GRCbit

Pruebas de Seguridad Aplicaciones y Servicios Web

2020 contacto@grcbit.com

Introducción

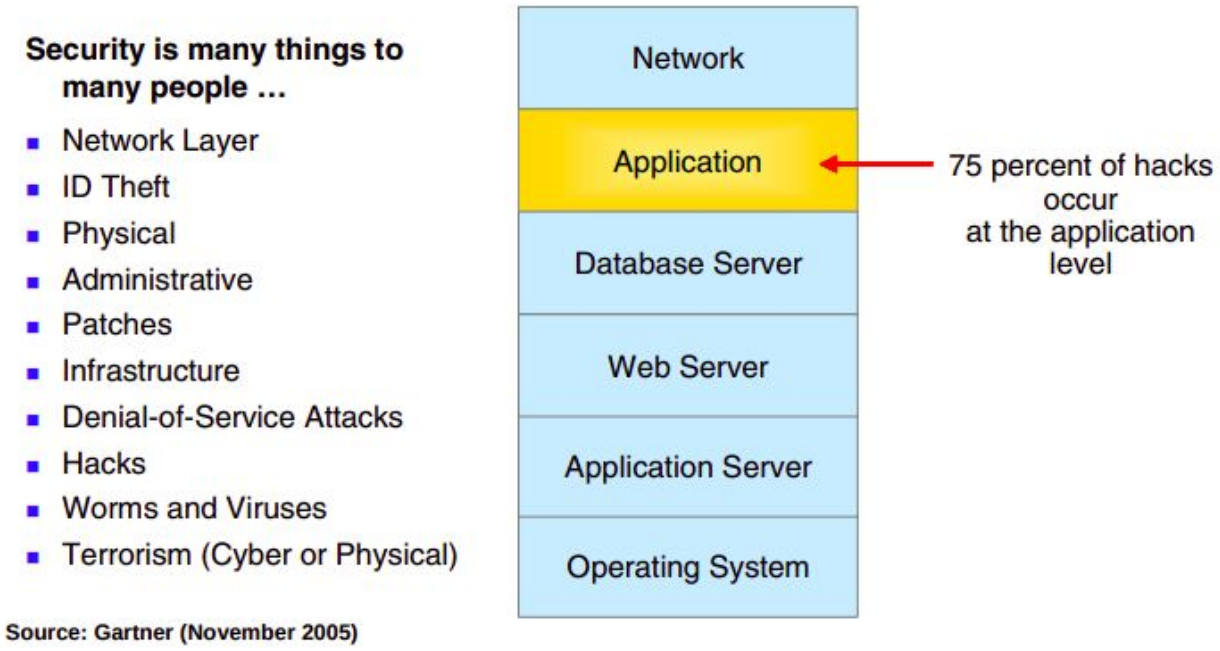
El creciente uso de aplicaciones y servicios Web para soportar negocios, redes sociales, servicios financieros, hacen que las vulnerabilidades en esta capa impacten de manera significativa a los usuarios, negocios y sociedad.

Adicionalmente el uso de nuevas tecnologías (IoT, microservicios, cloud, etc) y uso de metodologías ágiles ó DevOP, hace que la mitigación de riesgos sea más compleja.

Desarrollo

La capa de aplicación es una de las capas más expuesta a ataques, debido a que es accesible a diferentes usuarios, y en algunas ocasiones expuesta a redes públicas.

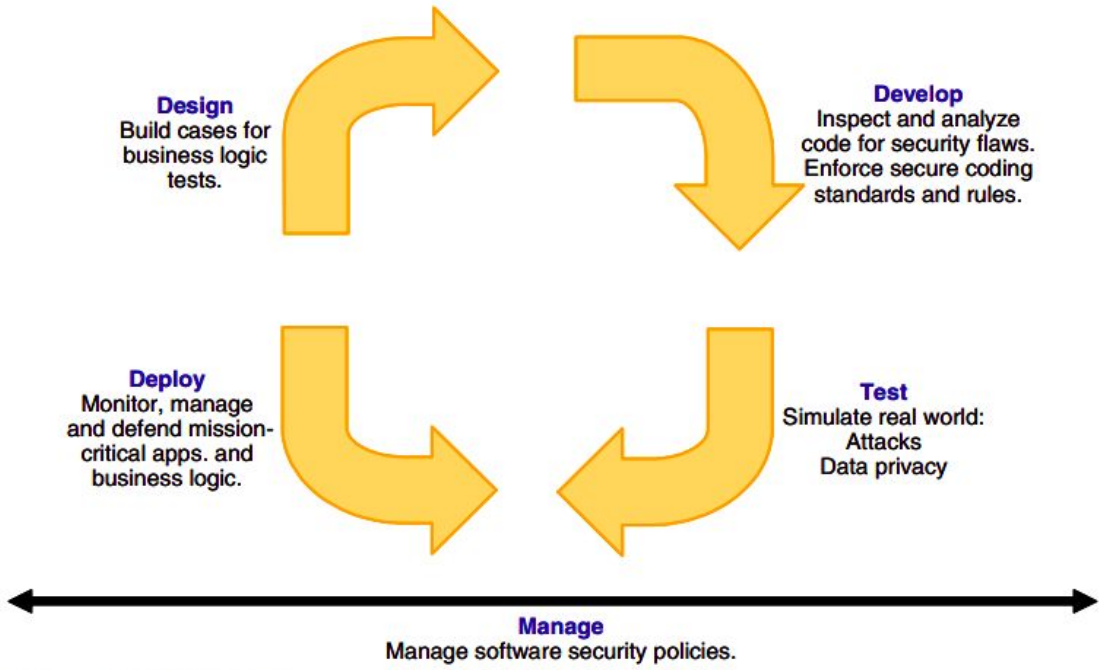
Adicionalmente los cambios constantes sobre la aplicación para soportar nuevos procesos de negocio, hacen de esta capa una de las más vulnerables.



Por lo anterior es importante considerar controles de seguridad en todo el ciclo del desarrollo del software para minimizar los riesgos, acompañando el desarrollo y cada una de sus fases para que la función de seguridad también sea ágil y se ajuste al ciclo de desarrollo.

La validación e implementación de controles de seguridad desde las fases iniciales del ciclo de desarrollo del software hace más eficiente y menos costosa la corrección de errores y vulnerabilidades.

Figure 4. Security in the Application Life Cycle



Source: Gartner (November 2005)

La explotación exitosa de una vulnerabilidad puede afectar no solo la aplicación, si no la infraestructura o la base de datos a la que se conecta, exponiendo información sensible, provocando accesos no autorizados u otro tipo de afectaciones.

Por ello es importante considerar la validación e implementación de controles en cada una de las fases del ciclo de desarrollo del Software, y no solo hasta que la aplicación se encuentra en producción.

¿Cómo podemos ayudarle?

- Ejecutar pruebas de seguridad para cada una de las fases de desarrollo de la aplicación, ajustandonos a la metodología de desarrollo utilizada.
- Ejecutar pruebas de seguridad considerando:
    - El uso de la aplicación y su contexto.
    - Procesos de negocio que soporta.
    - Tipo de datos que almacena, procesa o transmite.
    - Fase del ciclo de desarrollo de la aplicación.

- Diseñar controles de seguridad para mitigar las vulnerabilidades identificadas.
- Realizar análisis de riesgos y modelado de amenazas.
- Evaluar el impacto y probabilidad de cada una de las vulnerabilidades en base a los parámetros de CVSS 3.1.
- Revisar y diseñar una arquitectura de seguridad adecuada.
- Las pruebas ejecutadas se basan en OWASP.
    - Arquitectura, diseño y modelado de amenazas
    - Autenticación, Gestión de sesiones, Control de acceso
    - Manejo de entrada de datos maliciosos
    - Gestión y registro de errores
    - Protección de datos y Comunicaciones
    - Lógica de negocio
    - ...