Administración Electrónica

SEGURIDAD EN APLICACIONES WEB

CCN-CERT
Centro Criptológico Nacional

Centro Criptológico Nacional

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos establece, en su Título Preliminar, que "*Las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias*".

Para reforzar este objetivo, en su artículo 42, la Ley crea el Esquema Nacional de Seguridad que, en estos momentos, se encuentra en fase de desarrollo. La mayoría de los servicios electrónicos que pondrán las diferentes administraciones (general, autonómica y local) a disposición de los ciudadanos serán a través de servicios web o, en su defecto, estos servicios se verán involucrados en algún momento.

Se considera crítico, por tanto, la verificación de la seguridad de los servicios y aplicaciones web, así como disponer de los mecanismos de alerta necesarios que permitan identificar compromisos en estos servicios.

Además, por desgracia, estos servicios suelen estar sometidos a la presión del tiempo y la necesidad de una puesta en funcionamiento urgente, para poder, de esta forma, incrementar los trámites "on line" de los ciudadanos. Esta rapidez en el ciclo de vida de desarrollo provoca que la gestión de seguridad se realice de manera deficiente y las aplicaciones y servicios web se pongan en producción sin una completa validación desde el punto de vista de la seguridad.

Para mitigar este problema, en apoyo al desarrollo de la citada Ley 11/2007 y en virtud de las funciones contempladas en el RD 421/2004, que regula al Centro Criptológico Nacional (CCN), y a través de la Capacidad de Respuesta ante Incidentes Gubernamental (CCN-CERT), se han realizado diversas acciones relacionadas con la seguridad de los servicios y aplicaciones web de las sedes electrónicas.

> Desde el CCN se intenta concienciar a las diferentes administraciones para que mejoren la seguridad de los servicios prestados al ciudadano

Como **primera medida**, y dentro de la función del CCN de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la

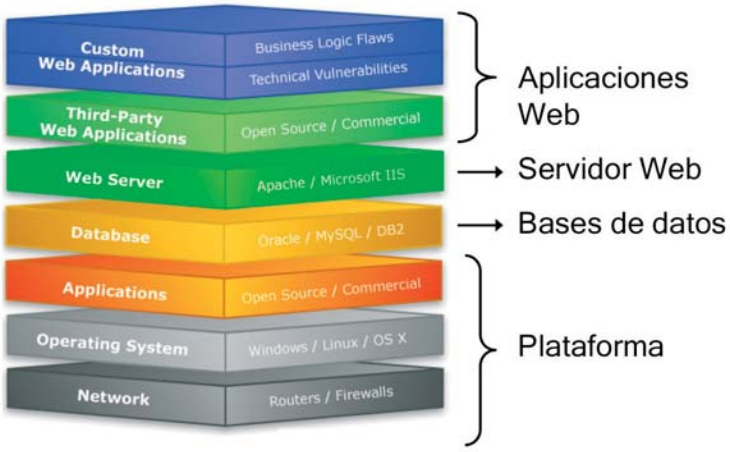

Figura 1. Capas de seguridad de una aplicación web típica

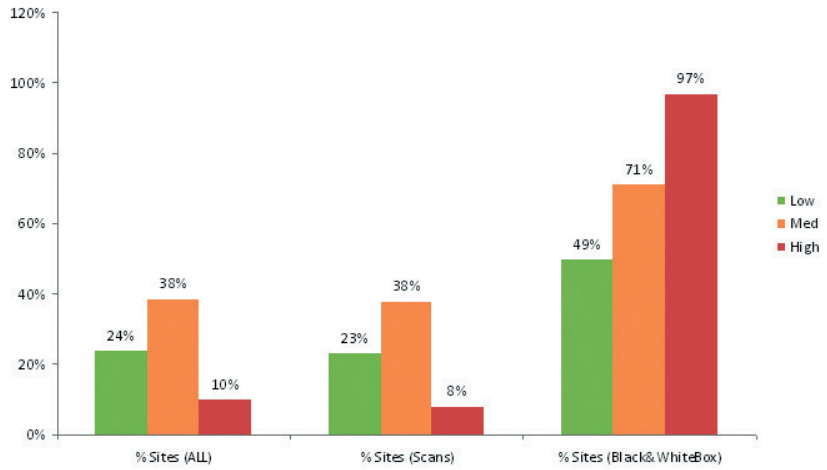

Figura 2. Estadísticas de detección de vulnerabilidades críticas dependiendo del método utilizado

Se considera crítico la verificación de la seguridad de los servicios y aplicaciones web, así como disponer de mecanismos de alerta

seguridad de las TIC en la Administración establecida en el RD 421, se ha desarrollado la Guía CCN-STIC 412 "*Requisitos de seguridad de entornos y aplicaciones web*" y está en proceso la CCN-STIC 413 "*Auditorías en entornos y aplicaciones web*".

Como **segunda medida**, y dentro del cometido de formar al personal de la Administración que tiene el CCN, desde el año 2008 se desarrolla un curso sobre aplicaciones web, en las que se realiza una aproximación multidisciplinar a los diferentes elementos de la arquitectura de seguridad de la sede electrónica.

En la guía 412 y en este curso del plan de formación STIC del CCN, se identifican la arquitectura de un servicio web seguro, el detalle técnico de los posibles ataques, los requisitos para realizar una auditoría y unas listas de comprobación que permitan al responsable la verificación de la seguridad implementada en el servicio web.

En la CCN-STIC 412 se citan diversas fuentes, entre las que destaca el consorcio de seguridad en aplicaciones web (www.webappsec.org). Este consorcio proporciona diversas estadísticas, como la que muestra la probabilidad de detección de vulnerabilidades críticas en diferentes páginas web, según el procedimiento de análisis utilizado. Además, se resalta que, mediante análisis automáticos, la probabilidad de detección de vulnerabilidades críticas que pueden comprometer el sistema es del 8% pero, utilizando el conjunto completo de técnicas de auditoría (automáticas y manuales), la probabilidad de detección de estas vulnerabilidades se eleva al 97%. Esta estadística se muestra en la figura adjunta.

Pensando en las vulnerabilidades y la exposición de las aplicaciones web, el CCN-CERT considera como incidentes prioritarios para su actuación, tanto el ataque contra las infraestructuras en Internet de las administraciones públicas, como cualquier ataque distribuido contra esta infraestructura. En la figura adjunta se muestra la relación de incidentes prioritarios del CCN-CERT.

Así se remiten alertas tempranas a diferentes organismos sobre posibles infecciones con código dañino o sobre la existencia de páginas web con vulnerabilidades

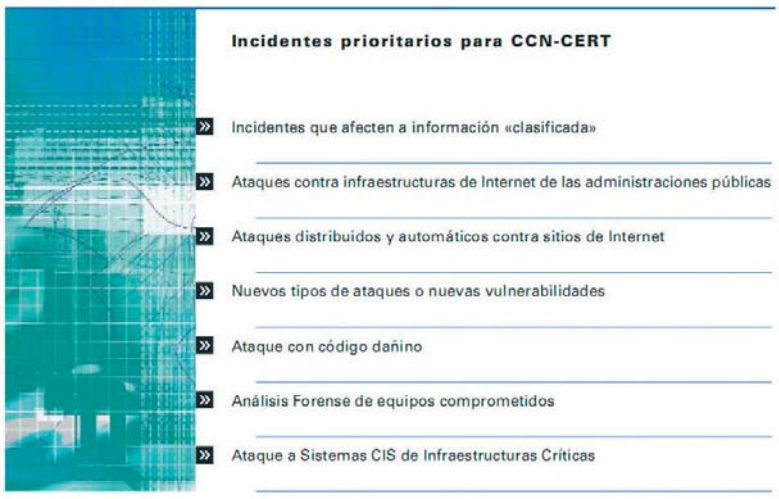

Figura 4. Incidentes prioritarios para el CCN-CERT

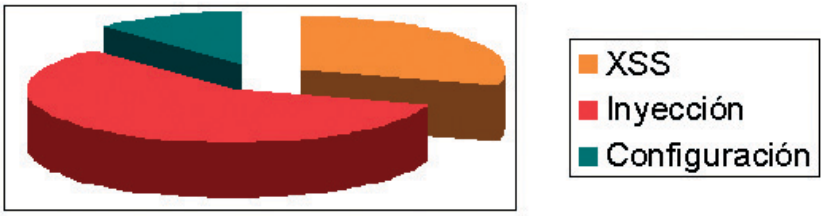

Figura 3. Tipos de vulnerabilidades detectadas por el CCN, en porcentaje

identificadas en las diversas comunidades de *hackers*.

Como **tercera medida**, el CCN-CERT lleva a cabo auditorías a páginas web de distintos Organismos de las administraciones públicas en busca de posibles vulnerabilidades críticas, con el fin de establecer las pautas adecuadas para reducirlas o eliminarlas.

Estas auditorías demuestran que los problemas de seguridad en las diferentes sedes electrónicas son similares y siguen patrones parecidos a las estadísticas publicadas en organismos como el citado anteriormente sobre servicios web. En este sentido, destacan las vulnerabilidades de inyección de código SQL, las vulnerabilidades del tipo XSS (Cross Site Scripting) y las deficiencias de configuración del equipamiento como se muestra en la figura adjunta.

Los problemas de seguridad en las diferentes sedes electrónicas son similares y siguen patrones parecidos a las estadísticas publicadas

Estas vulnerabilidades pueden provocar alteraciones no autorizadas de la base de datos y ejecución remota de procesos en el servidor, permitiendo, entre otros ataques, la denegación de todo el servicio web, la posibilidad de sustitución total o parcial de los contenidos web en el servidor (*defacement*), o, como resultado de los procesos anteriores, la escalada de privilegios y compromiso de los sistemas accesibles.

A través de las auditorías realizadas se determina la necesidad de verificación de los servicios y aplicaciones web de las diferentes administraciones.

Otra amenaza que se considera crítica es la posibilidad de que un atacante emplee las páginas web legítimas de las diferentes administraciones públicas para infectar a los ciudadanos que las visiten, redirigiendo sus enlaces a páginas web con código dañino.

Por ello, se encuentra en fase de desarrollo un servicio que verifique los enlaces de las diferentes páginas web de las AAPP y que verifique que todas las redirecciones son legítimas.

Es de vital importancia que las diferentes administraciones consideren la evaluación del nivel de seguridad de los servicios electrónicos que proporcionan a los ciudadanos para que estos reúnan las características de confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad esperadas.

Por este motivo, se recomienda la verificación periódica de estos servicios bien por parte del personal responsable de seguridad de los distintos organismos, bien contemplando la contratación de servicios externos independientes que realicen dicha verificación.

Esta acción debe ser complementada con:

- Sistemas de monitorización que detecten los posibles ataques contra los servicios web, entre ellos, se deberían incluir sistemas de detección de intrusiones y sistemas que permitan la correlación de eventos de seguridad que generan actividades no autorizadas en los diferentes elementos de los servicios web.
- Sistemas de protección de perímetro que complementen a la tradicional seguridad perimetral como cortafuegos a nivel aplicación.
- Análisis del código de las diferentes aplicaciones web antes de su paso a producción.

Así pues, desde el CCN se intenta concienciar a las diferentes administraciones para que mejoren la seguridad de los servicios prestados al ciudadano. En este artículo se han apuntado una serie de instrumentos que podrían utilizar los distintos responsables para conseguir dicho objetivo sin merma en la eficacia del servicio ofrecido.

Es de vital importancia que las diferentes administraciones consideren la evaluación del nivel de seguridad de los servicios electrónicos que proporcionan a los ciudadanos