Ciberseguridad:
Amenazas y vulneravilidades en la red

Tecnologías para la Sociedad Digital

31 de Diciembre de 2020

Equipo: Equipo de trabajo número 6

Autores: Carlos Yanguas Durán, Alberto Larena Luengo, David Márquez Mínguez

Tutor: Jesús Alpuente Hermosilla

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" [**?**].*

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.).[**?**],[**?**]

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.[**?**]

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 [**?**].

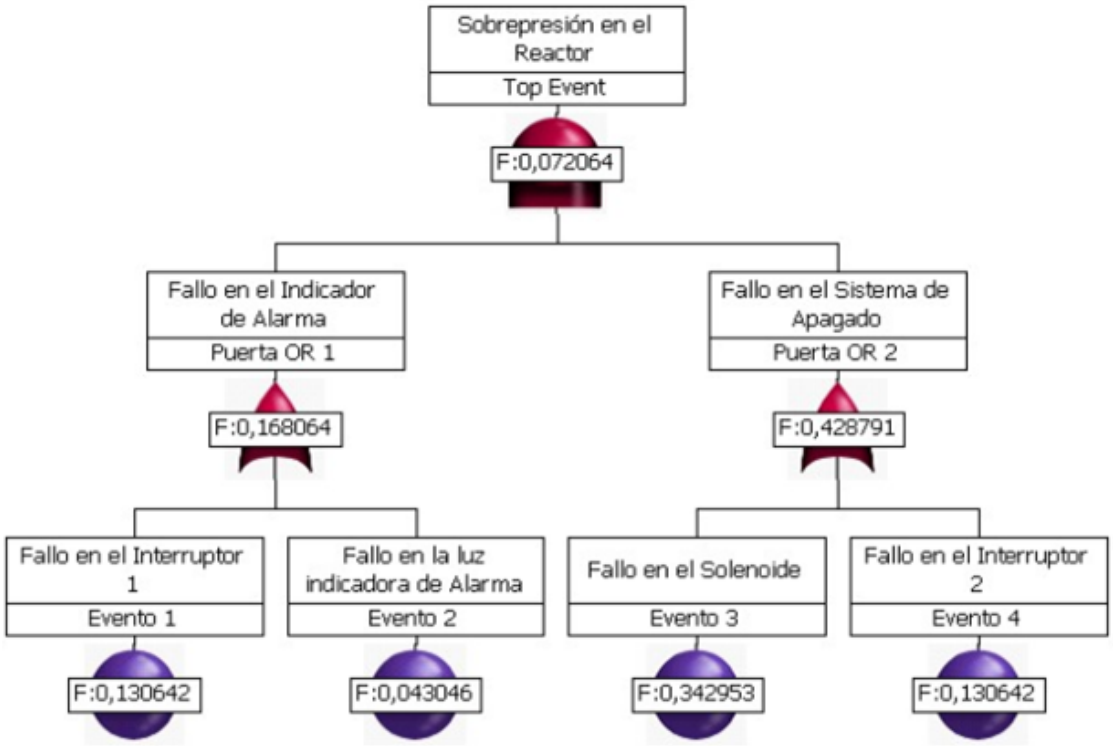

Figura 3.2: Diagrama árbol de fallas.

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 [**?**].

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 [**?**].

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 [**?**].

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 [**?**].

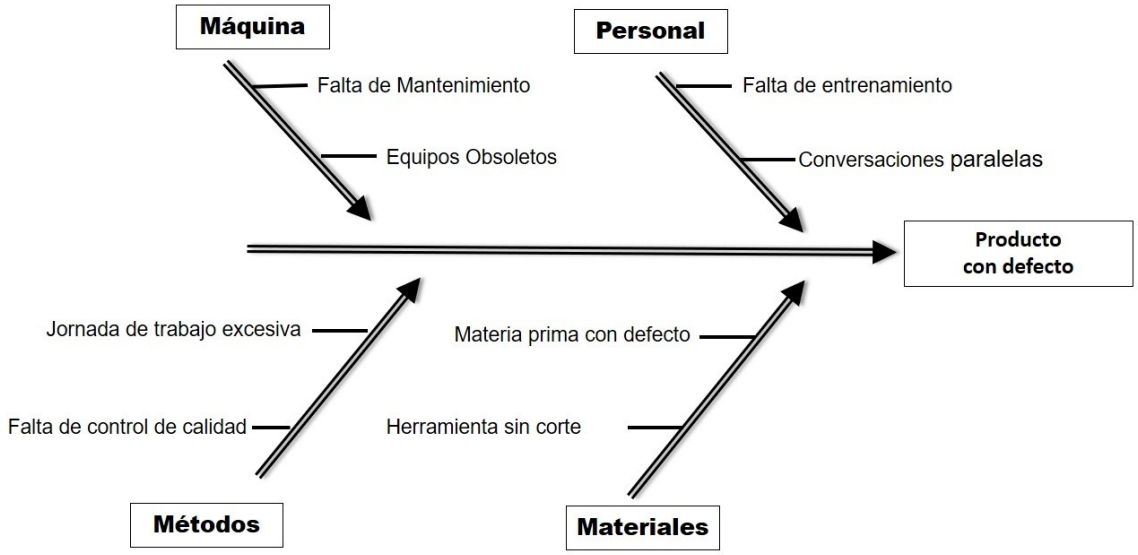

Figura 3.3: Diagrama causa-efecto.

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."[?].

Estos ciberataques aprovechan alguna de las vulnerabilidades ya comentadas en el capítulo 2, estando asociadas al software, a los dispositivos informáticos o a las personas que los administran y utilizan. Mientras tanto, los piratas informáticos y cibermercenarios crean, distribuyen y utilizan sofisticadas herramientas de exploit y malware 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.

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) y los ataques de fuerza bruta, adaptándolos o usándolos de forma combinada para llevar a cabo elaborados ciberataques. 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.

4.1 Spear-phishing

A partir de los correos electrónicos de phishing 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.

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.

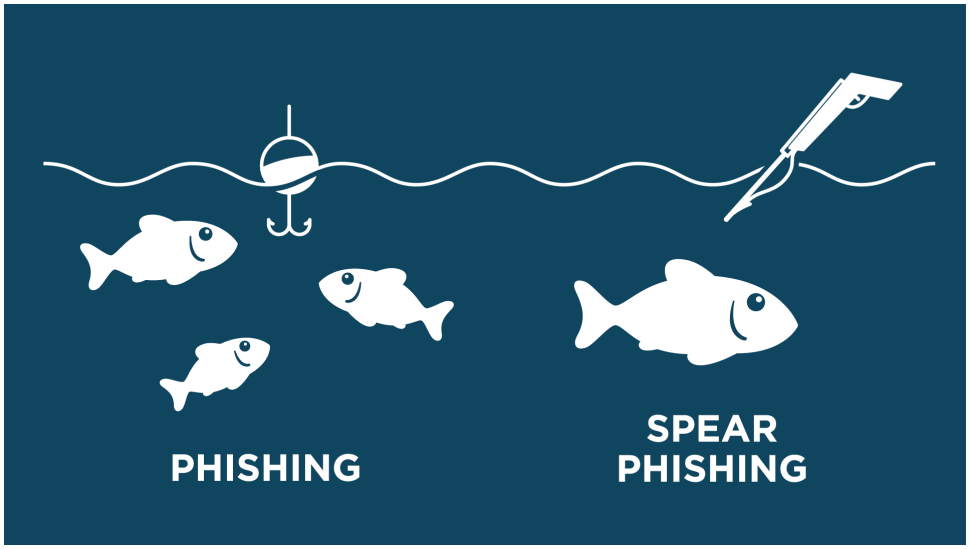

Figura 4.1: Pishing vs Spear-phishing [**?**]

El spear-phishing, en cambio, 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.

4.2 SQL Injection

Este Ciberataque consiste en usar un trozo de código para manipular una base de datos y acceder a información potencialmente valiosa.

Capítulo 5

Planificación de respuesta a incidentes

Capítulo 6

Protección informática

(Añadir aquí introducción de este apartado) Las características que garantizan la 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.

Capítulo 7

Sistemas utilizados para mantener la seguridad y la privacidad

En primer lugar.[**?**]. holaaa