Seguridad en la entrega de aplicaciones

Joaquin Malo de Molina

BDM Security Enterprise

Agenda

GDPR	Fundamentos e implicaciones
ADC	Qué es y que papel cumple
Vulnerabilidades	Definiciones y conceptos básicos
Ataques	Tipos de ataques, efectos. Ejemplo de ataque
WAF	Protección y Mitigación de problemas

GDPR: Principales Cambios & el papel del ADC

- Los cambios se basan en 3 elementos principales:

  I. **Proteger** los datos de las personas, estableciendo un conjunto de derechos de sus propietarios
  II. Implicar y comprometer a los **responsables del tratamiento** de dichos datos
  III. Proporcionar credibilidad a lo dispuesto en el reglamento mediante una **cooperación** reforzada entra las autoridades de las diferentes naciones que puede dar lugar incluso a la adopción de decisiones y sanciones comunes

- Responsabilidad activa → **Orientación hacia la prevención** frente a actuación posterior a la infracción

GDPR: Notificación de Violaciones de Seguridad de Datos

Violaciones de seguridad de los datos: “destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos”.

El responsable debe notificar a la autoridad de protección de datos competente y a los interesados dentro de las 72 horas siguientes a que el responsable tenga constancia.

¿Qué pasa si infringes GDPR?

- Las multas establecida por incumplimiento del nuevo reglamento podrán alcanzar los **20 millones de euros o equivales al 4% de la facturación** global anual de tu empresa.

- **Daño reputacional**

Que es un ADC y como nos ayuda?

¿Qué son las Aplicaciones Web?

las **Aplicaciones Web** son programas informáticos que permiten a los visitantes de un sitio web enviar y recibir datos desde y hacia una base de datos a través de Internet utilizando un navegador web.

- ✓ Disponibilidad
- ✓ Seguridad
- ✓ Integridad de la info
- ✓ Trazabilidad

Vulnerabilidades

Definición

- ✓ **Debilidad en un sistema o aplicación**, que permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones

- ✓ En el contexto de seguridad de la información un **incidente** es un evento que compromete la integridad, confidencialidad o disponibilidad de un **activo de información**. Un activo de información es cualquier activo que contenga información, puede ser desde una hoja de papel hasta una computadora u **aplicación**

- ✓ Es el **resultado de bugs o de fallos en el diseño** del sistema o **aplicación** .

Definición de Ataque:

Consiste en **aprovechar alguna debilidad o vulnerabilidad** en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

Efectos negativos:

- Denegación de servicio
- Ejecutar código arbitrario
- Obtener información confidencial
- Escalar privilegios
- Administrar el sistema
- Tomar el control del mismo
- Detener o dañar el sistema informático

Ataques a Aplicaciones Web:
Fuente más frecuente de fuga de datos

Ataques

Ataques a aplicaciones Web

Según la investigación realizada por Verizon [“2017 Data Breach Investigations Report”], el 88% de los casos de fuga de datos confirmados en el mundo cae dentro de alguno de los siguientes patrones.

TechTarget en Español | Seguridad de datos | Seguridad de la información | Buscar en la red de TechTarget

NOTICIAS

Crecen 35% los ataques sobre aplicaciones web en el primer trimestre del año

por SearchDataCenter en Español

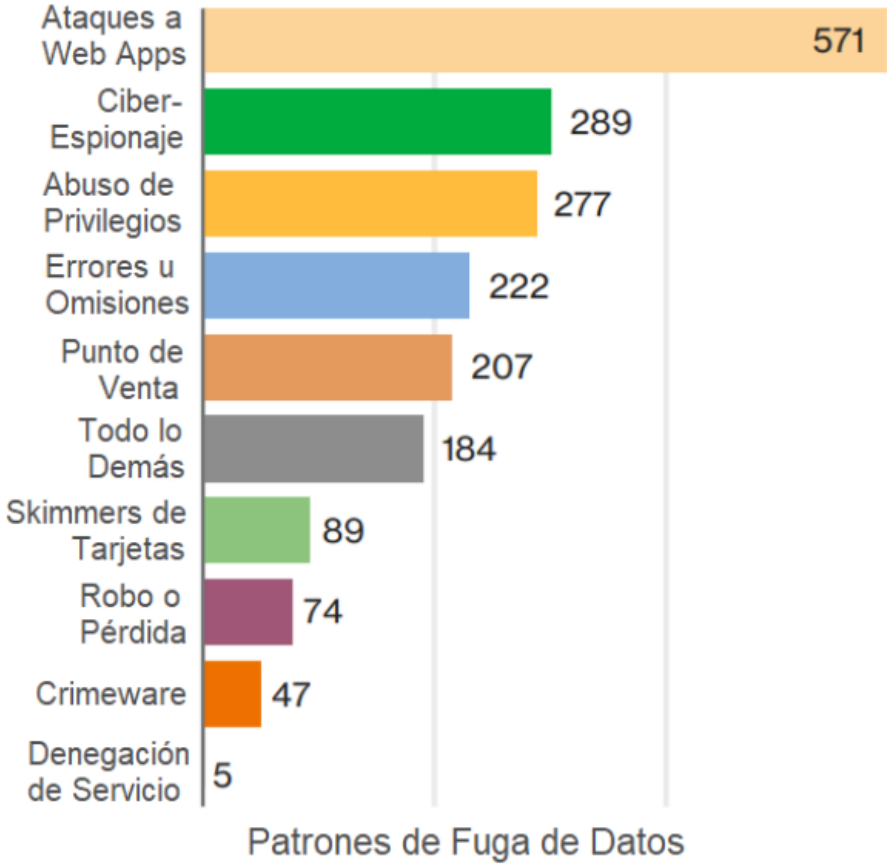
Publicado: 24 may 2017

Además, hay 57% de alza en este tipo de ataques originados desde Estados Unidos, según muestra un estudio de Akamai sobre el estado de internet y la seguridad. El ranking de objetivos lo lideran Estados Unidos, Brasil, Reino Unido y Alemania.

ESTE ARTÍCULO CUBRE
Seguridad de la información
TEMAS RELACIONADOS
Auditoría y cumplimiento
Gestión de la seguridad
Identidad corporativa
Protección de datos

¿BUSCA OTRA COSA?
- Las Olimpiadas de Invierno 2018 en riesgo
- Exploit de día cero en Telegram es una advertencia
- Juegos de Invierno de PyeongChang reciben ciberataques

SI NECESITA AYUDA PARA
Proyectos de virtualización
Aquí reunimos las mejores soluciones de virtualización para sus redes, servidores, escritorios y centros de datos en general
DESCARGA GRATUITA



Patrones de Fuga de Datos

Ataques

Tipos de ataques

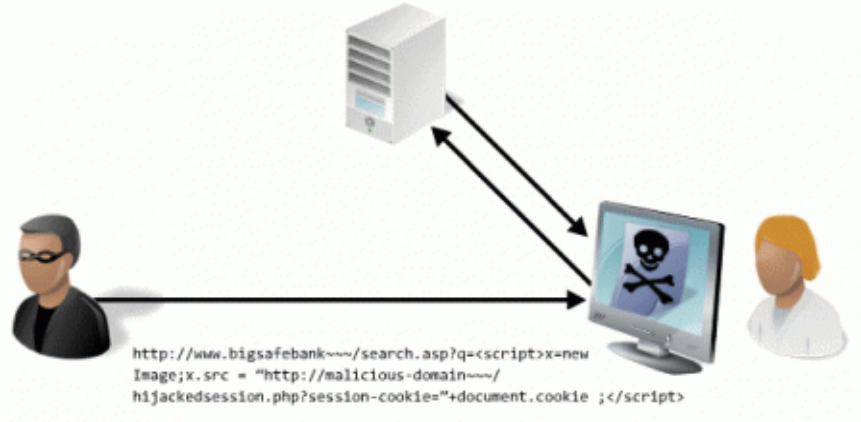
- Ataques de inyección de scripts
  - XSS: Cross Site Scripting
  - ClickJacking
  - CSRF: Cross Site Request Forgery
- Ataques de Path Transversal
- Ataques de inyección de código
  - LDAP Injection
  - Xpath
  - Blind LDAP Injection
- Ataques de inyección de ficheros
  - Remote File Inclusion
  - Local File Inclusion
  - Webtrojans
- Google Haking

Ataques: Inyección de Código

- Un ataque por inyección de código se plantea como **objetivo lograr inyectar** en el contexto de un dominio un código Javascript, Visual Basic Script o simplemente HTML, con la finalidad de engañar al usuario o realizar una acción no deseada suplantándole

- Es una vulnerabilidad que **aprovecha la falta de mecanismos de filtrado y validación en campos de entrada**, permitiendo así el envío de scripts completos (como VBScripts o Java Scripts) con secuencias de comandos maliciosos que podrían impactar directamente en el sitio web o en el equipo de un usuario.

- Esta **limitación se debe a que el código HTML se interpreta en el navegador de un usuario y no en el servidor**. Así que si alguien inyecta código HTML en alguna aplicación web no podría hacer daño alguno al servidor, ya que éste nunca interpreta el código HTML, sólo los navegadores. Por eso este ataque se denomina **ataque del lado del cliente**.



Ataques: XSS

XSS ocurre cuando un atacante es capaz de inyectar un **script**, normalmente **Javascript**, en el ***output*** de una aplicación web de forma que se ejecuta en el **navegador del cliente.** Los ataques se producen principalmente por **validar incorrectamente datos de usuario**, y se suelen inyectar mediante un **formulario web** o mediante un **enlace alterado**.

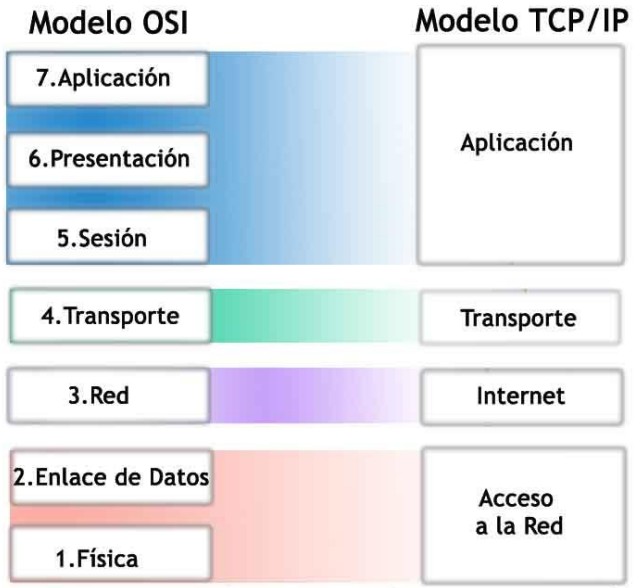
Una página es vulnerable a XSS cuando aquello que nosotros enviamos al servidor (un comentario, un cambio en un perfil, una búsqueda, etc.) se ve posteriormente mostrado en la página de respuesta.

Esto es, cuando escribimos un comentario en una página y podemos leer posteriormente nuestro mensaje, modificamos nuestro perfil de usuario y el resto de usuarios puede verlo o realizamos una búsqueda y se nos muestra un mensaje: “No se han encontrado resultados para <texto>”, se está incluyendo dentro de la página el mismo texto que nosotros hemos introducido.

Ataques de inyección: Ejemplos

- Samy Worm
- Zone-H
- My Space
- Hacker Safe

- Los WAF son un tipo de Firewall que se utilizan para **controlar el acceso a una aplicación o servicio web**.
- A diferencia de un *firewall* tradicional, un IPS o IDS, la ventaja de un **WAF es que opera sobre la capa de aplicación (capa 7 del modelo OSI),** por lo que es posible considerar algunos tipos de protecciones más allá de las tradicionales con los dispositivos mencionados.



Las semejanzas más importantes las encontramos en la capa de Red y de Transporte.

WAF

Cómo funciona un WAF

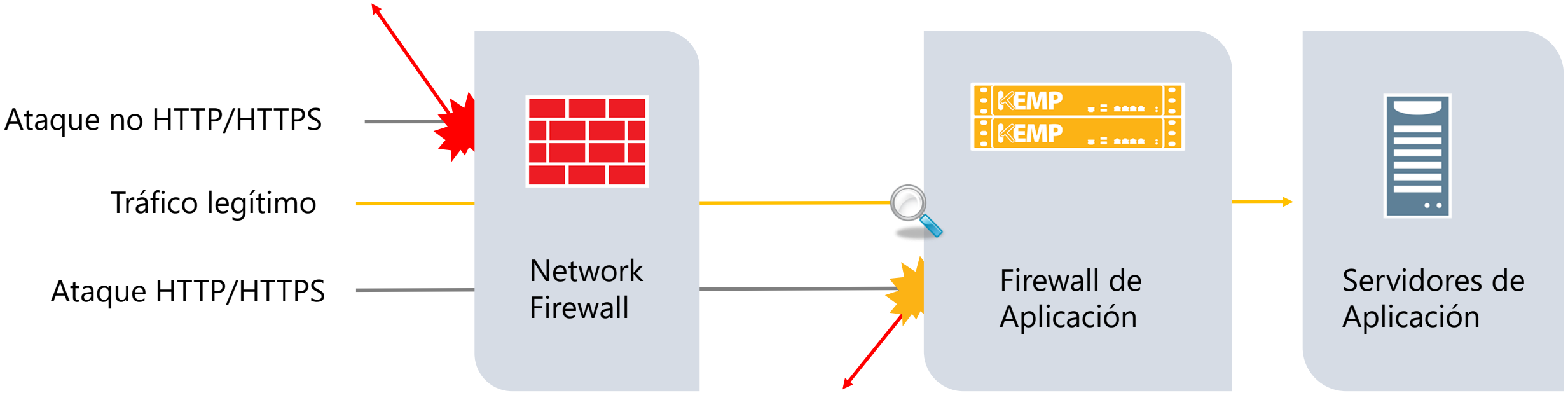
- Se trata de un **dispositivo físico o virtual que analiza el tráfico web** (entre el servidor web y la WAN), los datos recibidos por parte del usuario y protege de diferentes ataques web como: SQL Injection, Cross Site Scripting, Remote and Local File Inclusion, , Buffer Overflows, Cookie Poisoning, etc. Este dispositivo, trata de **proteger de los ataques dirigidos al servidor web** que los IDS/IPS no nos pueden defender

- En general, todas las soluciones WAF funcionan de la misma manera. Básicamente son un muro entre la aplicación de tu sitio web y el visitante que navega por el mismo. El objetivo principal de un WAF es impedir que las solicitudes maliciosas afecten al sitio protegido

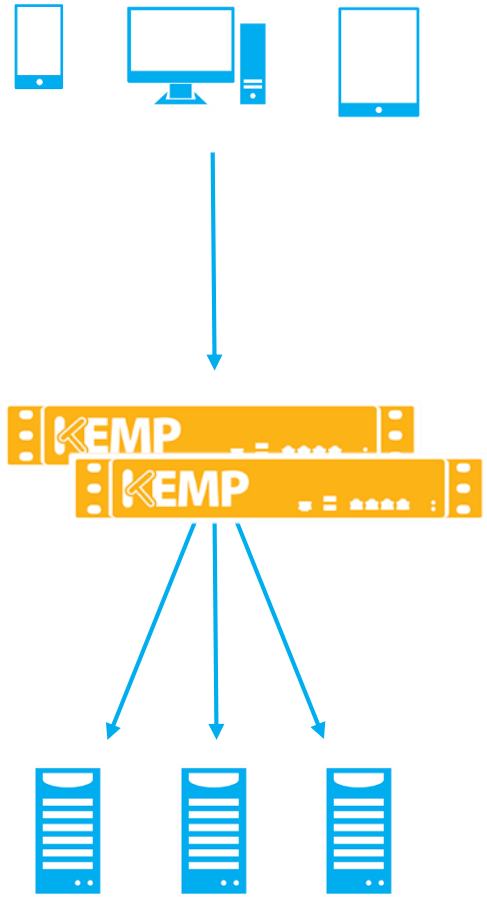
- Los firewalls para aplicaciones van más allá de los metadatos de los paquetes transferidos a nivel de red. Estos se enfocan en los datos en movimiento. Los firewalls para aplicaciones se crearon para comprender el tipo de datos permitidos para cada protocolo, por ejemplo SMTP y HTTP.

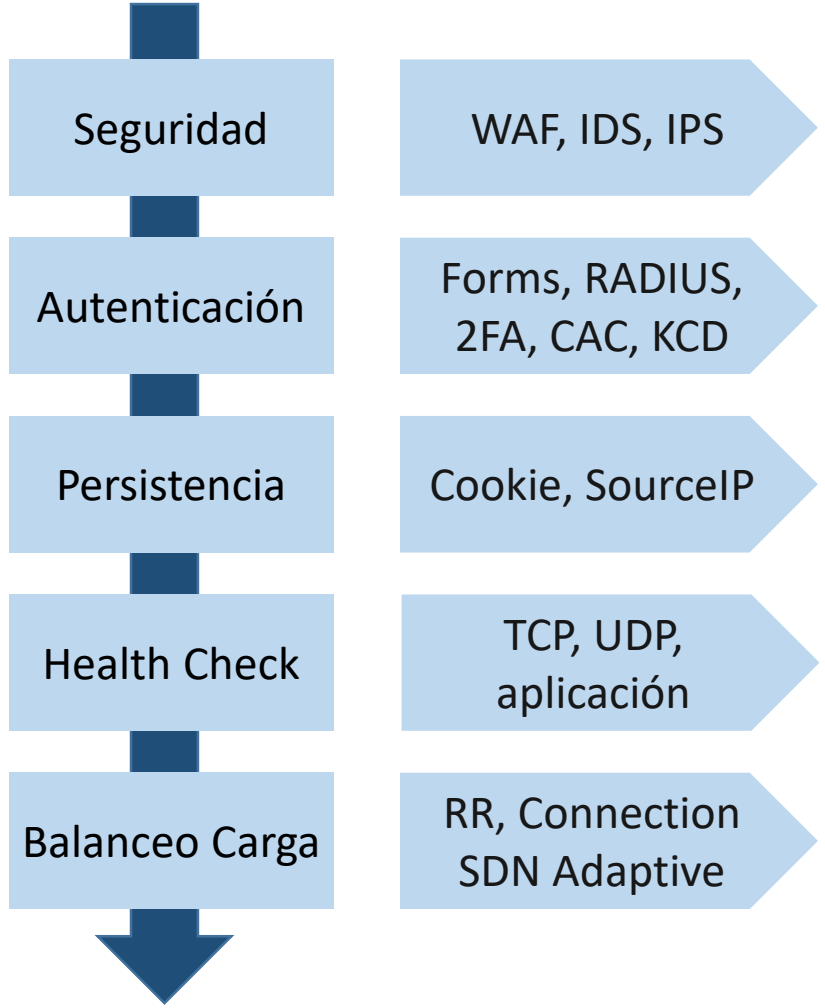
Los firewalls específicos para sitios web se llaman Firewalls para Aplicaciones Web (WAF).

Protección contra ataques Web: WAF



Resumen: Entrega de aplicaciones securizada





Joaquin Malo de Molina
BDM Enterprise Security

nunsys
Tu socio tecnológico

Gracias

IREO

KEMP