METPROSEG en RSI: construir la seguridad en el proceso de desarrollo desde unos cimientos sólidos

Consciente de que la seguridad en el proceso de desarrollo de software y aplicaciones es un aspecto clave para robustecer y llegar a conseguir un nivel de seguridad razonable y apropiado de las infraestructuras telemáticas, Rural Servicios Informáticos (RSI) abordó un proyecto de diseño e implantación de una Metodología de Programación Segura (METPROSEG) dentro de lo que se denomina S-SDLC (Secure Software Development Lifecycle), asociado al SDLC. La decisión fue atacar este asunto desde la raíz, comenzando por el diseño de una metodología y por la concienciación y formación en seguridad en el proceso de desarrollo de su personal, siendo éstas las dos primeras piezas claves y fundamentales dentro del Proyecto. Además se trazó la hoja de ruta de las siguientes fases como la auditoria de código y *hacking*, *benchmark* comparativo de resultados respecto al mercado, plan de acción, corrección y mejora de posibles debilidades, diseño de controles y análisis de riesgos en el SDLC en lo relativo a seguridad y, sobre todo, se sentaron las bases de que esto es una parte más del proceso de mejora continua, sistematizando las auditorías de código y *hacking* de manera periódica.


Pedro Pablo López Bernal / Vicente Aguilera Díaz

A pesar del trabajo realizado por organizaciones como OWASP [1], SANS [2] o NIST [3] en la difusión y educación en seguridad, el último informe de Cenzic [4] relativo a la evolución de la seguridad en las aplicaciones web en el segundo semestre del año pasado, pone de manifiesto que las vulnerabilidades y el número de ataques sobre dichas aplicaciones sigue en aumento.

Quizás uno de los aspectos más preocupantes es que las vulnerabilidades más explotadas actualmente se deben a problemas que ya son públicos desde hace años (SQL Injection y Cross Site Scripting encabezan la lista) y que, por lo tanto, deberíamos conocerlas con el suficiente nivel de detalle como para no sufrirlas en nuestros desarrollos.

Este hecho revela que hay algo que no se está haciendo bien: o no se entiende la amenaza, o no se conoce cómo aplicar las medidas de seguridad para evitarla; o asumimos de forma consciente o inconsciente estos riesgos, quizás porque desconocemos la dimensión real del problema.

Cualquier estrategia de seguridad que aborde la creación de software seguro debe incluir, entre otras muchas actividades, la educación y concienciación, a la vez que la puesta a disposición de medios y guías de ayuda, del personal involucrado, en la creación del mismo.

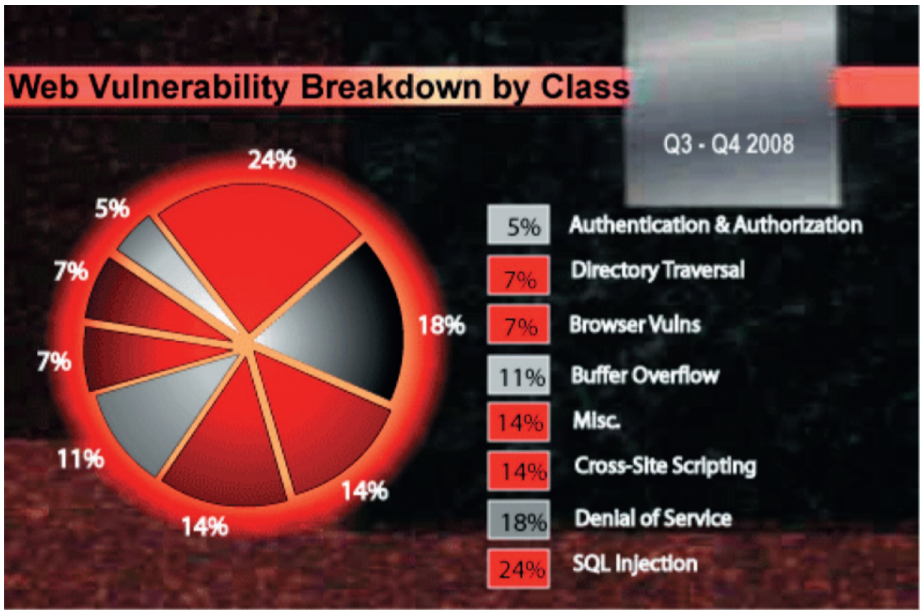

Figura 1. Web Vulnerability Breakdown by Class. (Fuente: Cenzic Inc.)

Para comenzar con la fase de diseño e emplantación de la metodología METPROGSEG, RSI seleccionó a Internet Security Auditors como proveedor con experiencia en este campo.

Dicha educación debe ocupar un lugar destacado dentro de las buenas prácticas de seguridad, y así lo recogen las principales estrategias que existen actualmente, donde algunas de éstas, como BSIMM (*Building Security In Maturity Model*) [5] u OWASP OpenSAMM (*Software Assurance Maturity Model*) [6], dedican una parte importante de sus cuatro dominios de actuación a esta actividad.

En el planteamiento propuesto por Rural Servicios Informáticos (RSI) para implantar un S-SDLC (*Secure Software Development Lifecycle*), se contempló que la formación y entrenamiento de su personal debía ser el punto de inicio de su estrategia para desplegar con éxito sus aplicaciones, entendiendo como éxito que los desarrollos dispongan del nivel de seguridad y calidad requerido según las características de cada aplicación. Para dicho entrenamiento seleccionó a Internet Security Auditors, entidad con amplia experiencia en la auditoría de aplicaciones y formación de equipos de desarrollo.

Cabe destacar que la adopción de un S-SDLC no implica reemplazar el SDLC actual, sino complementarlo con las buenas prácticas de seguridad requeridas en cada etapa. Así, el trabajo de Internet Security Auditors no debía consistir en redefinir las actividades que llevaban a cabo los equipos de desarrollo, sino en integrar las buenas prácticas de seguridad en dichas actividades.

En el proyecto para RSI, se abordó la educación del personal como el eje vertebral que iniciaría la hoja de ruta hacia la consecución del S-SDLC.

Como parte de dicha labor de educación, Internet Security Auditors abordó dos tareas

principales: creación de guías prácticas de seguridad para el desarrollo seguro de aplicaciones web, y formación a los distintos equipos sobre la aplicación de dichas guías de seguridad.

Dicho proceso de educación se inició con una formación sobre conceptos genéricos y técnicas de seguridad en la que se instruyó a los distintos roles que componen los equipos de desarrollo de RSI. Esta formación, que permitió que todo el personal adquiriera una base de conocimientos común en los aspectos de seguridad, perseguía dos claros objetivos: concienciar a todo el personal involucrado en el desarrollo de la necesidad de aplicar unos principios de seguridad, y conseguir que los jefes de proyecto considerasen la seguridad como uno de los objetivos a cumplir, de la misma forma que un requerimiento funcional.

Esta primera formación se complementó con una guía de buenas prácticas para el desarrollo seguro de aplicaciones web. La elaboración de esta guía se basó en el proyecto de Clasificación de Amenazas de WASC (*Web Application Security Consortium*), en los principios de seguridad recogidos en la Guía de Desarrollo de OWASP (*Open Web Application Security Project*) y en la propia experiencia del equipo de Auditoría de Internet Security Auditors en sus más de ocho años realizando pentest y auditoría de código de aplicaciones.

Una vez completada esta primera etapa, se planificó conjuntamente con el personal de RSI la siguiente fase que consistía en profundizar en los conocimientos de seguridad que se habían adquirido. En este caso, resulta relevante destacar el hecho de que RSI utiliza un amplio abanico de tecnologías en sus desarrollos, por lo que se optó por instruir a su personal en función de la tecnología con la que trabajaban y con personal cualificado por parte de Internet Security Auditors para cada tecnología tratada.

De esta forma, se elaboraron guías de buenas prácticas en el desarrollo específicas para cada una de las tecnologías empleadas, y se impartió formación eminentemente práctica sobre cómo aplicar dichas buenas prácticas de seguridad en función de las capacidades que ofrece cada tecnología.

Así, las amenazas y riesgos presentados en la etapa anterior tuvieron su visibilidad en el contexto analizado, donde los distintos perfiles (desde jefes de proyecto, arquitectos, diseñadores, analistas, responsables de seguridad y, por supuesto, desarrolladores) pudieron experimentar, en el área de su responsabilidad, las medidas de seguridad a adoptar para evitar o mitigar las principales deficiencias que sufren las aplicaciones web.

De esta forma, y a través de aplicaciones de prueba especialmente diseñadas, se dieron a conocer, entre otros aspectos y de forma práctica, las principales vulnerabilidades que sufren actualmente las aplicaciones, a qué se deben, qué implicación tienen el negocio y, por supuesto, las técnicas y mecanismos de seguridad que nos ayudan a evitarlas, mitigarlas o minimizar su impacto en el caso de una explotación de las mismas. Asimismo, se dieron a conocer mediante ejemplos prácticos herramientas de gran utilidad para realizar pruebas de seguridad, análisis de código o búsqueda de vulnerabilidades, entre otros aspectos.

Como resultado, la aportación de Internet Security Auditors ha permitido a RSI:

- Evaluar las prácticas de seguridad adoptadas y conocer su evolución.
- Iniciar la construcción de un programa de madurez de seguridad en el desarrollo de software que complemente al ya existente CMMi, (nivel 3 ya alcanzado).

No cabe duda de que RSI es consciente de que el trabajo realizado no es suficiente para alcanzar el nivel de madurez de seguridad en el desarrollo de software deseado por la entidad, pero sí ha sentado la base para su consecución y para la iteración periódica de auditorías de código y *hacking* en distintas aplicaciones, que junto con otros programas basados en el cumplimiento PCI/DSS, ISO27001, LOPD, etc., pueden permitir alcanzar el nivel de expectativas deseado; y sobre todo, avanzar en la cultura de seguridad y construcción de servicios seguros, pensando ya en arquitecturas SOA. ■

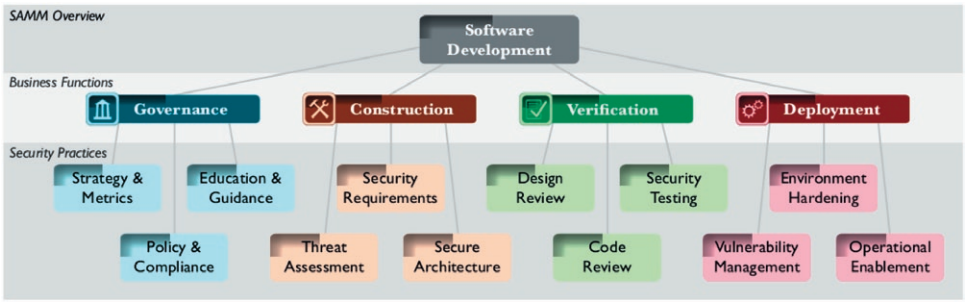

Figura 2. Dominios de actuación y principales actividades de OpenSAMM.

Aunque el trabajo realizado no es suficiente para alcanzar el nivel de madurez de seguridad en el desarrollo de software deseado, sí ha sentado la base para su consecución y para la iteración periódica de auditorías de código y hacking en distintas aplicaciones, que junto con otros programas basados en el cumplimiento PCI/DSS, ISO27001, LOPD, etc., pueden permitir alcanzar el nivel de expectativas deseado y avanzar en la cultura de seguridad y construcción de servicios seguros, pensando ya en arquitecturas SOA.

Pedro Pablo López Bernal
Gerente Infraestructura de Seguridad, Auditoría y Normalización
RURAL SERVICIOS INFORMÁTICOS-RSI
pedro_pablo_lopez_rsi@cajarural.com

Vicente Aguilera Díaz
Director de Auditoría
INTERNET SECURITY AUDITORS
vaguilera@isecauditors.com

REFERENCIAS

[1] OWASP (Open Web Application Security Project) http://www.owasp.org
[2] SANS Institute. http://www.sans.org
[3] NIST (National Institute of Standards and Technology). http://www.nist.gov
[4] Web Application Security Trends Report Q3-Q4 2008 http://www.cenzic.com/downloads/Cenzic_AppSecTrends_Q3-Q4-2008.pdf
[5] The Building Security In Maturity Model. http://www.bsi-mm.com
[6] OWASP OpenSAMM (Software Assurance Maturity Model). http://www.opensamm.org