Ciberseguridad:
Amenazas y vulneravilidades en la red

Carlos Yanguas Durán, Alberto Larena Luengo, David Márquez Mínguez

31 de Diciembre de 2020

Resumen

Aqui va el resumen

Índice general

Índice de figuras

Capítulo 1

Introducción

El término "Ciberseguridad" suele ser una expresión ampliamente utilizada por la sociedad, no solo en el ámbito informático, sino en muchas otras disciplinas no relacionadas con la tecnología. En la mayoría de los casos la palabra Ciberseguridad se suele emplear de forma errónea pensando que el termino funciona como símil de seguridad de la información, seguridad en computo o seguridad informática, pero esta idea no es del todo correcta.

Si bien es cierto que en la lengua española no existe una definición oficial para la palabra Ciberseguridad, podemos tomar la definición de profesionales del sector. Según ISACA (Information Systems Audit and Control Association) la Ciberseguridad se define como:

"Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" [6].

Como ya se ha afirmado antes, la Ciberseguridad no solo aplica al ámbito informatico, también se incluyen dentro de Ciberseguridad aquellas actividades orientadas a responder a determinadas amenazas, que usando la tecnología e Internet como medio, puedan verse tremendamente amplificadas. Podemos afirmar que cuando hablamos de Ciberseguridad estamos hablando de amenazas, de entender lo que está sucediendo, quién está detrás y por qué. En este documento nos centraremos fundamentalmente en la tecnología como medio en la amenaza, pero aportaremos otras perspectivas a la hora de ofrecer respuestas. .

Capítulo 2

Vulnerabilidades y ataques en los sistemas informáticos

Una vulnerabilidad en términos informáticos es una debilidad o fallo en un sistema de información, como puede ser una aplicación o un servicio web, que permite a un atacante comprometer la integridad (capacidad que tiene un sistema de información para garantizar que los datos no han sido modificados desde su creación sin autorización, asegurando que la información es válida y consistente), disponibilidad (capacidad de un sistema de información para garantizar que el este no va a sufrir caídas y que por tanto, el sistema y los datos van a estar disponibles al usuario en todo momento.) o confidencialidad (capacidad de un sistema de información de garantizar que la información almacenada o transmitida por la red, solamente va a estar disponibles para aquellas personas autorizadas a la misma.).[8],[9]

2.0.1 Vulnerabilidades y ataques más recurrentes:

1. **Vulnerabilidad Zero Day:** son aquellas vulnerabilidades que acaban de ser descubiertas, y que por tanto, no tienen un parche que las solucione. El principal problema de este tipo de vulnerabilidades es que desde que se descubre hasta que se lanza un parche correctivo y los usuarios lo instalan en sus equipos, los atacantes tienen vía libre para explotarla y sacar provecho de esta. Existen varios ejemplos de este tipo de vulnerabilidad, por ejemplo el ransomware(programa de software malicioso que llega a bloquear la pantalla de una computadora o cifrar archivos importantes con contraseña, tiene como objetivo el exigir un pago para restablecer el funcionamiento del sistema que contiene el mismo.) que afectó a multitud de equipos a partir del 2017. Algunas empresas importantes, para tratar de evitar este tipo de vulnerabilidades que suelen producirse a menudo en software recientemente desarrollado, es hacer concursos invitando a grandes expertos en ciberseguridad, ofreciendo grandes recompensas a aquellos que descubran y resuelvan posibles vulnerabilidades que tenga dicho software.

2. **Error en la gestión de recursos:** Este tipo de vulnerabilidad ocurre cuando no se tiene un control acerca de la gestión de recursos que puede utilizar un sistema de información, permitiendo que este consuma un exceso de recursos afectando a la disponibilidad de estos.

Un ejemplo típico de explotación de esta vulnerabilidad es el exigir constantemente recursos del sistema de información, cediendo la mayoría de estos a un único usuario, ralentizando o impidiendo el uso de esta al resto de usuarios.

3. **Validación de entrada:** Esta vulnerabilidad ocurre cuando no se tiene un control acerca de los datos que pueden entrar en el sistema de información. Entre los ataques que explotan esta vulnerabilidades nos encontramos con los ya conocidos SQL injection, que consiste en insertar código SQL malicioso en la base de datos de la víctima forzando a la base de datos a ejecutar dicha sentencia. Entre los daños principales que pueden llegar a causar este tipo de ataques nos encontramos con la destrucción de tablas o la extracción de información privada como contraseñas.

4. **Permisos, privilegios y/o control de acceso:** Esta vulnerabilidad ocurre cuando no se tiene un control acerca de los privilegios o permisos que se les dan a los usuarios. En varias ocasiones, las empresas han sufrido ataques ayudados o llevados a cabo por sus propios empleados causados de manera consentida o no. Si se les dan permisos a todos los empleados de la empresa por igual, podría ocurrir que algún empleado realizase acciones que causasen grandes daños irreversibles para la misma. Por ejemplo, algún empleado trabajando en bases de datos, podría sin querer eliminar algunos datos relevantes para la misma al introducir mal alguna instrucción. También ocurre frecuentemente que no todas las partes del sistema de información tienen el mismo nivel de ciberseguridad, por tanto, si se distribuye por igual los permisos o privilegios entre las diferentes partes de esta, será atacada por el punto más vulnerable.

5. **Vulnerabilidad de Cross Site Scripting(XSS):** Esta vulnerabilidad sucede cuando es posible ejecutar scripts de lenguajes como JavaScript. Consiste en la suplantación de un sitio web verdadero por otro que no lo es, pero que a nivel visual es idéntico al original. El ataque más conocido que aprovecha esta vulnerabilidad es el denominado Phising, que consiste en la obtención de los datos de los usuarios introducidos por ellos mismos. Un ejemplo frecuente de este tipo de ataques, se da a través de los emails, al usuario le llega un correo con una URL[5] que tiene un nombre semejante al nombre de su banco, el usuario al abrir el link se encuentra con un aspecto idéntico al de su banco habitual, por lo que introduce los datos, seguidamente estos datos son almacenados por el creador de dicho ataque y le redirige a la página web oficial introduciéndole los datos aportados por el usuario, de esta manera el usuario no sospecha que pueda ser algún tipo de ataque, ya que todo parece haber resultado con normalidad.

2.0.2 Clasificación de vulnerabilidades según gravedad y dificultad de tratamiento:

1. **Gravedad baja:** Representa aquellas vulnerabilidades que tienen un impacto mínimo y que no presentan problemas para reducir este. En muchas ocasiones este tipo de vulnerabilidades no son tratadas, ya que puede ocurrir que implantar el sistema de seguridad para cubrir las mismas, sea más caro que cubrir las consecuencias de los ataques producidos por esta.

2. **Gravedad media:** En este nivel se incluyen aquellas vulnerabilidades que son fáciles de solucionar pero que representan un impacto medio, normalmente pueden ser eliminadas mediante auditorías o configuraciones que se han establecido previamente en otros sistemas.

3. **Gravedad de gran importancia:** En este grupo se incluyen aquellas vulnerabilidades que pueden ser explotadas produciendo un ataque rápido y de gran impacto sobre el sistema informático, normalmente este tipo de ataques tienen como objetivo buscar la pérdida de confidencialidad e integridad de los datos o recursos, además no suelen tener una solución previamente implantada.

4. **Gravedad crítica:** Es el grupo de vulnerabilidades que conllevan mayores consecuencias al sistema. El ataque sobre este tipo de vulnerabilidad conlleva normalmente problemas no solo para el equipo a través del cual se descubre la vulnerabilidad, sino que lo expande por toda la red al que está conectado. Son ataques difíciles de detectar y que además, no necesitan que el usuario lleve a cabo algún tipo de acción para poder cumplir con su objetivo.

Este tipo de vulnerabilidades son imprescindibles que sean cubiertas por el equipo de ciberseguridad.

Como conclusión sobre este tema, es importante destacar, que los ordenadores personales normalmente no sufren ataques pese a tener algún tipo de vulnerabilidad, ya que resulta complicado obtener información lo suficientemente valiosa como para pedir un rescate por el mismo, o este no puede ser igual de cuantioso que el exigido a una empresa, por lo que en la mayoría de los casos es suficiente con tener las actualizaciones del sistema operativo y del antivirus al día para hacer frente a los más habituales. En el caso de las empresas, sin embargo, es común tener un área destinada específicamente destinada a la ciberseguridad, ya que se tratan con datos sensibles(Son aquellos datos que están sujetos a condiciones de tratamiento específicas dictadas por el RGPD) de gran valor.

Capítulo 3

Sistemas de riesgo

> Para determinar si un sistema informático es de riesgo, es necesario llevar a cabo un análisis de riesgo. El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.[10]

Según el BS ISO/IEC 27001:2005, la evaluación de riesgo incluye las siguientes actividades y acciones:

1. **Identificación de los activos:** Este proceso busca identificar los activos de la empresa.
2. **Identificación de los requisitos legales y de negocio que son relevantes para la identificación de los activos:** Este paso recoge la información acerca de la normativa que debe cumplimentar la empresa para llevar su actividad acabo, normalmente se encuentran recogidos en artículos como el BOE.
3. **Valoración de los activos identificados, teniendo en cuenta los requisitos legales y de negocio identificados anteriormente, y el impacto de una pérdida de confidencialidad, integridad y disponibilidad.**
4. **Evaluación del riesgo, de las amenazas y las vulnerabilidades a ocurrir.**
5. **Cálculo del riesgo.**
6. **Evaluación de los riesgos frente a una escala de riesgo preestablecidos.**

A través de este análisis intentamos gestionar los posibles riesgos potenciales para prevenir este tipo de situaciones negativas para la actividad empresarial, recogiendo los factores fundamentales para su consecución en diferentes documentos según la metodología aplicada, que dependerá fundamentalmente de la actividad de la empresa: No se describen los pasos de las metodologías nombradas, ya que todas ellas cumplen con las exigencias de BS ISO/IEC 27001:2005 (descritas al comienzo del punto 3), y por tanto son semejantes, en vez de eso se mostrarán las

metodologías existentes más importantes según la actividad de la empresa o por su característica más llamativa.

3.0.1 Metodologías principales para la evaluación de riesgos:

1. **ARLI-CIB:** Esta metodología está destinadas a empresas del sector industrial.
2. **MAGERIT:** Esta metodología está enfocada a empresas con grandes sistemas de información.
3. **OCTAVE:** Esta metodología está enfocada hacía empresas con grandes infraestructuras TI al igual que MAGERIT.
4. **Citicus One:** Brinda un enfoque para administrar el riesgo de la información, el riesgo del proveedor y otras áreas clave de riesgo operacional en toda la empresa.
5. **COBIT 5:** Es un marco mundialmente aceptado para la gestión de TI, alinea las metas de negocio con los procesos y metas TI proporcionando herramientas, recursos y orientación para lograr, identificar y asociar las responsabilidades de los procesos empresariales.
6. **CRAMM:** Esta metodología se considera mixta, ya que hace un análisis cualitativo y cuantitativo del análisis de riesgo.

3.0.2 Herramientas para la evaluación de riesgos:

Las herramientas que se muestran a continuación sirven de apoyo a las metodologías para la consecución de su objetivo.

1. **Matriz de riesgo:** Su función más importante es mostrar de manera resumida los riesgos, su probabilidad y sus posibles soluciones de manera visual en una tabla, esta herramienta no se encarga de obtener estos datos, solo mostrarlos de manera gráfica. El objetivo de esta matriz es obtener una idea general de los riesgos de la empresa y la posibilidad de que estos ocurran de manera visual.
   Se muestra un ejemplo de esta herramienta en 3.1

RIESGO	PROBABILIDAD	IMPACTO	POSIBLE SOLUCIÓN	NOTA CUALITATIVA DEL RIESGO
Rotura del servidor	baja	alta	mantenimiento	media
Fuga de desarrolladores	media	alta	aumento salarial	media
Ransomware en equipo	baja	media	actualización de antivirus	baja

Figura 3.1: Matriz de riesgo.

2. **Check-lists:** Es una técnica que permite identificar los riesgos de una manera simple, proporcionando una lista de incertidumbres típicas a considerar.
3. **SWIFT:** Al igual que check-lists, sirve para identificar riesgos.

4. **Análisis de árbol de fallas:** Esta técnica se inicia viendo cómo se comporta algunos de los recursos del sistema de información ante un evento no deseado, y determina todas las maneras en las que este podría ocurrir, se representa gráficamente en un diagrama de árbol lógico.
   Se muestra un ejemplo de esta herramienta en Figura 3.2 [11].

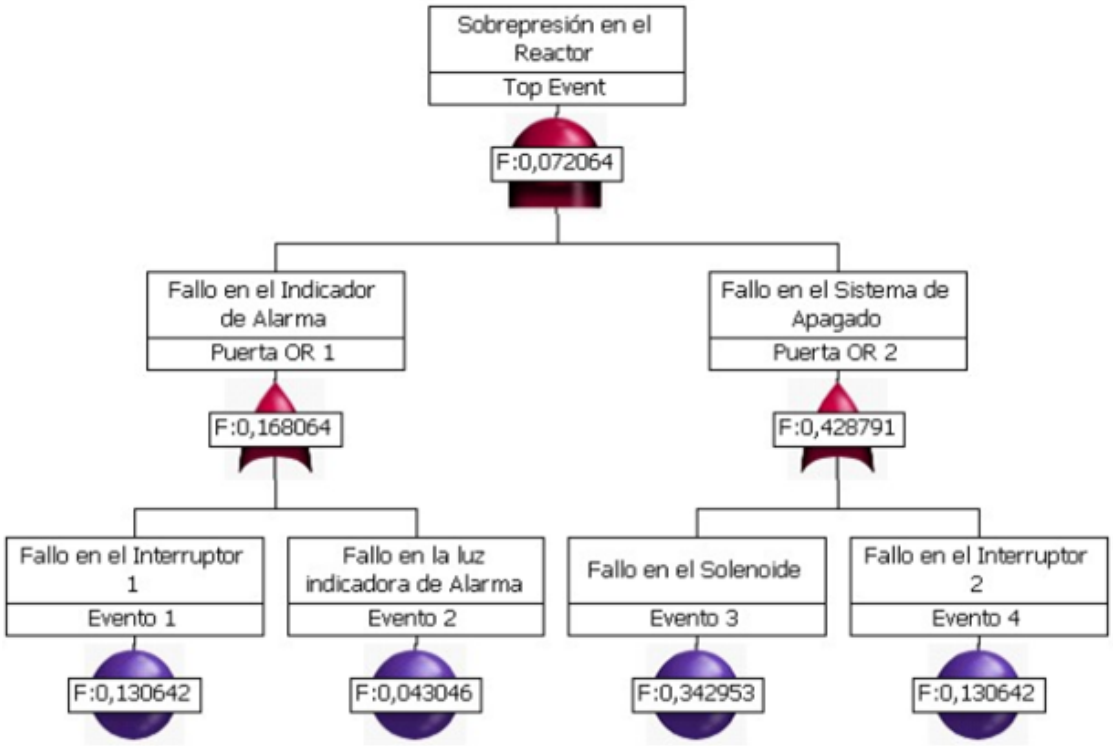

Figura 3.2: Diagrama árbol de fallas.

5. **Diagrama causa-efecto:** Esta herramienta permite conocer la raíz de un problema y cuellos de botella en procesos. Se representa mediante un diagrama denominado espina de pescado.
   Se muestra un ejemplo de esta herramienta en Figura 3.3 [12].

6. **AMFE:** Esta técnica identifica y analiza los fallos potenciales, mecanismos y los efectos de esos fallos.
   Se muestra un ejemplo de esta herramienta en Figura 3.4 [13].

7. **HAZOP:** Esta herramienta tiene como objetivo detectar situaciones de inseguridad en plantas industriales, debido a la operación o a los procesos productivos.
   Se muestra un ejemplo de esta herramienta en Figura 3.5 [14].

8. **LOPA:** Permite la evaluación de controles, así como la determinación de su eficacia.
   Se muestra un ejemplo de esta herramienta en Figura 3.6 [15].

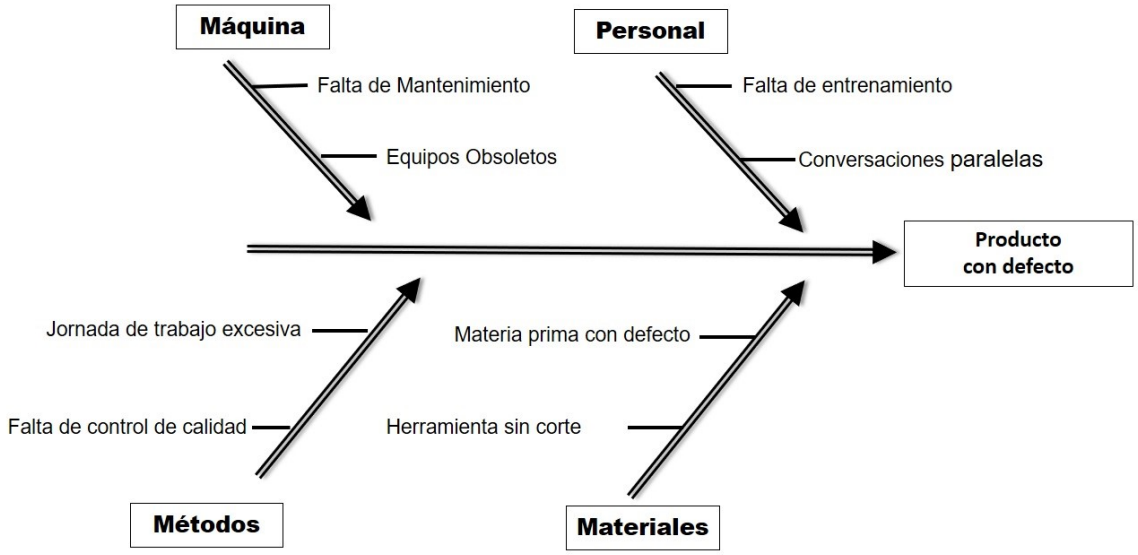

Figura 3.3: Diagrama causa-efecto.

AMFE: ANÁLISIS MODAL DE FALLOS Y EFECTOS POTENCIALES (PROCESO)																
Nombre del proceso: Ensamble de componentes			Proveedor del material: Empresa ABC						Nombre y firma:							
Producto: Silla modelo TL-65			Fecha de fabricación:						Supervisor:							
Fecha AMFE Inicial: 02/05/2017			Fecha AMFE última revisión: 15/05/2017													
			Condiciones Existentes								Resultados					
Modos de fallo	Efecto potencial del fallo	Causa potencial del fallo	Controles actuales	O	G	D	Índice prieoritario del riesgo (NPR)	Estado y acción recomendados	Área responsable acción correctora	Acción correctora	O	G	D	Índice prieoritario del riesgo (NPR)		
Falta de soldadura	Rebajos, ruidos y falta de rigidez	Defectos de acoplamiento	Ninguno	8	8	2	128	Control	Fabricación	Previstos grupos de aprietes en la zona	6	8	2	96		
		Pestañas fuera de geometría	Ninguno	6	8	2	96	Rediseño	Diseño	Pestañas bien diseñadas para la geometría	3	6	2	36		
Soldadura defectuosa	Agujeros en la chapa	Desacoplamiento de chapas	Ninguno	8	8	2	128	Rediseño	Diseño	Garantizar acoplamientos	6	8	2	96		
	Mala ejecución de la soldadura	Falta capacitación soldadores	Ninguno	8	8	4	256	Formación	RR.HH y supervisor	Formación y supervisión a los soldadores	5	6	3	90		
Adriana Gómez Villoldo										http://asesordecalidad.blogspot.com						

Figura 3.4: AMFE.jpg

PALABRA GUÍA	SIGNIFICADO	EJEMPLO DE DESVIACIÓN	EJEMPLO DE CAUSAS ORIGINADORAS
NO	Ausencia de la variable a la cual se aplica	No hay flujo en una línea	Bloqueo; fallo de bombeo; válvula cerrada o atascada; fuga, válvula abierta, fallo de control.
MAS	Aumento cuantitativo de una variable	Más flujo (más caudal)	Presión de descarga reducida, succión presurizada, fuga, lectura errónea de instrumentos.
		Más temperatura	Fuegos exteriores, bloqueo, explosión en reactor, reacción descontrolada
MENOS	Disminución cuantitativa de una variable	Menos caudal	Fallo de bombeo, fuga, bloqueo parcial, sedimentos en línea, bloqueo de válvulas.
		Menos temperatura	Pérdidas de calor, vaporización, fallo de sellado.
INVERSO	Analiza la inversión en el sentido de la variable. Se obtiene el efecto contrario al que se pretende.	Flujo inverso	Fallo de bomba, sifón hacia atrás, inversión de bombeo, válvula antirretorno que falla o está insertada en la tubería en forma incorrecta.
ADEMÁS DE	Aumento cualitativo. Se obtiene algo más que las intensiones de diseño	Impurezas o una fase extraordinaria	Entrada de contaminantes del exterior como aire, agua o aceites, productos de corrosión, fallo de aislamiento, presencia de materiales por fugas interiores, fallos de la puesta en marcha.
PARTE DE	Disminución cualitativa. Se obtiene solamente una parte de las intensiones del diseño.	Disminución de la composición en una mezcla	Concentración demasiado baja en la mezcla, reacciones adicionales, cambio en la alimentación
DIFERENTE DE	Actividades distintas respecto a la operación normal	Cualquier actividad	Puesta en marcha y parada, pruebas e inspecciones, muestreo, mantenimiento, eliminación de tapones, corrosión, fallo de energía, emisiones indeseadas, etc.

Figura 3.5: HAZOP.

Initiating Cause	Likelihood, events/yr	Likelihood, 10^{-x}
Control Loop Failure	1/10	10^{-1}
Seal Failure	1/10	10^{-1}
Gasket Failure	1/100	10^{-2}
Rotating Equip Trip	1/1	10^{0}
Fixed Equip Failure	1/100	10^{-2}
Loss of Power	1/10	10^{-1}
Utility Failure	1/10	10^{-1}

Table 1: Initiating Event Frequencies Example

Figura 3.6: LOPA.

Capítulo 4

Ciberataques y sus consecuencias

Antes de conocer los distintos tipos de ciberataques y las consecuencias de los mismos, debemos definir que es un ciberataque. La Real Academia de la Ingeniería define ciberataque como:

"Forma de ciberguerra o ciberterrorismo donde, combinado con ataque físico o no, se intenta impedir el empleo de los sistemas de información del adversario o el acceso a la misma."[16].

Estos ciberataques aprovechan alguna de las vulnerabilidades ya comentadas en el capítulo 2, para robar o destruir no solo datos empresariales fundamentales, sino comprometer sitios web e interrumpir estructuras operativas, así como el robo de identidad de personas.

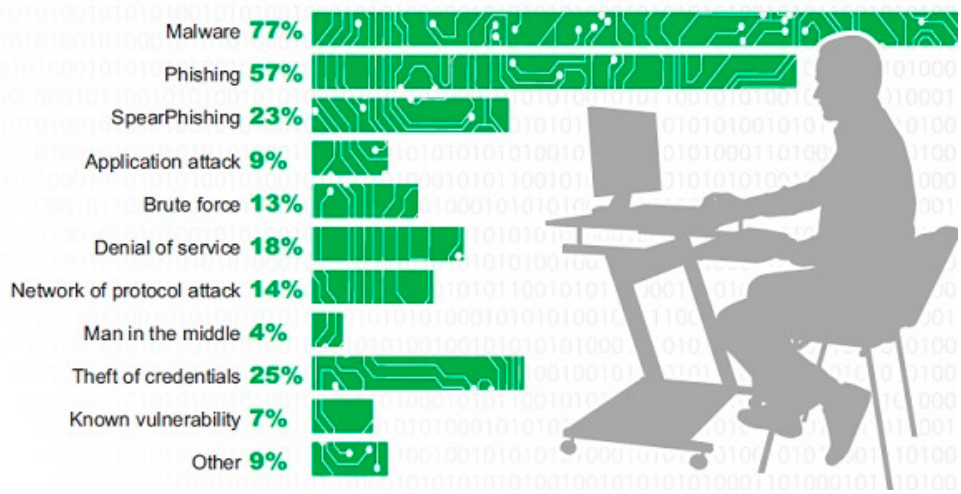

Figura 4.1: Ciberataques mas comunes [1]

Tanto si el motivo es el espionaje como el sabotaje, los ciberdelincuentes emplean distintos métodos de ataque, algunos de ellos son el "spear-phishing", el ataque de inyección SQL, el filtro de scripts de sitios (XSS), los ataques de fuerza bruta... Una de las tácticas más perturbadora utilizada en los ciberataques es el ataque distribuido de denegación del servicio (DDoS), en el que se utilizan bots infectados para congestionar un sitio web o una aplicación web hasta el punto de que los usuarios legítimos no pueden acceder a él, algo que cuesta a las empresas millones de dólares en ingresos, pérdida de productividad y daños en la reputación. En este capitulo se mencionan algunos de los ciberataques mas conocidos, así como su funcionamiento y las consecuencias del mismo.

4.1 Software malicioso: Malware

La palabra malware viene del inglés, y es el resultado de la unión de las palabras malicious software(software malicioso). Se trata de un tipo de software o de aplicación que tiene como objetivo hacer daño al dispositivo en el que se ha conseguido alojar, instalar o infiltrar, ya sea un ordenador, un teléfono móvil... Existen muchos tipos de malware, los troyanos, los gusanos, el spyware, el ransomware. Sin embargo, malware es el término principal que se emplea para hablar de todas esas amenazas informáticas. La forma de actuar de cada uno suele ser diferente, pero en común tienen el objetivo de dañar el equipo o a su usuario. A continuación, se enumeran los tipos de malware más conocidos:

1. **Virus informático:** Este es un tipo de malware cuyo objetivo es alterar el correcto funcionamiento de un dispositivo. Un virus necesita ser ejecutado por el usuario pensando que es una aplicación legítima, y una vez lo hace, puede replicarse e infectar el equipo.

2. **Gusano informático:** A diferencia del virus informático, este malware no necesita de la intervención del usuario ni modificar ningún archivo existente. Se suelen utilizar para crear redes de ordenadores "zombies" que pueden actuar de forma simultánea para enviar SPAM de forma masiva, difundir malware o lanzar diferentes tipos de ataques informáticos.

3. **Troyano:** Este malware se oculta dentro de un programa legítimo o se disfraza de él para introducirse en un equipo como si de un Caballo de Troya se tratase. Mientras que un virus suele ser destructivo, un troyano trata de pasar desapercibido mientras accede a tu dispositivo con la intención de ejecutar acciones ocultas.

4. **Spyware:** Al igual que el troyano, spyware se instala en el equipo mediante la interacción de una segunda aplicación que lo lanza, trabaja en segundo plano intentando no ser detectado para recolectar información sobre el usuario u organización dueña de un ordenador de forma no autorizada.

5. **Ransomware:** Se trata de un tipo de malware que secuestra los datos de cualquier dispositivo electrónico, bloqueándolos y pidiendo un rescate económico a cambio de recuperarlos.

4.2 Phishing y Spear-phishing

El principio del phishing es relativamente sencillo, los estafadores crean correos electrónicos, páginas web e incluso mensajes cortos de carácter falso que solicitan información de inicio de sesión de los usuarios. Es así como los estafadores se hacen con los datos de acceso para tiendas online, redes sociales, espacios de almacenamiento en la nube y en el peor de los casos, se hacen incluso con información bancaria o datos de la tarjeta de crédito. De esta forma, con una página web de phishing sencilla se pueden obtener datos sensibles, información que tiene un alto valor económico en el mercado negro digital.

A partir de los correos electrónicos, los ciberdelincuentes acaban consiguiendo datos de acceso y contraseñas. No obstante, hoy en día, las probabilidades de que los usuarios caigan en el engaño

de los mensajes falsos son bastante reducidas. Ahora hay una nueva variante de este tipo de engaño, el spear-phishing, mucho más concreta y, por lo tanto más peligrosa.

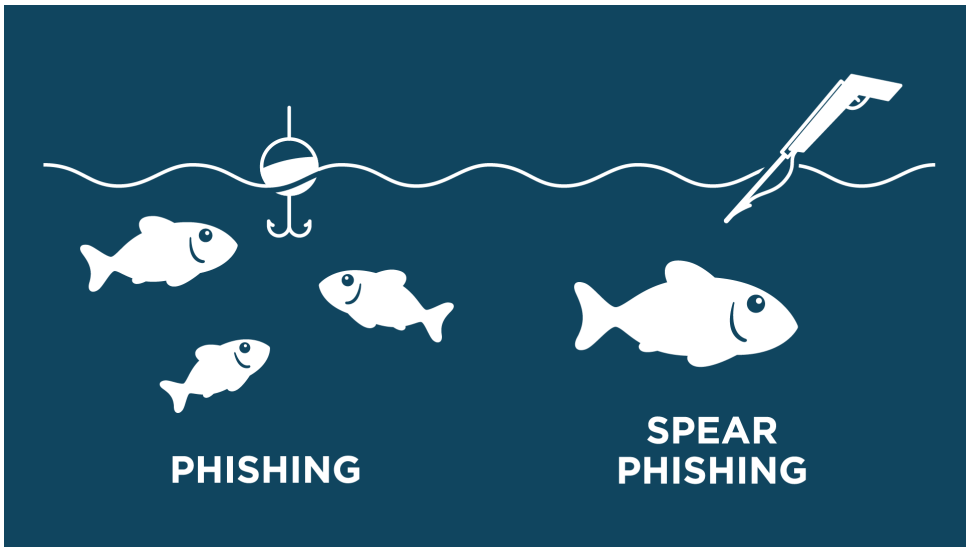

Figura 4.2: Pishing vs Spear-phishing [2]

El spear-phishing, a diferencia del phishing tradicional, es mucho más específico. En este caso, se selecciona a una víctima concreta y el engaño se adapta de forma precisa a la persona elegida. Por eso, el principal foco de estos ataques suelen ser empresas y organizaciones. Los agentes que emplean esta variante de phishing también suelen diferenciarse de los estafadores habituales. En lugar de recopilar todo tipo de información aleatoria para venderla al mejor postor, estos ladrones actúan específicamente contra la víctima seleccionada para causar daño a la empresa o la organización afectada. Por ello, al margen del robo de datos bancarios, también se perpetúan crímenes de espionaje industrial y ciberataques sobre objetivos militares o la infraestructura de una región.

4.3 SQL Injection

SQL Injection es uno de los Ciberataques más frecuentes y amenazadores, ya que puede atacar cualquier sitio web o aplicación que use una base de datos. El ataque consiste en usar un trozo de código para manipular una base de datos y acceder a información potencialmente valiosa empleando consultas SQL. Una consulta SQL no es mas que una solicitud enviada a una base de datos.

Por ejemplo, la información de inicio de sesión de una página web se envía a través de un formulario antes de que el usuario pueda acceder al sitio. Normalmente, este tipo de formulario web está diseñado para aceptar solo tipos muy específicos de datos, como un nombre o una contraseña. Cuando se agrega esa información, esta se coteja contra una base de datos y, si coincide, se otorga acceso al usuario. De lo contrario, se deniega el acceso.

Los problemas surgen porque la mayoría de los formularios web no tienen forma de detener el ingreso de información adicional a través de consultas SQL. Así, los cibercriminales pueden

aprovechar esta vulneravilidad y utilizar los cuadros de entrada del formulario para enviar sus propias solicitudes a la base de datos. Esto podría permitirles llevar a cabo una amplia gama de actividades maliciosas, desde el robo de datos confidenciales hasta la manipulación de la información de la base de datos para sus propios fines.

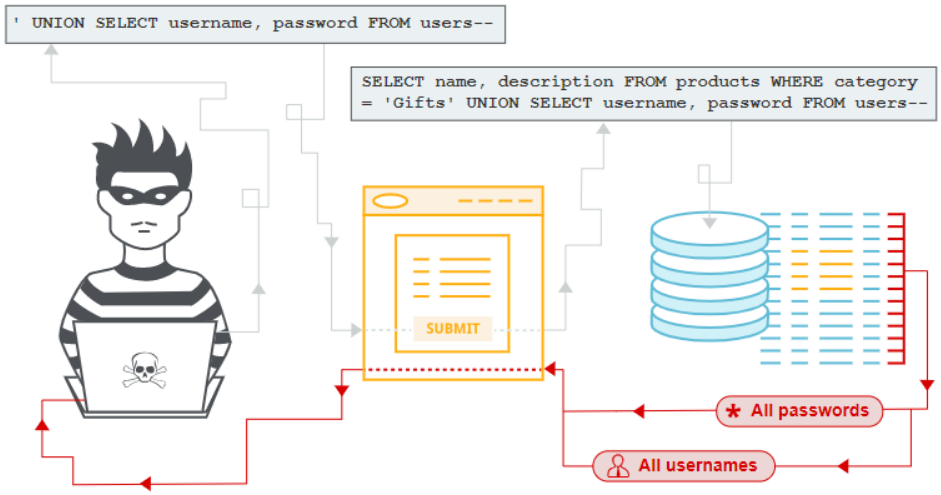

Figura 4.3: SQL Injection [3]

Debido a la prevalencia de sitios web y servidores que utilizan bases de datos, el método de ataque de inyección SQL es uno de los tipos de ciberataques más antiguos y generalizados. Varios avances han aumentado el riesgo de este tipo de ataques, en especial la llegada de programas de inyecciones SQL automatizadas. Estos programas permiten realizar ataques automáticamente en tan solo minutos, pudiendo acceder a cualquier tabla o columna de una base de datos con tan solo un clic y un proceso de ataque.

4.4 Cross site scripting(XSS)

Como acabamos de ver en la sección anterior 4.3, el objetivo de los ataques por inyección de código SQL es obtener información de la base de datos de una empresa u organización. Los ataques por Cross site scriting tienen la misma finalidad que SQL Injection, obtener información a través de consultas SQL, pero en este caso el objetivo no son empresas ni organizaciones sino usuarios individuales.

La inyección de código, al igual que en el caso del SQL, consiste en intercalar pequeños programas o comandos en medio del texto que se escribe en ese recuadro, pero ahora no será el servidor web, ni el sistema de gestión de la base de datos quienes ejecutarán ese código, como en el caso del SQL Injection, sino que ahora con la vulnerabilidad XSS quien ejecutará ese código es el navegador del usuario víctima.

1. **Cross Site Scripting persistente:** Si el código SQL insertado se queda almacenado en el servidor, formando parte de una aplicación web, se dice que el ataque es persistente.

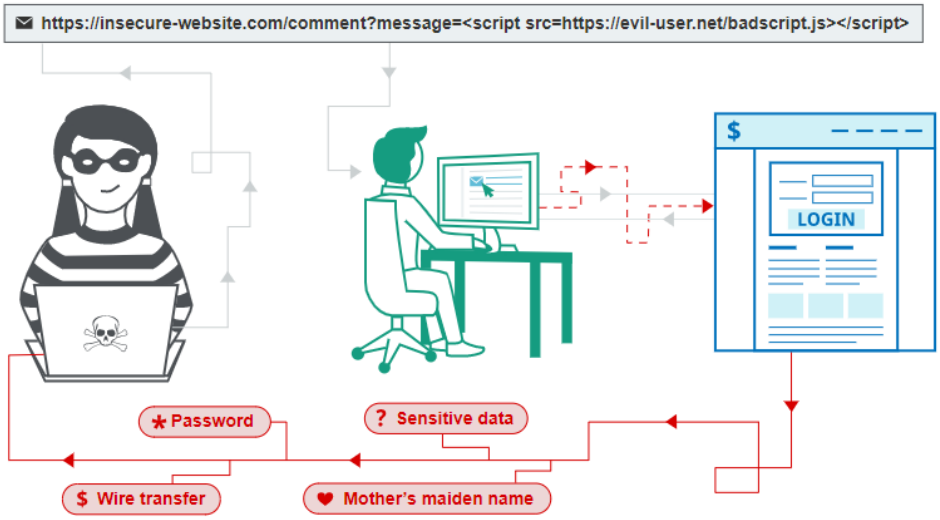

Figura 4.4: Cross site scripting [4]

Normalmente el atacante trata de insertar tags propios de HTML como <iframe>, o <script>, de esta forma el atacante podría ejecutar código malicioso.

2. **Cross Site Scripting reflejado:** Si el código que insertamos no se queda almacenado en la web, sino que va embebido dentro de un enlace que se hace llegar de algún modo a la víctima para que pinche en él, se dice que este tipo de ataque es reflejado. La característica diferencial con el anterior ataque es que en este caso en el servidor web no queda almacenado nada.

4.5 Ataque por denegación de servicio

Un ataque de denegación de servicio tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina, con el fin de bloquear su servicio. Este ataque puede afectar, tanto a la fuente que ofrece la información como puede ser una aplicación o el canal de transmisión, como a la red informática. Existen dos técnicas de este tipo de ataques, la denegación de servicio o DoS (Denial of Service) y la denegación de servicio distribuido o DDoS (Destributed Denial of Service).

En los ataques DoS se generan una cantidad masiva de peticiones al servicio desde una misma máquina o dirección IP, consumiendo así los recursos que ofrece el servicio hasta que llega un momento en que no tiene capacidad de respuesta y comienza a rechazar peticiones, esto es cuando se materializa la denegación del servicio.

En el caso de los ataques DDoS, se realizan peticiones o conexiones empleando un gran número de ordenadores o direcciones IP. Estas peticiones se realizan todas al mismo tiempo y hacia el mismo servicio objeto del ataque. Un ataque DDoS es más difícil de detectar, ya que el número de peticiones proviene desde diferentes IP´s y el administrador no puede bloquear la IP que está realizando las peticiones, como sí ocurre en el ataque DoS.

Como hemos visto, los ataques de denegación de servicio son utilizados para inhabilitar un

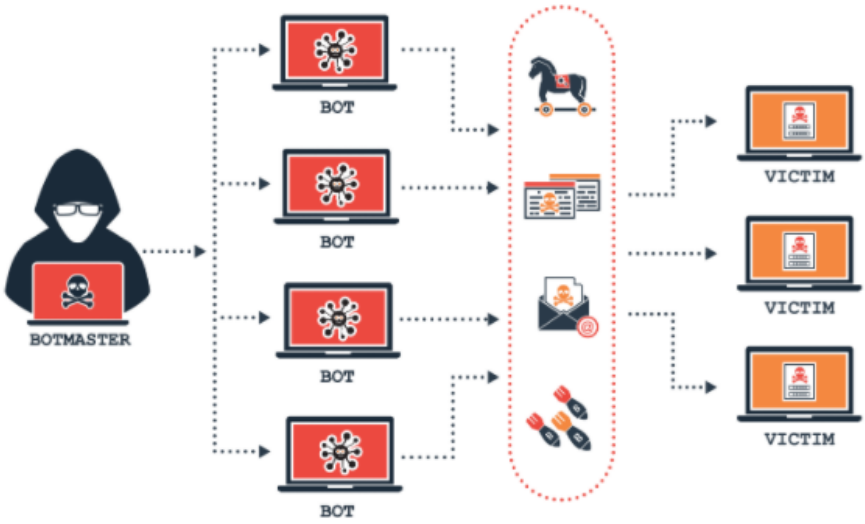

Figura 4.5: Ataque por denegacion de servicio [5]

servicio ofrecido por un servidor, haciendo colapsar el sistema aprovechando sus vulnerabilidades. El objetivo de los ciberdelincuentes es provocar un perjuicio, tanto a los usuarios que se abastecen del servicio, como al administrador que lo ofrece, inhabilitando su funcionalidad y provocando pérdidas, tanto económicas, como de prestigio

Capítulo 5

Planificación de respuesta a incidentes

Mientras que las organizaciones durante estos últimos años han mejorado lentamente en su capacidad de detectar y responder a los ciberataque, su capacidad de contener un ataque ha disminuido en un 13 % durante este mismo período según un estudio realizado por Cyber Resilient Organization Report.[19]

Según la encuesta, los esfuerzos en materia de seguridad se vieron obstaculizados por el uso de demasiadas herramientas, así como por la falta de planes estratégicos específicos para los tipos de ataque más comunes. Aunque la planificación para la respuesta de seguridad está mejorando poco a poco, la gran mayoría de las organizaciones carecen de una guía concreta con los pasos a seguir.

Un plan de respuesta a incidentes cibernéticos consiste en un documento que incluye un conjunto de instrucciones diseñadas para ayudar a las empresas a detectar, responder y recuperarse de los incidentes de seguridad de la red. La mayoría de estos planes se centran en la tecnología y abordan problemas como la detección de malware, el robo de datos y las interrupciones del servicio. Sin embargo, cualquier ataque cibernético ya sea alguno de los mencionados en el Capítulo 4 o cualquier otro, puede afectar a una organización a través de sus funciones de múltiples maneras.

Una vez que tenemos clara la necesidad de contar con un plan de respuesta ante ciberataques, el siguiente paso es el de definir los distintos puntos que debe contemplar dicho documento, que ha de ser lo más completo posible para abarcar todas las situaciones que puedan suceder. Existen una serie de puntos que deben ser analizados en un plan de esta índole:

1. **Auditoría e identificación de la amenaza:** El primer punto del plan de respuesta ante ciberataques debe ser el que especifique los mecanismos necesarios para identificar correctamente la amenaza, incluyendo tanto los procesos internos como la gestión de fuentes de información externas. En este primer punto también debe analizarse y valorarse si la amenaza es real o no, así como qué nivel de gravedad representa para la organización.

2. **Comunicación y notificación:** Una vez detectado el incidente, el plan debe recoger el procedimiento para notificar lo más rápido posible el problema a todos los individuos implicados en el equipo de respuesta.

3. **Equipo de respuesta:** Para poder enviar estas notificaciones y responder al cibercriminal, debe existir un equipo de respuesta perfectamente organizado, con responsabilidades bien definidas, preparado y disponible las 24 horas para atender esta necesidad.

4. **Comunicación externa:** En la línea anteriormente mencionada, el plan de respuesta ante ciberataques debe recoger cómo se afrontará esa crisis de forma pública, tanto ante los medios de comunicación como en redes sociales y también ante los organismos oficiales correspondientes.

5. **Comunicación externa:** El aspecto central del plan es la metodología y las tecnologías que serán utilizadas para eliminar la amenaza, reducir el impacto sobre el negocio y acabar con el problema en todas sus vertientes.

6. **Evaluación final y desactivación del plan:** Una vez que se haya desactivado el virus, el equipo de respuesta debe evaluar de nuevo la situación para decidir si ha llegado el momento de desactivar 'el estado de alarma'. Además, también es un buen momento para asimilar lo aprendido durante el episodio y modificar los métodos preventivos y sistemas de respuesta de forma que se evite cualquier réplica futura de la amenaza.

Capítulo 6

Protección informática

Antes de definir el concepto de protección informática debemos definir el concepto de información, que se define como el activo que tiene valor para alguna empresa o particular por lo que requiere una protección adecuada para garantizar la continuidad del negocio, minimizar daños de terceros y maximizar un entorno adecuado para inversiones y oportunidades de negocio. Sabiendo esto podemos definir como protección informática el conjunto de técnicas, herramientas, sistemas y procedimientos usados para proteger la información que se encuentra localizada en un sistema.

6.1 Caraterísticas de la protección informática

Las cinco características que garantizan una buena protección informática son:

1. **Autentificación:** Permite verificar que la identidad del propietario de un archivo mediante una referenciación en dicho documento. Esta cualidad genera que se pueda corroborar si alguien es quien dice ser, un ejemplo de este mecanismo es la autentificación mediante usuario y contraseña.

2. **Integridad:** Hace alusión a que la información no haya sido modifica y esté totalmente correcta sin que se hayan borrado o editado datos desde que fueron generados. Esto se logra mediante la generación de un hash, que se trata de la generación de un texto corto a partir del archivo original mediante funciones matemáticas. Si se compara el hash del archivo original con la del archivo actual y son iguales, significa que archivo sigue integro y no fue modificado, sin embargo, si son distintas implica que el archivo fue modificado.

3. **Confidencialidad:** Esta cualidad permite que los datos no sean accesibles a sistemas y personas no deseadas, haciendo que los datos estén cifrados y solo puedan ser legibles para las personas o sistemas autorizados. En el caso de que una persona no autorizada intercepte la información esta lo verá de una forma ilegible debido a que los datos estarán encriptados, esta cualidad se puede implementar mediante criptografía simétrica o asimétrica, en la criptografía simétrica tanto solo el emisor y receptor conocen una clave para desencriptar el archivo. Con la criptografía asimétrica el emisor tiene una clave privada que solo conoce

el mismo y una clave pública ligada a la privada que conoce todo el mundo, el emisor encriptará los datos con su clave privada y el receptor los desencriptará con la clave pública del emisor.

4. **Disponibilidad:** Como su nombre indica esta cualidad permite el acceso y la utilización cuando y donde sea de los servicios a través de un canal seguro. También se incluye que información eliminada sea recuperable en todo momento pudiendo evitar su pérdida o bloqueo. Esta característica es de las más importantes para las grandes empresas como Facebook y en hospitales y aeropuertos debido a que necesitan que sus servicios estén funcionando las 24 horas los 7 días de la semana.

5. **No repudio:** Consiste en la irrenunciabilidad por parte de la información de un emisor. Es muy similar a la autentificación, sin embargo, se diferencia en que la autentificación se centra en las personas implicadas y la cualidad de no repudio va enfocada frente a terceros. Un ejemplo de esta característica serían las firmas electrónicas, el proceso es bastante similar al de la criptografía simétrica usado en la confidencialidad, una persona crea un documento del que se obtiene el hash, este hash es encriptado con la clave privada dicha persona y el resultado de esto es la firma electrónica que es añadida al documento.

6.2 Tipo de seguridad en función del momento

Dependiendo del momento en el que apliquemos medidas de seguridad podemos clasificarlas en:

1. **Seguridad activa:** Se centra en prevenir y evitar daños a los sistemas ya sean de tipo hardware o software. Los mecanismos más frecuentes relacionados con este tipo de seguridad son por ejemplo los antivirus, la encriptación de datos, controles de acceso a salas, sistemas de redundancia de hardware. En conclusión, usaremos el término de seguridad activa para referirnos a técnicas para ser proactivos ante amenazas.

2. **Seguridad pasiva:** La seguridad pasiva, no es lo contrario a la seguridad activa sino que es un complemento al que se recurre cuando las medidas de seguridad activa no han sido adecuadas para frenar una amenaza. Un ejemplo sencillo son las copias de seguridad aunque el hecho de realizar las copias de seguridad es poner en marcha una seguridad activa ya que nos anticipamos a la amenaza de perder nuestra información. Sin embargo, el hecho de recuperar un archivo de una copia de seguridad, pasa a ser seguridad activa debido a que una vez producido el daño, podemos solucionarlos. En este caso nos referiremos a la seguridad pasiva como una forma de ser reactivos actuando una vez se haya producido el daño.

Capítulo 7

Sistemas utilizados para mantener la seguridad y la privacidad

7.1 Sistemas hardware:

Consiste en aplicar impedimentos físicos y funciones de control como medida de prevención y contra medidas ante amenazas a recursos confidenciales, estos procedimientos son aplicados en equipos del hogar, oficinas y a servidores y cpds.

1. **RAID (Redundant Array of Independent Disk):** Es usado para crear un único volumen lógico, el cual físicamente esté compuesto por varios discos físicos. Dependiendo de qué modo de RAID utilicemos, esto nos servirá para conseguir un volumen con mayor seguridad contra fallos de hardware de los discos que lo componen gracias al almacenamiento redundante de estos o para conseguir simplemente un volumen de capacidad mayor. Protegen la disponibilidad de la información. Los modos de raid que ofrecen una mayor seguridad del dispositivo son:

   (a) **RAID 1:** Para ello son necesarios al menos 2 discos de igual tamaño, se realiza una copia espejo es decir lo que de escribe en uno se copia en el otro permitiendo de esta forma que, aunque se produzca un fallo en uno de los 2 discos sigamos conservando la información en otro el disco.

   (b) **RAID 5:** En esta configuración necesitaremos mínimo 3 discos de la misma capacidad, la capacidad total de almacenamiento será la de todos los discos menos uno, es decir, dos y los datos se irán almacenando de forma parcialmente redundante permitiendo que, aunque suframos un fallo en uno de los discos, podamos seguir accediendo a toda la información. Este sistema es más eficiente que el RAID 1 debido a que en este solo tenemos la capacidad de almacenamiento de uno de los discos y en el RAID 5 tenemos la capacidad de dos, aunque la desventaja de este sistema es que requiere un disco más.

2. **Sistemas de Alimentación Ininterrumpida (SAI):** Son dispositivos que ofrecen protección contra apagones o irregularidades en la corriente eléctrica. Su principal función es suminis-

trar la energía eléctrica que tienen acumuladas en sus baterías cuando se producen cortes eléctricos evitando así posibles fallos y averías en los sistemas conectados el evitan que se apaguen de forma repentina, además algunos SAI poseen un regulador de tensión que asegura estabilidad en la corriente logrando una alimentación de los dispositivos conectados más constante y así prolongando la vida útil de dichos sistemas. Protegen la disponibilidad de la información.

3. **Firewall de hardware:**

   También conocido como cortafuegos se trata de un dispositivo que es capaz de bloquear comunicaciones no autorizadas, permitiendo las que si lo están. Los cortafuegos permiten una configuración para permitir y limitar el tráfico entre distintas redes o ámbitos de una red mediante un conjunto de reglas y normas. Sus principales características son el filtrado por aplicación, reglas de filtrado sobre el tráfico de entrada y salida de una red en una interfaz de red, filtrado de paquetes comprobando su MAC, IP o puerto destino y origen y almacenar el registro del filtrado de paquetes. También existe el firewall de software, la diferencia es que el cortafuegos de hardware se trata de un dispositivo dedicado únicamente como firewall y el de software no. Protegen la integridad de la información. Las arquitecturas de cortafuegos más implementadas son:

   (a) **Screening router:** Un router hace de frontera entre la red pública y la red privada, realizando la función de cortafuegos.

   (b) **Dual Homed-Host:** Un servidor con al menos dos interfaces de red divide la red pública de la red privada y la función de firewall.

   (c) **Screened Host:** Se trata de la combinación de un router como frontera y un servidor proxy que realizará las tareas de filtrado.

   (d) **Screened-subnet:** Se crea una red intermedia entre la red externa y la red privada denominada DMZ o zona desmilitarizada en la que se localizan los servidores, teniendo un nivel de seguridad mayor en el cortafuegos de acceso a la red interna y uno menor en el cortafuegos hacia la red externa.

4. **Servidor proxy:** Consiste en un sistema que gestiona conexiones de red, haciendo de intermediario entre las peticiones de los servidores y los clientes, como FTP, DNS, https, etc., generando de tal forma una memoria caché con las diversas peticiones y respuestas de los servidores. Aunque su principal finalidad no es la seguridad sino que es servir más rápidamente a las conexiones siguientes que hayan sido solicitadas, añade funciones de autentificación y control de usuarios, reglas de filtrado de contenidos solicitados y un registro de logs. Protegen la disponibilidad e integridad de la información. Los tipos de servidor proxy que ofrecen una mayor seguridad son:

   (a) **Proxy transparente:** Para el uso de este servidor proxy es necesario la configuración de cada cliente manualmente. Se encarga de redireccionar todas las conexiones al puerto 80 (http) hacia el puerto del servidor haciendo que estas conexiones sean más seguras.

(b) **Proxy anónimo:** Este servidor proxy aumenta la privacidad y el anonimato de los clientes mediante una eliminación activa de característica identificativas como la dirección IP del cliente, cookies, identificadores de sesión, etc.

(c) **Proxy caché web:**

-Proxy caché Web: Este proxy es usado específicamente para web y se encarga de hacer copias locales de los archivos más solicitados por los clientes.

(d) **Proxy inverso:** Consiste en un servidor proxy instalado en una red con varios servidores web y realizará en función de intermediario a las peticiones externas ofreciendo una capa de seguridad previa, además de distribuir la carga de las distintas peticiones externan y gestionar el SSL.

7.2 Sistemas Software:

Son usados para garantizar la protección del software frente a ataques maliciosos de hackers, pérdida de información y otros riesgos de manera directa.

1. **Cortafuegos:** Su funcionamiento es igual al del firewall de hardware con la única diferencia de qué el firewall de hardware consiste en un sistema únicamente dedicado cómo firewall y el de software simplemente se trata de una aplicación. Protege la integridad de la información.

2. **Antivirus:** Se trata de una aplicación que es usada para prevenir, detectar y eliminar virus localizados en un sistema. Su funcionamiento consiste en la comparación de los archivos del sistema con los de una base de datos que contiene distintos tipos de malware conocidos, dichas bases de datos son actualizadas constantemente debido a que los hackers generan y propagan nuevos virus constantemente. Protege la integridad de la información.

3. **Encriptación (cifrado de datos):** Los datos son enmascarados con una clave especial qué es creada mediante un algoritmo matemático. Solamente el emisor y el receptor conocen la clave y a la llegada del mensaje se produce el descifrado. El cifrado de datos fortalece la confidencialidad.

4. **Control de acceso:** se trata de la verificación de un usuario solicitando datos que solo debería de conocer el mismo, como un nombre de usuario y una contraseña. Protege la autenticidad de la información.

5. **Firma digital:** Es usada en la transmisión de mensajes telemáticos y en la gestión de documentación como por ejemplo en las oficinas virtuales. Su objetivo es identificar de forma segura al equipo qué se hace cargo de la información. Protege la integridad y la confidencialidad de la información.

6. **Certificados digitales:** Se trata de documentos digitales mediante los que una entidad certificadora asegura que una persona es quien dice ser, mediante su clave pública. Protege la integridad y la confidencialidad de la información.

Bibliografía

[1] T. para los negocios, "Qué es un ciberataque y qué tipos existen," https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-un-ciberataque-y-que-tipos-existen/ [Ultimo acceso 27/diciembre/2020].

[2] ClickArmor, "What is the difference between spear phishing and regular phishing?" https://clickarmor.ca/spear-phishing-vs-regular-phishing/ [Ultimo acceso 26/diciembre/2020].

[3] PortSwigger, "Sql injection," https://portswigger.net/web-security/sql-injection [Ultimo acceso 27/diciembre/2020].

[4] ——, "Cross site scripting," https://portswigger.net/web-security/cross-site-scripting [Ultimo acceso 27/diciembre/2020].

[5] O. de Seguridad del Internauta, "Â¿qé son los ataques dos y ddos?" https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos [Ultimo acceso 27/diciembre/2020].

[6] ISACA, "bsecure conference," Information Systems Audit and Control Association, Tech. Rep., 2017.

[7] G. Sanchez, *Temas candentes de la Ciberseguridad: Un nuevo espacio lleno de incognitas.* PwC.

[8] Incibe, "Amenaza vs vulnerabilidad," https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian.

[9] Infosegur, "Definición de integridad," https://infosegur.wordpress.com/tag/integridad/.

[10] Wikipedia, "Análisis de riesgo informático," https://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo_inform%C3%A1tico.

[11] S. L. Leedeo Engineering, "Diagrama árbol de fallas," https://www.leedeo.es/l/fta/.

[12] J. A. D. B. y Rosemary Martins, "Diagrama de ishikawa," https://blogdelacalidad.com/diagrama-de-ishikawa/.

[13] A. G. Villoldo, "Análisis modal de fallos y efectos," http://asesordecalidad.blogspot.com/2017/06/amfe-analisis-modal-de-fallos-y-efectos.html.

[14] SlidePlayer, "Hazop," https://slideplayer.es/slide/11119155/.

[15] G. Energy., "Lopa," https://gate.energy/the-arrow-blog/pme/opsread/gat2004-gkp-2014-07/introduction-to-layer-of-protection-analysis-lopa.

[16] R. A. de la Ingeniería, http://diccionario.raing.es/es/lema/ciberataque [Ultimo acceso 25/diciembre/2020].

[17] Akamai, "Ciberataques," https://www.akamai.com/es/es/resources/cyber-attacks.jsp [Ultimo acceso 26/diciembre/2020].

[18] Xataka, "Malware: qué es, qué tipos hay y cómo evitarlos," https://www.xataka.com/basics/malware-que-que-tipos-hay-como-evitarlos [Ultimo acceso 27/diciembre/2020].

[19] IBM, "Ibm: 2020 cyber resilient organisation report," *ELSEVIER Network Security*, vol. 2020, no. 7, pp. 1–4, July 2020.

[20] K. Lab, "Ransomware," https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware.

[21] D. Lázaro, "Ataques sql injection en php," https://infosegur.wordpress.com/tag/integridad/.

[22] E. I. B. School, "Tipos de vulnerabilidad en ciberseguridad," https://www.campusciberseguridad.com/blog/item/118-tipos-de-vulnerabilidades-en-ciberseguridad.

[23] T. . Informática, "Vulnerabilidades informáticas," https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/.

[24] C. Europea, "Datos personales sensibles," https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_es.

[25] ISOTools, "Matriz de riesgos," https://www.isotools.org/2015/08/06/en-que-consiste-una-matriz-de-riesgos/.

[26] P. SSI, "Gestionar los activos de información según sgsi," https://www.pmg-ssi.com/2017/01/como-gestionar-activos-informacion-sgsi/.

[27] Incibe, "Ensi_arli-cib_01- modelo de análisis de riesgos ligero de ciberseguridad en sistemas de control industrial (arli-cib)," https://www.incibe-cert.es/sites/default/files/paginas/publicaciones/ensi/ensi_arli-cib_01_metodologia-aarr_borrador.pdf.

[28] E. business school, "7 herramientas para la evaluación de riesgos," https://www.ealde.es/herramientas-evaluacion-de-riesgos/.

[29] E. D. R. Moncayo, "Análisis e integración de los modelos aplicados a riesgos tecnológicos," https://bibdigital.epn.edu.ec/bitstream/15000/8499/3/CD-5741.pdf.

[30] B. School, "Xss: qué es y cómo funciona el cross site scripting," https://blogs.imf-formacion.com/blog/tecnologia/xss-que-es-y-como-funciona-201805/ [Ultimo acceso 27/diciembre/2020].

[31] TICbeat, “Â¿cómo crear un plan de respuesta a ciberataques?” https://www.ticbeat.com/seguridad/como-disenar-un-plan-de-respuesta-a-ciberataques/ [Ultimo acceso 28/diciembre/2020].