Cybersecurity

Protection of information, through the treatment of threats that put at risk the information that is processed, stored and transported by the information systems that are interconnected.

Man in the middle

This method only requires the attacker to stand between the two parties trying to communicate.

Ramsomware

Malicious program for computers, which ensures that the device is locked for the user and can only be unlocked again with a key.

Adware

Adware is unwanted software designed to display advertisements on your screen, usually in a browser.

Phishing

Phishing is the crime of tricking people into sharing sensitive information like passwords and credit card numbers.

Doxing

Doxing is revealing identifying information about a person online, such as their real name, home address, place of work, phone number, financial data, and other personal information.

DDos

This type of attack takes advantage of specific capacity limits that apply to any network resource, such as the infrastructure that enables the company's website.

Standardization and reutilization of security functions

Consists on, as the name implies, standardizing various aspects of the security of the apps in order to be reutilized in the future to save time and work.

Secure Development Lifecycle (SDL) is the process of including security artifacts in the **Software Development Lifecycle (SDLC**). SDLC, in turn, consists of a detailed plan that defines the process organizations use to build an application from inception until decommission.

Development teams use different models such as Waterfall, Iterative or Agile.

However, all models usually follow these phases:

1. **Planning and requirements**
2. **Architecture and design**
3. **Test planning**
4. **Coding**
5. **Testing the code and results**
6. **Release and maintenance**

The main benefits of adopting a secure SDLC include:

- **Makes security a continuous concern including all stakeholders in the security considerations**
- **Helps detect flaws early in the development process reducing business risks for the organization**
- **Reduces costs by detecting and resolving issues early in the lifecycle.**

How Does Secure SDLC work?

Most companies will implement a secure SDLC simply by adding security-related activities to their development process already in place.

STRIDE Threat Modelling: It is a model that can be used to prevent any potential and dangerous vulnerabilities, even before a single line of code is written.

S: Spoofing identity, this is when someone pretends to be something or someone other than yourself. It violates the Authentication Property.

T: Tampering with data. It's when information or data is modified, be it on the disk, network, memory, or elsewhere. This violates the Integrity Property.

R: Repudiation. It's when you claim that you didn't do something or were not responsible for a problem, this can either be true or false. This violates the Non-repudiation Property.

I: Information Disclosure. It means to provide information to someone that is not authorized to see said information. This violates the Confidentiality Property.

D: Denial of Service. This means to exhaust all the resources that are needed to provide a certain service. This violates the Availability Property.

E: Elevation of privilege. It's when someone is allowed to do stuff they would normally not be authorized to do. This violates the Authorization Property.

What is the Threat Modeling Tool?

The Threat Modeling Tool enables any developer or software architect to: **Communicate about the security design of their systems. Analyze those designs for potential security issues using a proven methodology.**

La seguridad cibernética

Protección de la información, mediante el tratamiento de amenazas que pongan en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

Hombre en el medio

Este método solo requiere que el atacante se interponga entre las dos partes que intentan comunicarse.

Ramsomware

Programa malicioso para ordenadores, que asegura que el dispositivo está bloqueado para el usuario y solo puede volver a desbloquearse con una llave.

Publicidad

El adware es software no deseado diseñado para mostrar anuncios en su pantalla, generalmente en un navegador.

Suplantación de identidad

El phishing es el delito de engañar a las personas para que compartan información confidencial, como contraseñas y números de tarjetas de crédito.

Doxing

Doxing es revelar información de identificación sobre una persona en línea, como su nombre real, domicilio, lugar de trabajo, número de teléfono, datos financieros y otra información personal.

DDos

Este tipo de ataque aprovecha los límites de capacidad específicos que se aplican a cualquier recurso de red, como la infraestructura que habilita el sitio web de la empresa.

Estandarización y reutilización de funciones de seguridad

Consiste, como su nombre lo indica, en estandarizar varios aspectos de la seguridad de las apps para poder ser reutilizadas en el futuro para ahorrar tiempo y trabajo.

El ciclo de vida de desarrollo seguro (SDL) es el proceso de incluir artefactos de seguridad en **el ciclo de vida de desarrollo de software (SDLC).** SDLC, a su vez, consta de un plan detallado que define el proceso que utilizan las organizaciones para crear una aplicación desde el inicio hasta el desmantelamiento.

Los equipos de desarrollo utilizan diferentes modelos como Waterfall, Iterative o Agile.

No obstante, todos los modelos suelen seguir estas fases:

1. Planificación y requisitos

2. Arquitectura y diseño

3. Planificación de pruebas

4. Codificación

5. Probando el código y los resultados

6. Liberación y mantenimiento

Los principales beneficios de adoptar un SDLC seguro incluyen:

• Hace que la seguridad sea una preocupación continua que incluye a todas las partes interesadas en las consideraciones de seguridad

• Ayuda a detectar fallas en las primeras etapas del proceso de desarrollo, lo que reduce los riesgos comerciales para la organización.

• Reduce los costos al detectar y resolver problemas al principio del ciclo de vida.

¿Cómo funciona el SDLC seguro?

La mayoría de las empresas implementarán un SDLC seguro simplemente agregando actividades relacionadas con la seguridad a su proceso de desarrollo ya implementado.

Modelado de amenazas STRIDE: es un modelo que se puede utilizar para prevenir cualquier vulnerabilidad potencial y peligrosa, incluso antes de que se escriba una sola línea de código.

S: Suplantación de identidad, esto es cuando alguien finge ser algo o

alguien que no seas tú. Viola la propiedad de autenticación.

T: Manipulación de datos. Es cuando se modifica información o datos, ya sea en el disco, red, memoria o cualquier otro lugar. Esto viola la propiedad de integridad.

R: Repudio. Es cuando afirmas que no hiciste algo o que fuiste no es responsable de un problema, esto puede ser verdadero o falso. esto viola la propiedad de no repudio.

I: Divulgación de información. Significa proporcionar información a alguien que está no está autorizado a ver dicha información. Esto viola la Confidencialidad Propiedad.

D: Denegación de Servicio. Esto significa agotar todos los recursos que se necesitan para prestar un determinado servicio. Esto viola la propiedad de disponibilidad.

E: Elevación de privilegio. Es cuando a alguien se le permite hacer cosas que

normalmente no estaría autorizado a hacer. Esto viola la propiedad de autorización.

¿Qué es la herramienta de modelado de amenazas?

La herramienta de modelado de amenazas permite a cualquier desarrollador o arquitecto de software: **Comunicarse sobre el diseño de seguridad de sus sistemas. Analice esos diseños en busca de posibles problemas de seguridad utilizando una metodología comprobada.**