SEGURIDAD EN APLICACIONES

Por Marcos A. Polanco Velasco, CISSP, CISM, CISA

IMPACTO DE LA SEGURIDAD APLICATIVA EN EL NEGOCIO

Cada vez las aplicaciones tienen mayores funcionalidades y proveen más acceso a la información sensible del negocio, por otro lado la velocidad a la que crece esta información en la mayoría de las organizaciones sobrepasa su capacidad de protegerla y gestionarla.

La evolución rápida y constante de las técnicas de hacking es indiscutible, se estima que cada semana se publica al menos un incidente de seguridad que afecta a información sensible[1,2]. De 2005 a la fecha se estima que se ha comprometido la seguridad de más de 245 millones de registros conteniendo información sensible[1] y según un estudio de Forrester Reseach, el costo para una organización por registro perdido/robado ronda entre $90 y $300 dólares.

De acuerdo al análisis de los resultados de más de 300 proyectos de hacking ético realizados durante los últimos 4 años por el Application Defense Center (ADC) de Imperva, sólo el 5% de las aplicaciones están libres de vulnerabilidades.

Según el informe del Cenzic Intelligent Analysis Lab de Cenzic, el 80% de las aplicaciones tienen vulnerabilidades severas que pueden derivar en consecuencias como ejecución arbitraria de código, acceso no autorizado a información, daño financiero o negación de servicios. En este mismo informe, se estima que en el mundo Web el 79% de las vulnerabilidades están en las aplicaciones, mientras que el 12% en los plugins y controles ActiveX, el 7% en los navegadores y sólo el 2% en los servidores Web.

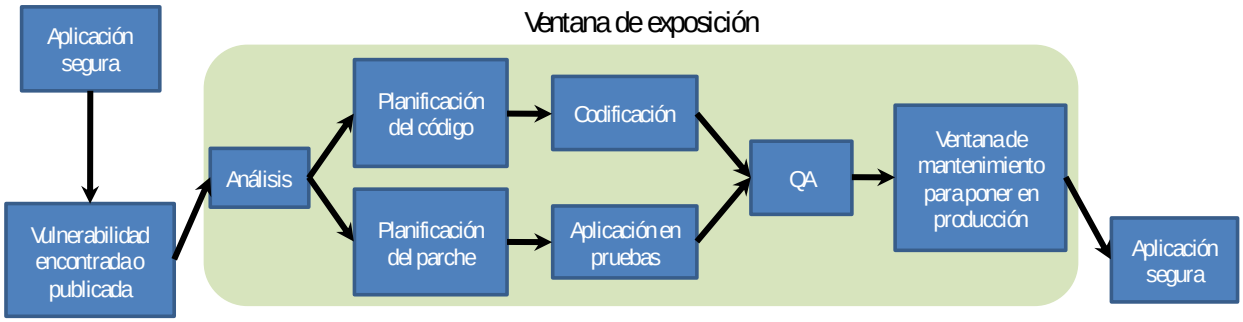
De acuerdo al informe de mitad de año de 2009 del X-Force de ISS/IBM del total de vulnerabilidades publicadas, el 49% de ellas no cuentan con un parche o fix al momento de darse a conocer.

Las vulnerabilidades que más han llamado la atención en los últimos años son las de SQL Injection y Cross-site Scripting y muchas organizaciones ya han tomado medidas al respceto, sin embargo, existe otros tipos de vulnerabilidades asociadas a fuga y exposición de información que están presentes en la mayoría de las aplicaciones (hasta en un 83%)[3].

Hoy por hoy, sin lugar a dudas, las aplicaciones representan uno de los más grandes retos en seguridad para las organizaciones.

EL COSTO DE LA GESTIÓN DE VULNERABILIDADES

Una nueva vulnerabilidad normalmente nos obliga a implementar soluciones de emergencia ya sean parches o cambios a la configuración y una vez hechos esos cambios es necesario realizar una serie de pruebas para asegurar que no afecten la funcionalidad de la aplicación y que no presenten nuevos problemas que puedan ser incluso más graves que la misma vulnerabilidad.



Esto puede tener implicaciones (tiempo, costo, improductividad) importantes en los ambientes de producción. El costo de solucionar una vulnerabilidad en una aplicación en las fases tempranas de desarrollo es mucho menor que hacerlo ya que está en fase de operación.

Se ha estimado que el costo por vulnerabilidad en la etapa de desarrollo es de aproximadamente $500 dólares, mientras que en la fase de pruebas llega a $7,000 dólares y en la fase de produccion alcance los $14,000[5].

Por otro lado, normalmente dejamos la seguridad aplicativa en manos de las pruebas de hacking ético, que aunque son un mecanismo importante para ayudar a mejorar la seguridad de las aplicaciones, no podemos depender únicamente de ellas.

La mayoría de las vulnerabilidades encontradas en una prueba de hacking ético deben ser resueltas y revalidadas (sobre todo las críticas), sin embargo, los estudios indican que en un alto porcentaje no se resuelven correctamente, generando una falsa sensación de seguridad.

Por otro lado, la naturaleza de estas pruebas conlleva una serie de problemas por ejemplo:

- Pueden existir vulnerabilidades en las aplicaciones pero que no hayan sido encontradas por los expertos (hackers éticos)
- Puede haber vulnerabilidades no cubiertas por el alcance de las pruebas ya sea por falta de tiempo o de presupuesto.
- Asimismo, pueden existir nuevas vulnerabilidades que se hayan descubierto o publicado después de haber sido realizado el estudio
- Pueden producirse nuevas vulnerabilidades que se hayan introducido a nivel código en el desarrollo evolutivo o correctivo de las aplicaciones.

Se estima que una aplicación que ha pasado por un proceso completo de análisis de vulnerabilidades (hacking ético) y parcheo antes de ponerse en producción, será vulnerable, con alta probabilidad, en un periodo entre 6 y 12 meses[1].

CÓMO LOGRAR SEGURIDAD EN LAS APLICACIONES

En nuestra experiencia la seguridad en las aplicaciones se logra a través de un enfoque integral que considere la combinación de una serie de elementos complementarios tales como aspectos tecnológicos, organizacionales y normativos.

Deberá considerarse la interacción entre distintas áreas de la organización entre las que al menos deben estar la de seguridad, de desarrollo, de operaciones y de bases de datos.

El enfoque deberá ser gradual, definiendo alcances específicos para cada fase de tal forma que se garantice que en cada una de ellas se aumenta escalonadamente el nivel de seguridad.

Finalmente se debe considerar que este tipo de iniciativas toman tiempo por lo que se deben plantear proyectos de largo plazo con avances continos y constantes.

Los componentes necesarios para lograr la seguridad en las aplicaciones son los siguientes:

- **Evaluación aplicativa**
  El primer elemento que a considerar es la evaluación continua de todas y cada una de las aplicaciones, considerando primero aquellas que son más críticas. Para ello es necesario iniciar con un inventario actualizado de todas las aplicaciones incluyendo versiones, actualizaciones, parches, configuraciones, etc.

  De igual forma se deberá tener visibilidad de todas y cada una de las bases de datos existentes sobre todo de aquellas que almacenan información sensible de la

organización. Así como una clasificación de la información para distinguir claramente lo que es sensible de lo que no lo es.

Para cada aplicación se deberá realizar una gestión de riesgos específica.

Asimismo, se debe tener una política de ejecución de pruebas de hacking ético de modo continuo, que evalué las vulnerabilidades de las aplicaciones antes de pasarlas a producción y después de cada modificación al entorno donde se ejecutan.

Una vez encontradas las vulnerabilidades deberán ser priorizadas para que sean solucionadas. Este proceso de evaluación y solución, también puede servir como un vehículo de formación, ya que al encontrar las vulnerabilidades en las aplicaciones, evaluar su impacto y buscar su solución hay un aprendizaje continuo.

Es necesario también utilizar los servicios públicos de alerta temprana y las bases de datos de vulnerabilidades para facilitar la evaluación.

- **Sensibilización y formación**
  Es indispensable sensibilizar a todos las partes interesadas sobre la existencia de los riesgos identificados en la etapa de evaluación aplicativa y transmitir claramente la necesidad de mitigarlos.

  También se debe realizar la formación tanto a los grupos de seguridad como a los de desarrollo. Es decir, los expertos en seguridad deben saber más sobre las aplicaciones y el ciclo de vida de desarrollo de sistemas (SDLC) y las áreas de desarrollo tienen que saber más de seguridad y considerarla una parte integral del proceso SDLC. Es decir, aprender Desarrollo Seguro. Según Fortify la formación en buenas prácticas de desarrollo seguro puede disminuir un 25% la introducción de vulnerabilidades a nivel código.

  Por otro lado también es importante la formación a los grupos de operación en temas de seguridad aplicativa, en especial a los responsables del monitoreo de aplicaciones. Los grupos de monitoreo tienen que entender lo que una alerta de seguridad en una aplicación significa y deberán contar con elementos para determinar si es o no una falsa alarma.

- **Desarrollo Seguro**
  Uno de los elementos clave para lograr la seguridad aplicativa es el uso de buenas prácticas en el desarrollo para que las aplicaciones sean seguras por diseño, desde las fases iniciales del SDLC (requerimientos) hasta las pruebas y puesta en producción. Incluyendo la asignación de los roles de arquitectura de seguridad y el de diseño de seguridad aplicativa.

  Se debe considerar también la evaluación automatizada de vulnerabilidades a nivel código. Deberán existir políticas (normatividad) que impidan la puesta en producción de aplicaciones que no hayan sido totalmente probadas.

- **Arquitectura de seguridad**
  Finalmente como parte de la arquitectura de seguridad de las aplicaciones se deberán considerar los controles normativos a implementar así como los controles tecnológicos (incluyendo productos comerciales) a implementar; principalmente firewalls aplicativos y de base de datos para tener visibilidad del tráfico aplicativo y poder distinguir lo que es legítimo de lo que no lo es.

  También es importante que los grupos de operaciones cuenten con elementos de monitoreo que les permitan saber lo que sucede con las aplicaciones.

Referencias:
[1] White Paper “How safe is it out there?” Imperva Inc.
[2] Annual Report: “The Web Hacking Incidents Database 2008” Breach security Inc.
[3] “Cenzic Web Application Security Trends Report Q3-Q4, 2008”, Cenzic Inc.
“IBM Internet Security Systems X-Force 2009 Mid-Year Trend and Risk Report”
[5] CISO’s Guide to Application Security” Fortify