resumen ejecutivo

Los CISOs necesitan métricas para reportar a la Gerencia la eficacia de la inversión realizada en el programa de seguridad de aplicaciones y el impacto en el riesgo del negocio. Los CISOs incluso las necesitan para gestionar y monitorear los recursos humanos, procesos y tecnologías que componen el programa de seguridad de aplicaciones.

Estas métricas están compuestos por tres categorías. Los CISOs deben ser capaces de responder las preguntas en base a las métricas y llevar a su equipo a brindar una respuesta lo más cercana posible al tiempo real, a través de medios automatizados. Las preguntas críticas incluyen:

- Métricas del proceso de seguridad de aplicaciones: ¿Cuán bien la organización organiza las políticas de seguridad, estándares técnicos y prácticas de la industria? ¿Cuán consistentemente se están ejecutando los SLAs de seguridad? ¿Por aplicación? ¿Por departamento? ¿Por canal?
- Métricas de riesgos de las aplicaciones de seguridad
    - Métricas de la gestión de riesgos de vulnerabilidad: ¿Cuál es el "tiempo significativo" para tener en cuenta de manera anual? ¿O de manera mensual? ¿Por aplicación? ¿Por departamento? ¿Cuáles son los puntos de seguridad conocidos que están actualmente en producción?
    - Métricas de incidentes de seguridad: ¿Qué puntos de seguridad han sido explotados? ¿Fueron esos puntos los que se liberaron en producción? ¿Cuál fue el costo para el negocio?
    - Métricas de informes sobre amenazas y monitoreo de ataques: ¿Cuáles son las aplicaciones que están recibiendo más ataques que otras? ¿Cuáles aplicaciones se prevé que tendrán un pico de utilización?
- Seguridad en las Métricas del SDLC
    - Métricas para las decisiones de mitigación de Riesgos: ¿Cuál es el tiempo significativo a considerar por una categoría de riesgo de aplicación? ¿Cumple con las expectativas? ¿Cómo es el mapa de riesgos? ¿Por aplicación? ¿Por departamento? ¿Por canal?
    - Métricas para la identificar los motivos del origen de la vulnerabilidad: ¿Cuáles son los motivos que originan vulnerabilidades para cada aplicación? ¿Hay algún problema sistemático? ¿Cuáles son las prácticas de seguridad que han sido mejor adoptadas por cada equipo de desarrollo? ¿Cuáles son los equipos de desarrollo que requieren más atención?
    - Métricas para inversiones en seguridad de software: ¿Qué fase del SDLC ha identificado la mayoría de los incidentes de seguridad? ¿Cuál es la madurez de las correspondientes prácticas de seguridad en cada fase del SDLC? ¿Cuál es la urgencia de más personal, procesos y tecnologías de seguridad en cada fase del SDLC?

Tenga presente que OWASP provee varios proyectos y orientación para CISOs, para ayudar a medir y monitorear seguridad y riesgos de los activos de aplicaciones en los cuales la organización desarrolla e implementa un programa de seguridad de aplicaciones. Mientras lee esta sección de la guía, por favor consulte el Apéndice B para más información sobre proyectos OWASP, acerca de la administración de riesgos de aplicación y dominio de monitoreo.

IV-2 Introducción

El objetivo en esta parte de la guía es ayudar a los CISOs a gestionar los diferentes aspectos del programa de seguridad de una aplicación - específicamente en riesgos y cumplimiento, además de los recursos de aplicaciones de seguridad tal como procesos, gente y herramientas. Una de las metas de estas métricas es medir los riesgos en la aplicación además de cumplir con los requisitos de seguridad impuestos por la legislación de seguridad de la información, sus regulaciones y estándares. En medio de esos procesos críticos de aplicaciones de seguridad que los CISOs necesitan informar y gestionar están procesos de desarrollo y aspectos operacionales tal como el manejo de vulnerabilidad de aplicaciones. Frecuentemente es responsabilidad de CISOs reportar el estado de la aplicación de seguridad al Dirección General, tal como, por ejemplo, el estado de las pruebas de seguridad de software y las actividades de seguridad del software en el SDLC.

Desde la perspectiva de gestión de riesgo, es importante que las métricas de seguridad de aplicación incluyan reportes técnicos sobre estos riesgos, tal como vulnerabilidades no mitigadas de aplicaciones que son desarrolladas y administradas por la organización. Otro aspecto importante de estas métricas es la cobertura de estas medidas, tales como el porcentaje del portafolio de aplicaciones regularmente evaluadas en el programa de verificación de seguridad de aplicaciones, el porcentaje de aplicaciones internas vs las externas cubiertas, los riesgos inherentes de estas aplicaciones y el tipo de evaluación de seguridad, y cuando en el SDLC estos son ejecutados. Estos tipos de métricas ayudan a los CISOs en la presentación de informes sobre el cumplimiento del proceso de seguridad de las aplicaciones así como sobre los riesgos en la seguridad de las aplicaciones, tanto a los responsables de la Seguridad de la Información como a los propietarios de las aplicaciones de negocios.

Como una de las responsabilidades de CISOs es gestionar ambas: seguridad de la información y los riesgos de seguridad de las aplicaciones y con ellas tomar decisiones de cómo solucionarlas, es importante que estas métricas sean capaces de medir estos riesgos en términos de exposición al riesgo que existe para los activos de la organización que incluyen aplicaciones de datos y funciones.

IV-3 Métricas y objetivos de las mediciones

El objetivo de las métricas del proceso de seguridad de aplicaciones es determinar qué tan bien los procesos de seguridad de aplicaciones de la organización cumplen los requisitos de seguridad definidos por las políticas de seguridad y los estándares técnicos. Por ejemplo, un proceso de vulnerabilidad de aplicaciones puede incluir la ejecución de evaluaciones de aplicaciones expuestas en Internet, cada 6 o cada 12 meses, dependiendo de la calificación de riesgo inherente a la aplicación. Otro requisito del proceso de vulnerabilidad de aplicaciones podría ejecutar seguridad en múltiples procesos del SDLC, tales como el análisis de riesgo de la arquitectura, modelado de amenazas, análisis de código fuente estático, revisiones de código seguro y pruebas de seguridad basadas en riesgo en aplicaciones que almacenan información confidencial de individuos, y en las cuales, la funcionalidad del negocio es un servicio crítico para ciudadanos, clientes, consumidores, empleados, etc.

Desde la perspectiva de la cobertura del proceso, uno de los objetivos de estas métricas puede ser informar acerca de la cobertura del proceso de seguridad de aplicaciones, tales como medir el modo en que las aplicaciones entran dentro del alcance de las evaluaciones de seguridad de aplicaciones, para identificar potenciales huecos en las evaluaciones de vulnerabilidad basadas en los tipos de aplicaciones y en los requisitos de seguridad de aplicaciones. Esto ayuda a los CISOs a proveer visibilidad en la cobertura de procesos así como del estado de la ejecución operativa de los programas de seguridad de aplicaciones. Por ejemplo, las métricas pueden mostrar (podría ser en estado rojo) que algunos de los procesos de seguridad de aplicaciones en el SDLC tales como revisiones de código seguro, no están siendo ejecutados por un número de aplicaciones catalogadas como de alto riesgo, y etiquetarlas como un elemento sin cumplir de los requisitos de pruebas de seguridad. Este tipo de indicadores permite al CISO priorizar recursos ubicando los mismos donde sean más necesarios para cumplir con los requisitos del estándar del proceso.

Otra medición importante para la verificación de la seguridad de aplicaciones es medir el tiempo cuando los procesos de seguridad de aplicaciones son planificados versus cuando son ejecutados, para identificar demoras potenciales en la revisión del código de seguridad, análisis de código fuente estáticos, *hacking* ético y procesos de pruebas de penetración.

IV-4 Métricas de riesgo de seguridad en las aplicaciones

Métricas para la gestión de riesgo de vulnerabilidades

Las responsabilidades de los CISOs incluye la gestión de riesgo de seguridad en las aplicaciones. Desde la perspectiva técnica del riesgo, los riesgos de seguridad en las aplicaciones pueden ser debido a vulnerabilidades en las aplicaciones que exponen los activos de aplicaciones tales como los datos y las funciones críticas sujetas a potenciales ataques que tratan de comprometerlos.

Típicamente, la gestión del riesgo técnico comprende la mitigación de los riesgos planteados por las vulnerabilidades mediante la aplicación de arreglos o contramedidas. La mitigación de los riesgos de estas vulnerabilidades normalmente se prioriza en base a una medición cualitativa de los riesgos.

Por ejemplo, por cada aplicación que es desarrollada y gestionada por la organización, habría un cierto número de vulnerabilidades identificadas a través de un ranking de severidad (por ejemplo: alto, medio, bajo). Cuanto mayor sea el número de vulnerabilidades con riesgo alto y medio, mayor es el riesgo para la aplicación. Cuanto mayor sea el valor conjuntos de datos protegidos por la aplicación y la criticidad de las funciones soportadas, mayor el impacto de esas vulnerabilidades en los activos de aplicaciones.

Un punto importante en las métricas de las vulnerabilidades es el número de vulnerabilidades que quedan sin corregir. Un determinado número de vulnerabilidades en las aplicaciones todavía podrían estar "abiertas", que si aún no se corrigió en el entorno de producción, y esto representa un riesgo para la organización y requiere que el CISO priorice las acciones de mitigación de riesgos como "cerrar" la vulnerabilidad dentro de los plazos de cumplimiento que se considera aceptable por las normas de gestión de vulnerabilidades de aplicaciones.

Métricas de incidentes de seguridad

Otras métricas importantes para los CISO gestionando los riesgos de seguridad de información son los informes de incidentes de seguridad relacionados con las aplicaciones que son desarrolladas y/o gestionadas por la organización. El CISO podría recopilar esta información desde SIRT *(Security Incident Response Team* o Equipo de Respuesta a Incidentes de Seguridad por sus siglas en inglés) que afectan a una aplicación determinada debido a la explotación de una vulnerabilidad. La correlación de los incidentes de seguridad reportados para una aplicación determinada con las vulnerabilidades reportadas por las pruebas de seguridad permite al CISO priorizar los esfuerzos para mitigar los riesgos en las vulnerabilidades que pueden causar el mayor impacto a la organización. Obviamente, esperar que un incidente de seguridad ocurra para decidir qué vulnerabilidad mitigar es un síntoma reactivo más que un enfoque proactivo hacia la gestión del riesgo, pero la retroalimentación es importante.

Informes inteligencia de amenazas e métricas de monitoreo de ataques

Las organizaciones que son proactivas con el riesgo no esperan que los incidentes de seguridad ocurran sino que aprenden de otros ataques, de vulnerabilidades publicadas y de información de amenazas, usando la información para ajustar las evaluaciones de gravedad y de riesgo, tomar medidas proactivas para la mitigación del riesgo tales como desarrollar e implementar contramedidas o priorizando la mitigación de vulnerabilidades conocidas con el riesgo, que pueden ser potencialmente explotadas para

causar el mayor impacto en la organización. El CISO puede usar el informe de inteligencia de amenazas así como también los indicadores de eventos de seguridad de la capa de aplicaciones monitoreada tales como las de sistemas SIEM y aplicaciones *"honeypot"* para evaluar el nivel de riesgo. Desafortunadamente hoy, la mayoría de los incidentes de seguridad son encontrados y reportados meses después de la intrusión inicial o desde el momento que fueron comprometidos los datos. Métricas de seguridad que disparen acciones y que apunten a la prevención de riesgos de ataques son de vital importancia para los CISOs porque pueden facilitar decidir cuáles aplicaciones poner bajo un monitoreo y alerta estricta para poder ser capaz de actuar más rápidamente en caso de un ataque, reduciendo el impacto del evento. Por ejemplo:

- Una alerta de amenaza de una posible denegación de servicio distribuida contra aplicaciones de banca online puede permitir al CISO poner a la organización en alerta y preparar para aplicar contramedidas para evitar una interrupción posterior.
- Una amenaza reportada de *malware* que tiene como objetivo las aplicaciones de *e-commerce* para robar credenciales de usuarios y llevar adelante compras no autorizadas permite al CISO emitir alertas de seguimiento para el equipo de gestión de monitoreo de eventos de incidentes.
- Una vulnerabilidad publicada en un *framework* o librería puede alterar la planificación del CISO de prueba de parches, implementación y verificación.

IV-5 Métricas de Gestión de Seguridad en SDLC

Métricas para decisiones de mitigación de riesgos

Una vez identificadas las vulnerabilidades, en cualquier etapa de desarrollo y operación, el paso siguiente es decidir qué debe corregirse, cuándo y cómo. La primera pregunta se puede responder a través del proceso de evaluación de vulnerabilidades, que podría indicar por ejemplo, que las vulnerabilidades de alto riesgo deben ser corregidas en lapsos de tiempo menores que las vulnerabilidades de mediano y bajo riesgo. El requerimiento puede variar también en función del tipo de aplicación, no siendo lo mismo por ejemplo una aplicación totalmente nueva, desarrollada recientemente, que una nueva versión de una aplicación existente. Como las nuevas aplicaciones no han sido probadas previamente, representan un riesgo mayor que las aplicaciones existentes, y por lo tanto, esto podría requerir que las vulnerabilidades de alto riesgo sean tratadas antes de la liberación de la aplicación en el ambiente de producción. Una vez que los problemas son identificados y priorizados para su corrección en base a la gravedad de la vulnerabilidad, el siguiente paso es determinar cómo solucionarlo. Esto depende de factores como el tipo de la vulnerabilidad, controles y medidas de seguridad que se ven afectados, y donde es más probable que dicha vulnerabilidad haya sido introducida. Este tipo de métrica permite al CISO identificar las causas de las vulnerabilidades y presentar el caso al equipo de desarrollo de aplicaciones para su corrección.

Métricas para identificar las causas raíces de las vulnerabilidades.

Cuando las métricas de vulnerabilidades se registran como una tendencia, esto permite a los CISO evaluar mejoras. Por ejemplo, en el caso de un único problema, medido a través del tiempo para el mismo tipo de aplicación, es posible para el CISO señalar causas potenciales y principales. Con indicadores de tendencia y categorización del tipo de vulnerabilidades, es posible para los CISO generar un modelo de negocio para invertir en ciertos tipos de actividades de seguridad, tales como la mejora de procesos, la adopción de las herramientas de *testing*, así como la formación y la concientización. Por ejemplo, la siguiente figura muestra que los indicadores presentaron tendencias positivas para cierto tipo de vulnerabilidades mediante la comparación de dos versiones trimestrales de la misma aplicación.

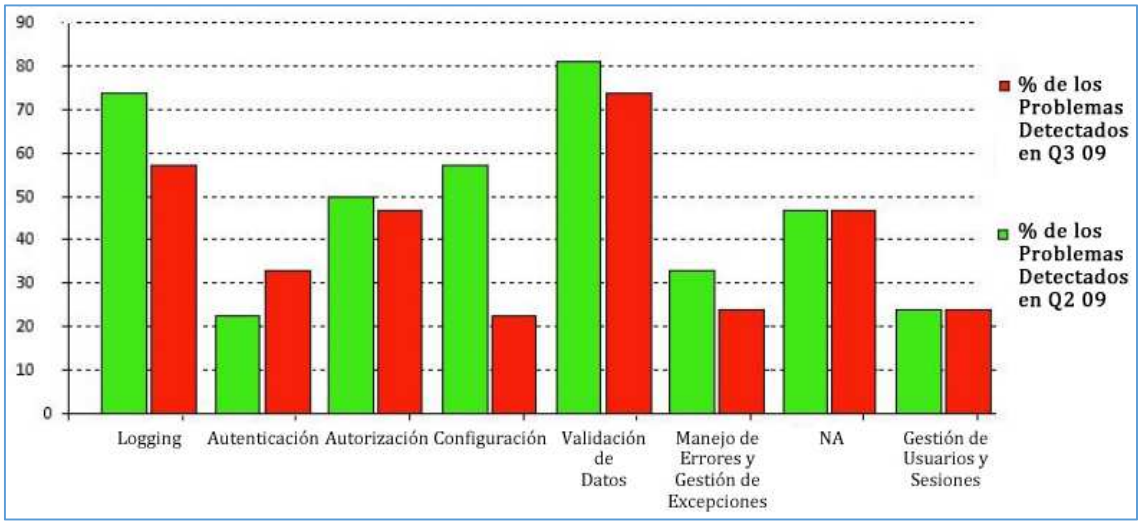

Figura 15 - Indicadores de evolución en dos versiones de una misma aplicación

Los CISO pueden utilizar estas métricas para discutir con los CIOs y directores de desarrollo, si la organización está mejorando o empeorando con el tiempo, al realizar liberaciones de aplicaciones más seguras, y para destinar recursos en seguridad (por ejemplo, procesos, personas y herramientas) a donde más se necesiten para la reducción de riesgos. Con las métricas que se muestran en la figura, por ejemplo, suponiendo que los cambios en la aplicación introducidos entre versiones no difieren mucho en términos de tipo y complejidad, así como tampoco en el número y el tipo de los desarrolladores en el equipo de desarrollo, y las herramientas utilizadas, se puede enfocar en el tipo de vulnerabilidades que la organización está teniendo problemas para corregir, tales como un mejor diseño e implementación de la autenticación y controles de administración de usuarios y sesiones. El CISO podría entonces coordinar con el CIO y los directores de desarrollo para planificar una capacitación específica en este tipo de vulnerabilidades, guías de desarrollo de documentos para la autenticación y gestión de sesiones y adoptar casos de prueba específicos de seguridad. En última instancia este esfuerzo coordinado facultará a los desarrolladores de software en el diseño, implementación y prueba, de controles de gestión de autenticación y de sesión más seguros, además de mostrar esto como mejoras en las métricas de vulnerabilidad.

Métricas para inversiones en seguridad de software

Otro aspecto importante de las métricas de seguridad del S-SDLC es decidir en qué lugar del SDLC se debe invertir en pruebas de seguridad y corrección. Para saber esto, es importante medir en qué fase del SDLC se originan la mayoría de las vulnerabilidades (el mayor porcentaje), cuándo estas vulnerabilidades han sido probadas, y cuánto es el costo para la organización de solucionarlos en cada fase.

Un indicador de ejemplo que mide esto se visualiza en la figura siguiente, basado en un caso de estudio sobre costos de pruebas de software y gestión errores *(Ref. Capers Jones Study)*.

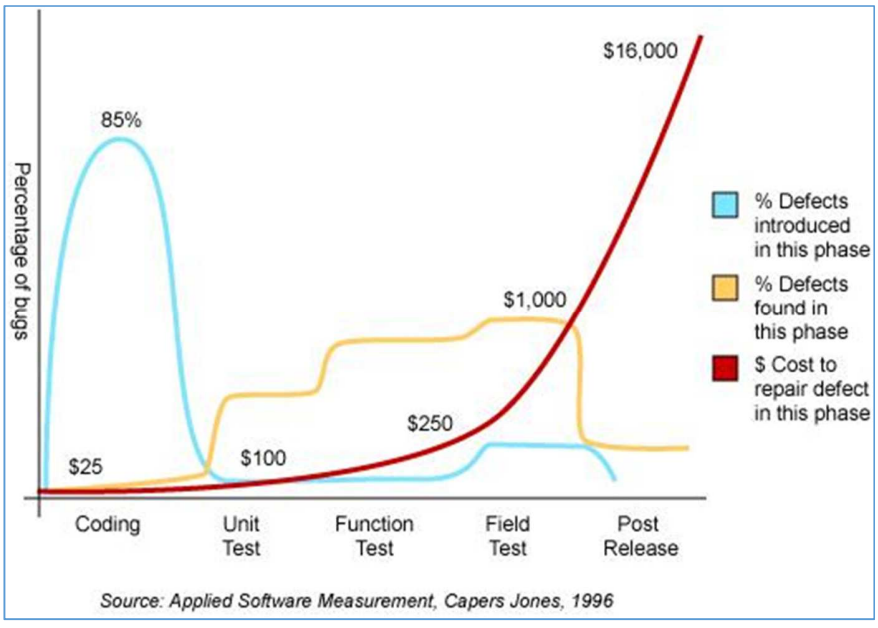

Figura 16 – Cómo manejar el testing y bugs en las diferentes etapas del SDLC

Un tipo similar de métricas de gestión de defectos de seguridad puede ser utilizado por los CISO para gestionar con eficacia los problemas de seguridad mediante la reducción de costos globales de seguridad.

Suponiendo que el CISO ha implementado seguridad en todo proceso de SDLC y ha asignado el presupuesto para la inversión en seguridad de actividades como la capacitación en programación segura, el proceso de revisión de código seguro y herramientas de análisis de código estático, estos indicadores permiten al CISO hacer inversiones en pruebas y corrección de problemas de seguridad en las primeras fases del SDLC. Esto basado en las siguientes mediciones del caso de estudio:

- La mayoría de las vulnerabilidades son introducidas por los desarrolladores de software durante la programación.
- La mayoría de estas vulnerabilidades son probadas durante las pruebas de campo antes liberar el software a producción.
- La prueba y corrección de vulnerabilidades en etapas tardías del SDLC es forma más ineficiente trabajar, ya que resulta aproximadamente diez veces más caro de solucionar un problema durante las pruebas de pre-producción que durante las pruebas unitarias.

CISO puede utilizar casos de estudios de vulnerabilidades como estos o utilizar sus propias métricas para hacer la propuesta para invertir en actividades de desarrollo seguro de software, ya que estas ahorrarán tiempo y dinero a la organización.

3. Información de soporte

Referencias

En orden de lanzamiento y publicación.

2013

- Verizon 2013 Data Breach Investigation Report: http://www.verizonenterprise.com/DBIR/2013/
- Security Innovation and the *Ponemon Institute*: The Current(2013) State of Application Security Report: https://www.securityinnovation.com/security-lab/our-research/current-state-of-applicationsecurity.html

2012

- Security Innovation and *Ponemon Institute*'s 2012 Application Security Gap Study: A Survey of IT Security & Developers: https://www.securityinnovation.com/uploads/Application%20Security%20Gap%20Report.pdf

2011

- Verizon 2011 Data Breach Investigation Report: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

- US Q2 2011 GDP Report Is Bad News for the US Tech Sector, But With Some Silver Linings: http://blogs.forrester.com/andrew_bartels/11-07-29-us_q2_2011_gdp_report_is_bad_news_for_the_us_tech_sector_but_with_some_silver_linings

- *Imperva*'s July 2011 Web Application Attack Report: http://www.*Imperva*.com/docs/HII_Web_Application_Attack_Report_Ed1.pdf

2010

- First Annual Cost of Cyber Crime Study Benchmark Study of U.S. Companies, Sponsored by ArcSight Independently conducted by *Ponemon Institute* LLC, July 2010: http://www.arcsight.com/collateral/whitepapers/Ponemon_Cost_of_Cyber_Crime_study_2010.pdf

- 2010 Annual Study: U.S. Cost of a Data Breach: http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach

2009 y anteriores

- OWASP Security Spending Benchmarks Project Report: https://www.owasp.org/images/b/b2/OWASP_SSB_Project_Report_March_2009.pdf

- Identity Theft Survey Report, Federal Trade Commission, September, 2003: http://www.ftc.gov/os/2003/09/synovatereport.pdf

- PCI DSS: https://www.pcisecuritystandards.org/security_standards/index.php
- OWASP Application Security Verification Standard: https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

Guidelines and Best Practices

- OWASP Top Ten: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Supplement to Authentication in an Internet Banking Environment: http://www.fdic.gov/news/news/press/2011/pr11111a.pdf
- Feiman, Joseph. Teleconference on Application Security. 9 Oct. 2008. Gartner. 30 Sept. 2013: http://www.gartner.com/it/content/760400/760421/ks_sd_oct.pdf

Security Incidents and Data Breaches

- Data Loss Database: http://*DataLossDB*.org/
- WHID, Web Hacking Incident Database: http://projects.webappsec.org/w/page/13246995/WebHacking-Incident-Database
- Sony data breach could be most expensive ever: http://www.csmonitor.com/Business/2011/0503/Sony-data-breach-could-be-most-expensive-ever
- Dmitri Alperovitch, Vice President, Threat Research, McAfee, Revealed: Operation Shady RAT: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf
- Health Net discloses loss of data to 1.9 million customers: http://www.computerworld.com/s/article/9214600/Health_Net_discloses_loss_of_data_to_1.9_million_customers
- Albert Gonzalez data breach indictment: http://www.wired.com/images_blogs/threatlevel/2009/08/gonzalez.pdf
- Share prices and data breaches: http://www.securityninja.co.uk/data-loss/share-prices-and-databreaches/
- EMC spends $66 million to clean up RSA SecureID mess: http://www.infosecurityus.com/view/19826/emc-spends-66-million-to-clean-up-rsa-secureid-mess/

Security Investments and Budgets

- Gordon, L.A. and Loeb, M.P. “The economics of information security investment”, ACM Transactions on Information and Systems Security, Vol.5, No.4, pp.438-457, 2002.
- Total Cost of Ownership: http://en.wikipedia.org/wiki/Total_cost_of_ownership
- Wes SonnenReich, Return of Security Investment, Practical Quantitative Model: http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf

- Tangible ROI through Secure Software Engineering: http://www.mudynamics.com/assets/files/Tangible%20ROI%20Secure%20SW%20Engineering.pdf
- The Privacy Dividend: the business case for investing in proactive privacy protection, Information Commissioner's Office, UK, 2009: http://www.ico.gov.uk/news/current_topics/privacy_dividend.aspx
- A commissioned study conducted by Forrester Consulting on behalf of VeriSign: DDoS: A Threat You Can't Afford To Ignore: http://www.verisigninc.com/assets/whitepaper-ddos-threatforrester.pdf
- The Security Threat/Budget Paradox: http://www.verizonbusiness.com/Thinkforward/blog/?postid=164
- Security and the Software Development Lifecycle: Secure at the Source, Aberdeen Group, 2011: http://www.aberdeen.com/Aberdeen-Library/6983/RA-software-development-lifecycle.aspx
- State of Application Security - Immature Practices Fuel Inefficiencies, But Positive ROI Is Attainable, Forrester Consulting, 2011: http://www.microsoft.com/downloads/en/details.aspx?FamilyID=813810f9-2a8e-4cbf-bd8f-1b0aca7af61d&displaylang=en
- Dan E Geer Economics and Strategies of Data Security: http://www.amazon.com/EconomicsStrategies-Data-Security-DANIEL/dp/B001LZM1BY

Acerca de OWASP

Descripción

El Proyecto Abierto de Seguridad en Aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a habilitar a las organizaciones para desarrollar, comprar y mantener aplicaciones confiables. Todas las herramientas, documentos, foros y capítulos de OWASP son gratuitos y abierto a cualquiera interesado en mejorar la seguridad de aplicaciones. Abogamos por resolver la seguridad de aplicaciones como un problema de gente, procesos y tecnología porque las soluciones más efectivas incluyen mejoras en todas estas áreas. Nos puede encontrar en www.owasp.org.

OWASP es un nuevo tipo de organización. Nuestra libertad de presiones comerciales nos permite proveer información sobre seguridad en aplicaciones sin sesgos, práctica y efectiva. OWASP no está afiliada a ninguna compañía de tecnología, aunque soportamos el uso informado de tecnologías de seguridad comerciales. Parecido a muchos proyectos de software de código abierto, OWASP produce muchos materiales en una manera abierta y colaborativa. La Fundación OWASP es una entidad sin ánimo de lucro para asegurar el éxito a largo plazo del proyecto.

OWASP se formó en 2001, de una manera totalmente orgánica, cuando un grupo de profesionales de la seguridad se dio cuenta de lo terriblemente insegura que era la forma en que desarrollamos nuestras aplicaciones web. El objetivo inicial se consideró que era modesto: escribir una guía para los desarrolladores, que documentaría las prácticas de desarrollo de seguridad de software. Mientras que el esfuerzo inicial estaba destinado a durar un par de semanas, lo que surgió fueron varios cientos de páginas. Cuando se libera la Guía de OWASP para construir aplicaciones web seguras fue un éxito inmediato. La Serie de Guías de OWASP ahora abarca seis documentos.

OWASP es un lugar donde la gente buena se reúne para ayudar a aumentar la conciencia sobre los problemas de seguridad en aplicaciones. Es un esfuerzo de base, con la fuerza impulsora de ser las personas que están lidiando con estos problemas todos los días, y con ganas de echar una mano para cambiar la situación para mejor. La Fundación OWASP es una entidad sin fines de lucro que asegura el éxito a largo plazo del proyecto.

La Fundación OWASP es una organización sin fines de lucro en EE.UU. tipo 501 ©. OWASP Europa VZW es una organización sin fines de lucro registrada en Bélgica.

Participación

Todo el mundo es bienvenido a participar en nuestros foros, proyectos, capítulos y conferencias. OWASP es un lugar fantástico para aprender sobre seguridad de la aplicación, para hacer *networking*, e incluso a construir su reputación como un experto. Documentos, herramientas y otros recursos de Todo de OWASP se publican mediante licencias de código abierto, y están disponibles de forma gratuita.

Capítulos locales

OWASP tiene casi 200 capítulos locales en todo el mundo. Reuniones de los capítulos son siempre libres para asistir, son un proveedor neutral y las presentaciones están disponibles sin costo alguno en la

página web de cada capítulo. Las reuniones ayudan discusión local de fomento de seguridad de aplicaciones en todo el mundo.

Para encontrar su local de capítulo, información sobre cómo iniciar una nueva, y cómo dirigir un capítulo ver:

https://www.owasp.org/index.php/OWASP_Chapter

https://www.owasp.org/index.php/Chapter_Leader_Handbook

Conferencias OWASP AppSec

Durante los últimos diez años, las conferencias OWASP AppSec promovieron a la industria, el gobierno, los investigadores de seguridad, y los profesionales a discutir el estado de la técnica en seguridad de aplicaciones. Conferencias AppSec mundiales se celebran cada año en América del Norte, América Latina, Europa y Asia Pacífico. Además, eventos regionales se celebran en lugares como Brasil, China, India, Irlanda, Israel, y Washington DC. Diapositivas de presentación y grabaciones de vídeo están disponibles de forma gratuita en el sitio web de OWASP después de cada conferencia.

Para los próximos eventos mundiales y regionales ver:

https://www.owasp.org/index.php/Category:OWASP_AppSec_Conference

Citas

Para encontrar casi 80 legislaciones, normas, directrices, comités nacionales e internacionales y códigos de prácticas del sector que hacen referencia a OWASP ver:

https://www.owasp.org/index.php/Industry:Citations

Ayudar a apoyar la misión de OWASP

Muchas organizaciones han sido apoyadores corporativos o educativos. Muchos más han alentado a sus empleados a contribuir con tiempo y recursos para proyectos de OWASP.

OWASP también ha producido seis documentos de orientación para otros grupos, lo que sugiere cómo podrían mejorar su apoyo a la misión de OWASP. Estos son conocidos como los Códigos de Conducta de OWASP de seguridad de aplicaciones, para organismos gubernamentales, instituciones educativas, grupos de estándares, organizaciones profesionales, organismos de certificación y organizaciones de desarrollo. Los códigos de conducta se pueden descargar desde la página del proyecto:

https://www.owasp.org/index.php/OWASP_Codes_of_Conduct

4. Apéndices

Apéndice A: Valor de los datos y costo de un incidente

Esta es una referencia rápida para guiar en como asignar un valor monetario a los activos de información para determinar el impacto monetario para la organización en caso de que tales activos se pierdan a causa de un incidente de seguridad. Se incluye también en este apéndice una sencilla fórmula para determinar el potencial riesgo de responsabilidad, en el caso de que ocurran incidentes con pérdida de datos, y también una herramienta de cálculo para estimar el costo en violación de datos, basada en datos estadísticos.

El valor de la información

La selección de las medidas de seguridad debe considerar el valor de los activos a ser protegidos. Del mismo modo que los datos personales, todos los tipos de datos pueden tener un valor determinado desde un número de diferentes perspectivas. Si bien puede ser comúnmente visto el valor del dato por su valor como activo de la organización o por el costo de un incidente, estos no siempre son las valorizaciones más apropiadas a considerar.

Por ejemplo, un informe que muestra el valor de un dato personal (información identificable personalmente) sugiere cuatro perspectivas desde la cual la información personal grafica su valor de privacidad. Estas son:

- Su valor como un activo utilizado en las operaciones de la organización
- Su valor para el individuo con el que éste se relaciona
- Su valor para con otras partes quienes pueden querer utilizar esa información, ya sea para propósitos legítimos o impropios
- Su valor social según la interpretación de reguladores y otros grupos

El valor para la persona sujeto del dato, terceros o a la sociedad, puede ser más apropiado para algunas organizaciones que otras. El informe también examina consecuencias más amplias sobre no proteger datos (personales) y los beneficios de su protección. Este describe como los incidentes que involucran datos personales y conducen a fraudes financieros, pueden tener impactos importantes en individuos, pero también que los efectos financieros no son el único impacto. El informe provee métodos de cálculo, y ejemplos donde el registro del dato personal de los individuos puede estar entre los U$S 800 y 1800 en el año 2008.

Violación de datos y pérdidas económicas

En relación a las pérdidas económicas por víctima, la cifra exacta varía dependiendo de los factores considerados para calcularlas, dependiendo del tipo de industria y del tipo de ataque que causa los incidentes de pérdida de datos. De acuerdo a un estudio realizado en Julio del 2010 por el *Ponemon Institute* en 45 organizaciones de diferentes sectores de la industria sobre costos en los ciberataques, el costo de los ataques vía web es el 17% de los costos de los ciberataques registrados por año. Este costo varía a través de diferentes sectores de la industria, siendo mayores los costos en Servicios de Defensa,

Energía y Financieros (U$S 16,31 millones, U$S 15,63 millones y U$S 12,37 millones respectivamente) que en comparación con las empresas de ventas minoristas, servicios y educación.

Del mismo modo, y de acuerdo al estudio anual del *Ponemon Institute* en el año 2011, sobre costos en pérdida de datos para las compañías en EEUU, el promedio de costo por registro comprometido en el 2010 fue de U$S 214, un 5% más con respecto al año 2009. De acuerdo a este estudio, el sector de comunicaciones sostiene los costos más altos, de U$S 380 por cliente, seguido por los servicios financieros con U$S 353, y luego por los servicios en salud con U$S 345, medios de comunicación con U$S 131, educación con U$S 112 y sector público con U$S 81.

La compañía de seguridad Symantec, que ha hecho de sponsor para el informe, desarrolló junto con el *Ponemon Institute* una herramienta de cálculo de riesgo para casos de violación de datos, y puede ser usada para calcular la probabilidad de pérdida de datos para los siguientes 12 meses, así como también para calcular el costo promedio por pérdida y costo promedio por registro perdido.

La estimación de costos directos realizada por el *Ponemon Institute*, también fue utilizada para la estimación de los costos directos de los incidentes de pérdida de datos recolectados por OSF *DataLossDB*. La cifra del costo directo para el año 2009 fue de U$S 60 por registro es multiplicado por el número de registros informados por cada incidente, para así obtener la estimación de la pérdida monetaria. Se asume que los costos directos son sufridos por las organizaciones vulneradas, si bien esto no siempre es verdad, como en el caso de las tarjetas de crédito donde los costos directos pueden a menudo sufridos por bancos y emisores de tarjetas. Además de lo mencionado, los costos estimados no incluyen costos indirectos (ej. tiempo, esfuerzo y otros gastos de recursos organizacionales) así como también los costos de oportunidad (Ej. el costo resultante de la pérdida de oportunidad de negocios debido al daño en la reputación).

Otra manera posible de tomar decisiones de gestión de riesgos, y en cuanto a si se debe mitigar una potencial pérdida, es determinar si la compañía será legalmente responsable por dicha pérdida de datos. Mediante el uso de la definición de "responsabilidad legal" a partir de la ley de casos de responsabilidad de los Estados Unidos, tomando la Probabilidad (P) de pérdida, (L) el monto de la Pérdida, entonces existe responsabilidad siempre que el costo de las precauciones adecuadas o la Carga (B) de la compañía sea:

$$B < P \times L$$

Mediante la adopción de esta fórmula, en los datos del año 2003 de la Comisión Federal de Comercio (FTC), la probabilidad de pérdida es del 4,6%, que representa la población que ha sufrido ataque de fraude de identidad, mientras que la Pérdida por Víctima es calculada mediante la factorización del dinero que se gastará para recuperarse de la pérdida, considerando el tiempo gastado, y fue de 300 millones de horas con un salario por hora de U$S 5,25, más los gastos de bolsillo de U$S 5 billones.

$$L = [\text{Tiempo Gastado} \times \text{Recupero de la Pérdida} \times \text{Salario por Hora} + \text{Gastos de Bolsillo}]/\text{Número de Víctimas}$$

Con esta fórmula para calcular la cantidad de pérdida esperada para un incidente de fraude de identidad, basada en los datos de FTC del año 2003, la pérdida por cliente/víctima es aproximadamente de U$S 655 y la carga impuesta a la compañía es de U$S 30,11 por cliente/víctima por incidente.

La decisión de administración del riesgo está en definir cuándo es posible proteger un cliente por U$S 30,11 por cliente por año. Si es así, entonces la responsabilidad existe y hay riesgo de responsabilidad para

la compañía. Este cálculo puede ser muy útil para determinar el potencial riesgo de responsabilidad en casos de incidentes de pérdidas de datos, por ejemplo aplicando la cifra del FTC al *TJX Inc.* Incidentes en el 2007, donde inicialmente fue anunciada la exposición de la información confidencial de 45.700.000 clientes, la exposición de los incidentes para las víctimas afectadas podría calcularse como:

Costo de la exposición al incidente = Número de víctimas expuestas por el incidente x Pérdidas por víctima

Con esta fórmula usándolos datos de *TJX Inc.* o víctimas afectadas y aplicando la pérdida por víctima usando los datos de la FTC, el costo del incidente que representa la pérdida potencial es de U$S 30 billones. Factorizándolo con la probabilidad de ocurrencia del incidente, entonces es posible determinar cuánto dinero debería gastarse en medidas de seguridad. En el caso de los incidentes de *TJX Inc.* por ejemplo, asumiendo una chance de 1 en 1000 de ocurrencia, entonces estaría justificado un programa de seguridad con una erogación de 30 millones de dólares para la empresa *TJX Inc*.

Herramientas de cálculo para violación de datos

Un calculador para estimar costos incurridos por organizaciones, a través de sectores de la industria, después de experimentar una pérdida de datos, es provisto por Symantec basado en los datos encuestados del *Ponemon Institute*: https://databreachcalculator.com/

Estimando la probabilidad de aprovechamientos de vulnerabilidad

Para estimar la probabilidad de un aprovechamiento de vulnerabilidad en una aplicación web específica, podemos referirnos a informes de la WHID. La WHID es un Consorcio de Seguridad para Aplicaciones Web, proyecto creado para proporcionar informes de análisis estadísticos de incidentes de seguridad en aplicaciones web recogidos de fuentes públicas. En 2010 WHID categorizó 222 incidentes y observó que el 33% de los incidentes fueron dirigidos a hacer caer los sitios web (ej. con Denegación de Servicio), el 15% a desfigurar los sitios web y el 13% a robar información. De la totalidad de los tipos de ataques que buscan explotar vulnerabilidades tales como Inyecciones SQL ocupan el 21%.

Tomando los datos de WHID para el 2010 de los incidentes reportados y analizando, la probabilidad total de que un ataque esté dirigido a robar información a través explotando una vulnerabilidad de inyección SQL es por lo tanto 13% x 21% = 2.7%. Debido a que la Inyección SQL también fue reportada para para desfigurar un sitio, debe ser considerada una estimación aproximada.

En otro estudio del tráfico de ataques web maliciosos observados sobre un período de 6 meses, de Diciembre de 2010 a Mayo de 2011 desde la compañía de Seguridad *Imperva*, la inyección SQL fue identificada en el 23% de los ataques como tercera más frecuente luego de los *Cross-site Scripting* como segunda más frecuente en el 36% de los ataques, siendo finalmente la indexación de directorios abiertos el que más frecuente con el 37% de todos los ataques.

Estimando el Impacto en el Negocio de las Explotaciones de Vulnerabilidades

Comparando los estudios de los ataques vía web de WHID e *Imperva*, un orden de magnitud de 21 al 23% para los ataques de explotación de la vulnerabilidad inyección SQL parece una estimación aproximada. Asumiendo que el costo de la pérdida de datos de los incidentes de seguridad para una organización financiera de U$S 355 por registro (Datos del año 2010 del *Ponemon Institute*), y la probabilidad de que tal

incidente explote una vulnerabilidad del tipo inyección SQL es del 2.7 % (Datos del año 2010 de WHID), en 2010 la responsabilidad para el sitio web de una compañía tal como *homebanking* para la pérdida de datos de 1 millón de registros es de esta manera de U$S 9.585.000. Con esta cifra, un presupuesto de U$S 9.000.000 gastado por una organización financiera para la aplicación de medidas de seguridad, específicamente enfocadas en prevenir riesgos de pérdida de datos debido a ataques de inyección SQL, podría haber sido justificable.

Asumiendo que gastará como mucho en medidas de seguridad, esta es la cantidad máxima estimada para gastos en medidas de seguridad para frustrar ataques de inyección SQL que incluyan adquisición de tecnología para desarrollar software de seguridad, documentación, estándares, procesos, herramientas y costos para el reclutamiento de personal calificado y entrenamiento en códigos de seguridad especialmente para desarrolladores web. Normalmente esta cifra en dólares debería ser considerada un valor máximo dado que asumimos por ejemplo una pérdida total de los datos del usuario.

Es importante notar que las vulnerabilidades por inyección son consideradas por OWASP (2013 A1-Inyección) el riesgo de seguridad más crítico de aplicaciones para las explotaciones de vulnerabilidad oportunistas.

OWASP califica el riesgo de inyección de datos, incluyendo la vulnerabilidad por inyección SQL como severa ya que *"puede resultar en corrupción o pérdida de datos de la contabilidad, o denegación de acceso o en algunos casos conducen a una completa caída del host"*. El impacto de negocio que hemos calculado como responsabilidad para una compañía de servicios financieros de tamaño medio (1 millón de usuarios registrados para el *homebanking*) asume que el valor de los activos de datos pueden ser robados por un hacker para causar un daño tangible a la compañía.

Históricamente, los ataques de Inyección SQL han sido de alto impacto y en los Estados Unidos, han estado asociado con una de las rupturas más importantes de datos que se haya cometido y procesado. En Agosto de 2009, un caso de acusación contra Albert Gonzalez (también acusado en mayo del 2009 en Massachusetts por una violación contra *TJX Inc.*) y otros dos hackers Rusos, ataques de inyección SQL fueron usados para introducirse dentro de la red *7-Eleven* en agosto 2007 cuyo resultado fue el robo de datos de tarjetas de crédito. Supuestamente, el mismo tipo de ataque fue utilizado para infiltrarse en *Hannaford Brothers* en noviembre 2007 el cual resultó en 4,2 millones de números de tarjetas de débito y crédito robadas y 130 millones de números de tarjetas de créditos de *Heartland Payment Systems* en diciembre de 2007. En 2010, Albert Gonzalez fue encontrado culpable y sentenciado a cumplir 20 años de prisión, mientras que *Heartland* pagó cerca de U$S 140 millones de dólares en multas debido a las brechas de seguridad.

Resumen

Podemos ver que hay diferentes formas de determinar el valor de la información y que algunos de estos están puramente basados en los costos relacionados a la violación de datos. Pero en promedio, las referencias sugieren que típicamente los datos individuales pueden ser valuados en un rango entre U$S 500 y U$S 2000 por registro.

Apéndice B: Referencia rápida a otras guías y proyectos en OWASP

Guía AppSec CISO: Referencia Rápida para Guías y Proyectos de OWASP

Esta referencia rápida mapea las típicas funciones de los CISO y los dominios de seguridad de la información a diferentes secciones de la Guía CISO y proyectos de relevancia de OWASP.

Función del CISO	Dominio de seguridad	Guía OWASP CISO	Proyectos OWASP
Desarrollar e implementar políticas, estándares y guías para seguridad de aplicaciones.	Estándares y políticas	I- 3 Estándares de Seguridad de la Información, Políticas y Cumplimiento	• Development Guide - Policy *Frameworks* • Project CLASP - Identify Global Security Policy • Project SAMM - Policy & Compliance • Guía de revisión de código - Revisión de código y cumplimiento
Desarrollar, implementar y gestionar el gobierno de la seguridad de aplicaciones	Gobierno	I- 3 Estándares de Seguridad de la Información, Políticas y Cumplimiento	• Project SAMM - Governance • Project ASVS - How to Write Job Requisitions
Desarrollar e implementar desarrollo seguro de software y procesos de pruebas de seguridad	Procesos de Ingeniería de Seguridad	III-4 Enfocando las actividades de Seguridad en Software y procesos del S-SDLC III-5 Cómo elegir los proyectos de OWASP adecuados para su organización	• Development Guide • Code Review Guide • Secure Coding Practices • Testing Guide • Comprehensive Lightweight Application Security Process (CLASP) Introduction • CLASP Concepts • Software Assurance Maturity Model (SAMM) • Testing Guide - Tools • Project Application Security Verification Standard Project (ASVS)
Desarrollar, articular e implementar una estrategia de gestión de riesgo para aplicación	Estrategia de Riesgos	I-4 Gestión de riesgos II - Criterios para gestionar riesgos de seguridad en aplicaciones III-4 Estrategia de riesgos	• SAMM - Strategy & Metrics • Application Threat Modeling - Mitigation Strategies
Trabajar con la dirección ejecutiva, directores de negocio, auditoría interna y consejero legal para definir requerimientos de seguridad de aplicaciones que puedan ser verificados y auditados	Auditoría y Cumplimiento	I-3 Capturando requerimientos de seguridad en aplicaciones III-3 Abordando las Funciones de seguridad de aplicaciones del CISO	• Application Security Verification Standards • CLASP - Capture Security Requirements • SAMM - Security Requirements • Testing Guide - Security Requirements Test Derivation • Project Cornucopia • Project Secure Software Contract Annex
Medir y monitorear la seguridad y los riesgos de los activos de aplicación dentro de la organización	Métricas de riesgo y monitoreo	IV - Selección de Métricas para Gestionar Riesgos e Inversiones en Seguridad de Aplicaciones	• CLASP - Define and Monitor Metrics • SAMM - Strategy & Metrics • Types of Application Security Metrics
Definir, identificar y evaluar la seguridad inherente de activos de aplicación crítica, evaluar las amenazas, vulnerabilidades, impactos comerciales y recomendar	Análisis de riesgo y gerenciamiento	I-4 Gestión de riesgos II - Criterios para gestionar riesgos de seguridad en aplicaciones	• Project Top Ten Web Application Risks • Project Top Ten Mobile Application Risks • Project Top Ten Cloud Risks • ASVS - Implementation of NIST Risk Management Verification Activities • Risk Rating Methodology • Threat Risk Modelling

acciones correctivas/contramedidas			• Application Threat Modelling
Evaluar la contratación de nuevos procesos de aplicación, servicios, tecnologías y herramientas de seguridad	Licitaciones	III-4 Evaluar riesgos antes de la adquisición de componentes/servicios de terceros	• Project Secure Software Contract Annex • ASVS - Verification of Contract Requirements
Supervisar el entrenamiento en seguridad de aplicaciones para el desarrollo, operación y equipos de seguridad de la información	Entrenamiento de seguridad	III-5 Personas, procesos y tecnología	• Project CLASP Institute Awareness Programs • Education Projects • Appsec Training Videos • Conference Videos • Application Security FAQs
Desarrollar, articular e implementar continuidad planificación/recuperación ante desastres	Continuidad de negocios y Pla de recuperación de desastres	III-3 Abordando las Funciones de seguridad de aplicaciones del CISO	• Cloud Business Continuity and Resiliency
Investigar y analizar los incidentes de seguridad sospechosos y reales y recomendar acciones correctivas	Gestión de vulnerabilidades y respuesta a incidentes	I-4 Responder a las expectativas del negocio después de un incidente de seguridad	• SAMM Vulnerability Management • CLASP - Manage Security Issue Disclosure Process • .NET Incident Response