Conceptos básicos de la seguridad informática

Pablo Sanchez Galdamez (21001135)

06/11/22

Contenidos

Glosario

AES Acrónimo en inglés de Advanced Encryption Standard (AES); en español, estándar de cifrado avanzado. Es un algoritmo de cifrado de acceso público basado en clave compartida (Algoritmo criptográfico simétrico), en el que, tanto el tamaño de bloque como el de la clave, son fijos.

Amenaza Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

Análisis de vulnerabilidades Consiste en la búsqueda y documentación de fallos, carencias o debilidades físicas (inundaciones, incendios, controles de acceso...) y lógicas (configuraciones, actualizaciones...) en un sistema informático, que puedan ser empleados por terceros con fines ilícitos, suponiendo un riesgo para la organización y los propios sistemas. El análisis propone vías de mitigación a implementar para subsanar las deficiencias encontradas y evitar ataques a los sistemas informáticos.

Antivirus Software de protección para evitar que ejecutemos algún tipo de software malicioso en nuestro equipo que infecte al equipo.

Backup Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados.

Botnet Una botnet es un conjunto de ordenadores (denominados bots) controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de spam, ataques de DDoS, etc.

Bug Es un error o fallo en un programa de dispositivo o sistema de software que desencadena un resultado indeseado.

Captcha Acrónimo en inglés de Completely Automated Public Turing test to tell Computers and Humans Apart; en español, prueba de Turing completamente automática y pública para diferenciar ordenadores de humanos, es

un tipo de medida de seguridad que consiste en la realización de pruebas desafío-respuesta controladas por máquinas que sirven para determinar cuándo el usuario es un humano o un bot según la respuesta a dicho desafío.

Cifrado Proceso de codificación de información para poder evitar que esta llegue a personas no autorizadas. Solo quien posea la clave podrá acceder al contenido.

Corta Fuegos Sistema de seguridad compuesto o bien de programas (software) o de dispositivos hardware situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios.

Denegación de Servicio Ataque a un sistema, aplicación o dispositivo para dejarlo fuera de servicio debido a una saturación de peticiones.

Doble factor de autenticación Esquema de autenticación básica a la que se añade otro factor como puede ser un código enviado a un móvil, huella dactilar, sistema OTP, etc., más seguro que la autenticación simple

Exploit Secuencia de comandos utilizados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto.

Gusano Es un programa malicioso (o malware) que tiene como característica principal su alto grado de «dispersabilidad», es decir, lo rápidamente que se propaga.

Hacker Persona con grandes conocimientos en el manejo de las tecnologías de la información que investiga un sistema informático para reportar fallos de seguridad y desarrollar técnicas que previenen accesos no autorizados.

Hash Operación criptográfica que genera identificadores alfanuméricos, únicos e irrepetibles a partir de los datos introducidos inicialmente en la función. Los hashes son una pieza clave para certificar la autenticidad de los datos, almacenar de forma segura contraseñas o firmar documentos electrónicos, entre otras acciones.

Ingeniería social Conjunto de técnicas que los delincuentes usan para engañar a los usuarios de sistemas/servicios TIC para que les faciliten datos que les aporten valor, ya sean credenciales, información sobre los sistemas, servicios instalados etc.

Keylogger Es un tipo de spyware que se encarga de monitorizar toda la actividad realizada con el teclado (teclas que se pulsan) para luego enviarla al ciberdelincuente

Malware Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra

que nace de la unión de los términos en inglés de software malintencionado: malicious software.

Pentest Una prueba de penetración es un ataque a un sistema software o hardware con el objetivo de encontrar vulnerabilidades. El ataque implica un análisis activo de cualquier vulnerabilidad potencial, configuraciones deficientes o inadecuadas, tanto de hardware como de software, o deficiencias operativas en las medidas de seguridad.

Phishing Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo.

Ransomware Malware cuya funcionalidad es «secuestrar» un dispositivo (en sus inicios) o la información que contiene de forma que si la víctima no paga el rescate, no podrá acceder a ella.

Troyano Malware diseñado para tener múltiples utilidades, la más común es crear una puerta trasera en el equipo infectado, para poder descargar actualizaciones y nuevas funcionalidades. Esta diseñado para ser controlado desde un centro de comando y control (C&C). Como funcionalidades habituales encontramos: keylogger, escaneo de redes locales buscando otros equipos para infectar, envío de correos, robo de datos/ficheros, minado de cryptomonedas, descarga de otros malwares como ransomware.

XSS Se trata de una vulnerabilidad existente en algunas páginas web generadas dinámicamente (en función de los datos de entrada). XSS viene del acrónimo en inglés de Secuencias de comandos en sitios cruzados (Cross-site Scripting).

Investigación de Ataque

Consideraremos el ataque **Wannacry** del 2017.

Linea del tiempo

- **Viernes 12 de Mayo:** La empresa española *Telefónica* sufre el inicio del ataque. Este se fue expandiendo sin control, llegando a afectar al menos 16 hospitales en el Reino Unido, y a la empresa FedEx en Estados Unidos.
- **Sábado 13 de Mayo:** El fabricante de vehículos francés Renault, la japonesa Nissan y el Ministerio de Interior ruso se vieron afectados por el virus. Microsoft, en una maniobra inaudita, decidió publicar un parche para solventar la vulnerabilidad en Samba para sistemas operativos ya no soportados como Windows XP.
- **Domingo 14 de Mayo:** Brad Smith, presidente de Microsoft, dijo que el ataque da un ejemplo más de por qué es un problema que los gobiernos almacenen vulnerabilidades de software para sus propios intereses. Llamó a la cooperación entre empresas, consumidores y gobiernos. Señaló claramente a la NSA como uno de los responsables del desastre.
- **Lunes 15 de Mayo:** China descubrió una nueva versión del virus que se ha saltado las medidas de seguridad implantadas tras el primer ataque. Europol aumentó el número de víctimas hasta los 230.000 en 179 países.

Consecuencias del ataque

El ataque de ransomware WannaCry afectó aproximadamente a 230.000 ordenadores en todo el mundo.

Un tercio de las fundaciones hospitalarias del NHS se vieron afectadas por el ataque. Se informó a las ambulancias de que cambiaran de ruta, lo que dejó a muchísimas personas necesitadas de atención urgente en la estacada. Se estimó que el ataque costó al NHS la escalofriante cantidad de 92 millones de libras, ya que 19.000 citas se cancelaron como resultado del ataque.

El ransomware se extendió más allá de Europa, y se paralizaron los sistemas informáticos de 150 países. El ataque de ransomware WannaCry tuvo un impacto

financiero significativo en todo el mundo. Se estima que este cibercrimen provocó pérdidas por valor de 4.000 millones de dólares en todo el mundo.

Referencias

Glosario

Basado en el glosario del `incibe`: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Investigación de Ataque

Cronología tomada de un blog en `genbeta`: https://www.genbeta.com/a-fondo/cronologia-de-wannacry-asi-se-expandio-el-virus-que-paralizo-a-medio-mundo

Consecuencias tomadas de el articulo de `kaspersky`: https://www.kaspersky.es/resource-center/threats/ransomware-wannacry