CRIPTOGRAFÍA AVANZADA

AUTOR: LUIS RAMÍREZ LORÍA

MARZO: 2021

San Marcos

Tabla de contenido

Introducción

Durante el desarrollo del curso se han establecido una serie de conceptos y mecanismos importantes para la gestión de riesgo informático, estableciendo cómo las organizaciones y empresas pueden tomar acciones para la preparación de planes de respuesta a los riesgos (amenazas y vulnerabilidades informáticas), su identificación, valoración, clasificación e incluso, la priorización del abordaje de las salvaguardas o contramedidas sobre las cuáles es requerido establecer mecanismos de implantación, atención, evaluación y evolución, tal como lo señala el ciclo de Deming (planificar, hacer, verificar y actuar), siendo fundamental la mejora continua y evaluación continua.

Como tal, cuando se analizan aspectos asociados con tecnología, se presentan retos para las empresas, inicialmente por los costos implicados y en segundo lugar por las frecuentes modificaciones que se presentan en los recursos TIC, asociado con el acceso a los datos, el uso de los sistemas de información y el aumento en las actividades comerciales digitales y transformación digital de los negocios, aumentan los retos asociados a la seguridad de la información.

Con esta base es importante continuar con el abordaje de conceptos asociados con la seguridad informática, tales como:

- Ingeniería criptográfica
- Ataques de red y defensas
- Teléfonos (y dispositivos móviles)
- La guerra electrónica y de información
- Copyright y DRM,
- Balances, vigilancia vs privacidad.

Lo anterior busca ampliar el conocimiento en una materia en constante cambio y evolución, por lo cual, estos conceptos brindan a los estudiantes un marco general sobre el cual ahondar en su proceso de formación académica.

Ingeniería criptográfica avanzada

Tal cual fue analizado en la lectura anterior, el concepto de encriptación en seguridad informática nos señala que:

- *"La encriptación o también conocido como cifrado, es un procedimiento en el que se busca que la información sea ilegible, ya aplicado este procedimiento la información es inservible para cualquier persona que no sea la autorizada, aunque el mensaje sea interceptado, como en muchos casos la información simplemente no significa nada para el interceptor, ya que no cuenta con los elementos involucrados en la encriptación, así que la información simplemente no sirve."* (Romero Castro, y otros, 2018)

Fuente: (Romero Castro, y otros, 2018)

La encriptación busca asegurar la persistencia de los datos e involucra este proceso de llaves o claves que se utilizan como contraseñas para autentificar la encripción y desencripción de los mensajes y su información, según el estudio anterior este proceso nos garantiza que se cumplas los objetivos asociados a las características de la información reconocidas como:

- Confidencialidad
- Autenticación
- Integridad.

Pilares de la seguridad. Fuente: (Romero Castro, y otros, 2018)

La confidencialidad implica que la información solo pueda ser accesada por las personas que requieren su uso o para quienes ha sido preparada, autenticación permite que el emisor y receptor puedan ser identificados adecuadamente y la integridad es una garantía de que la información no ha sido alterada durante su comunicación. Para garantizar estas características la encriptación ofrece métodos de encriptación simétrica, y métodos de encriptación asimétrica de clave pública y privada, encriptaciones tipo WPA, WEP y la muy reconocida firma digital.

Encriptación simétrica

Este modelo de encripción utiliza la misma clave para cifrar y descifrar el mensaje, estos extremos cuando establecen la comunicación deben establecer un acuerdo sobre la clave que tienen que usar, para posteriormente los dos tener acceso a la misma clave, en donde el remitente cifra el contenido de la misma y el destinatario la descifra con el mismo mecanismo. Los siguientes son ejemplos de algoritmos de encriptación simétricos:

- Algoritmo de cifrado DES, usa claves basados en 56 bits
- Algoritmos de cifrado 3DES, Blowfish, e IDEA, usan claves de 128 bits
- Algoritmos de cifrado RC5 y AES

Encriptación asimétrica

Este tipo de encriptación se basa en que, si el emisor cifra o encripta la información, en este escenario el receptor lo puede descifrar o viceversa, en este caso cada usuario del sistema debe poseer una pareja de claves y se tiene dos tipos.

- Clave privada: Custodiada por el propietario, por lo cual únicamente él tiene acceso a esta clave sin darla a conocer a nadie.
- Clave pública: conocida por uno o todos los usuarios, permitiendo los procesos de encripción y desencripción por varias partes.
- Ejemplos de estos algoritmos son:
    - MD5. Abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado. Uno de sus usos es el de comprobar que algún archivo no haya sido modificado
    - SHA. Secure Hash Algorithm, un conjunto de funciones hash diseñado por la Agencia de Seguridad Nacional de los Estados Unidos para encriptar de información. El más utilizado es el SHA-256 en el protocolo para Bitcoins.

Firma digital

Como mecanismo de ingeniería criptográfica avanzada, la firma digital tiene como objetivo autentificar la identidad de quién envía el mensaje y quién firma un documento electrónico,

las firmas digitales acostumbran manejar diferentes datos según la entidad que la otorga y la regulación que sigue. Además de información que se envía datos como hora y fecha en que se hizo. La firma digital es una forma matemática de adjuntar la identidad de una persona a un mensaje mediante mecanismo de encripción, está basada en la criptografía de clave pública, esto quiere decir que estos sistemas están utilizando dos claves, la primera sería la clave pública que es la que se conoce y la otra clave sería una clave privada qué es la que solamente el emisor del mensaje conoce.

Encriptación WEP y WPA

Acorde a lo señalado por Romero Castro y otros, estos dos modelos de encriptación, WEP y WPA, son modelos aplicados al cifrado de las señales inalámbricas e indican que ambos están basados en protocolos de conexión Wifi la primera y la segunda se basa en servidores de autentificación.

- "En el caso de WEP se tiene tres opciones, de 64 bits, de 128 bits y 256 bits, en donde la más utilizada es la de 128 bits ya que ofrece un buen nivel de seguridad sin tener que ser tan grande y sin aumentar lo complicado del tema. Actualmente la encriptación de 256 bits aún no es soportada por todos los dispositivos." (Romero Castro, y otros, 2018)

Adicionalmente estos autores señalan que existen diferentes opiniones entre los expertos en seguridad sobre si un método de cifrado, es una buena opción para aportar seguridad a las comunicaciones, es decir, si es un método confiable, pero a su vez concluyen que, un sistema de cifrado se puede considerar como bueno cuando la seguridad de cifrado se basa o consiste en la clave de encripción y no en el algoritmo, dado que estos algoritmos son altamente conocidos en la actualidad.

- *"Aunque se conozca el algoritmo, no se puede llegar a un descifrado de la información gracias a la clave. La mayoría de las aplicaciones que se dan a la encriptación hoy en día son:*
    - *Mensajes de autenticidad*
    - *Facturas electrónicas*
    - *Banca electrónica*
    - *Votos electrónicos*
    - *Notificaciones*
    - *Mensajería instantánea*
    - *Correos electrónicos*
    - *Almacenamiento de información"* (Romero Castro, y otros, 2018)

Ataque de red y defensa

Al igual que otros aspectos asociados a la seguridad informática, se deben establecer principios para asegurar las redes de información y la defensa de información, ya que se indica por parte de los autores que cerca de un 90% de los ataques informáticos obedecen a malas prácticas de las personas.

Principio de mínimos privilegios

Romero Castro y otros nos señala que: *"La ley de mínimos privilegios establece que para la realización de una tarea, un usuario debe disponer de los privilegios mínimos necesarios durante el tiempo imprescindible y con el alcance limitado a lo que exija la tarea, por ejemplo si se trabaja con una computadora se debería tener un usuario normal y otro con privilegios de administrador, de este modo solo se usaría el usuario administrador cuando se tuviese que hacer cambios de configuración, instalar o desinstalar software, aplicar actualizaciones parches de seguridad o gestionar las copias o respaldos, el resto del tiempo para operar con el contenido habitual, para navegar por internet, gestionar el correo electrónico, etc., se operaría con un usuario sin privilegios especiales lo que minimiza el riesgo de infección por malware, espionaje, filtración de datos, corrupción de archivos del sistema"* (Romero Castro, y otros, 2018). A nivel de red aplican los mismos principios, es decir, un usuario o varios usuarios con privilegios de acceso y administración, manejo inseguro de claves, claves de autenticación por defecto, inexistencia de políticas de vencimiento de claves de red de usuario, de administrador y de súper usuarios (root o admin) incorporan vulnerabilidades fácilmente aprovechables por los intrusos en las redes de información de las organizaciones y empresas.

Fuente: Elaboración propia

Escáneres de vulnerabilidades

Una forma práctica de analizar las amenazas y vulnerabilidad de ataque que posean nuestras redes e infraestructura de TI es la aplicación de un escáner de vulnerabilidades, este tipo de sistemas por lo general se pueden aplicar sin problema para su ejecución ni riesgo, Romero Castro y otros nos señalan varios de estos sistemas como:

- **Acunetix:** analiza la parte web y no sólo permite escanear, también permite la explotación real de ciertas vulnerabilidades o incluso la comprobación de estas. Los escáneres web trabajan con proxys y a partir de estos se realiza la captura de las tramas de la información y se puede realizar la modificación. Algunos escáneres utilizan métodos que van a permitir listar el contenido del servidor de acuerdo a los directorios más conocidos con el objetivo de encontrar agujeros de seguridad en las aplicaciones web, los cuales puedan ser aprovechados por determinados atacantes para accesar a los sistemas y la información.
- **Netsparker y ProxyStrike** que permiten detectar vulnerabilidades. Permiten identificar inyecciones de SQL y Cross Site Scripting.
- **LanGuard y OpenVAS**, pueden utilizar el escáner sin tener credenciales o con credenciales de la red local, aparte de realizar un escaneo, evaluar las políticas tanto del equipo, como las de seguridad e incluso se podría empezar a ver si realmente las áreas de administración están teniendo un cumplimiento de sus políticas internas y analizar los procedimientos para la gestión de los equipos cuando se hace una prueba de penetración.
- **Nessus**: Este sistema permite incorporar políticas de seguridad en la infraestructura de TI, a nivel de red permitir identificar o descubrir servicios publicados en la red, permite descubrir los equipos que están en la red e incluso realizar pruebas hacia aplicaciones web, permite el análisis de malware directamente en equipos Windows sobre los que se pueden analizar si los equipos están comprometidos con malware específicos, hasta vulnerabilidades muy específicas las cuales se pueden ir personalizando de acuerdo a lo que se necesite una contramedida de gestión o administración. En el caso de que el escaneo fuera hacia una infraestructura web, se pondría ya sea la URL del sitio o se bastaría con ubicar la IP con el puerto que se está trabajando, en este caso existen también otras opciones, en el cual se pueden manejar notificaciones y para esto se tendría que configurar los servicios de SMTP, POP3 de acuerdo al servidor que va a enviar el correo.

Los escáneres de vulnerabilidades funcionan de una manera muy práctica y pueden traer ventajas con una aplicación simple, ya que por medio de estos los expertos en TI pueden identificar con mayor claridad la vulnerabilidad de red que tenga gran relevancia y con esto desarrollar planes de acción. Sobre las firmas y actualizaciones que van a validar estas vulnerabilidades, los escáneres tienen mecanismos bajo los cuales se actualizan directamente, bajan las firmas y a partir de allí se puede realizar el escaneo.

Tipos de ataques a las conexiones

Los ataques a las conexiones son muy comunes, principalmente en las redes inalámbricas o redes Wifi sobre las cuales los ciberdelincuentes se sirven de diversos software y herramientas con las que saltarse las medidas de seguridad e infectar o tomar control de nuestros dispositivos. Por lo general este tipo de ataques se basan en interponerse en el intercambio de información entre las personas y el servicio web, para monitorizar y robar datos personales, bancarios, contraseñas, y otros, sobre estos se analizarán los principales señalados por el Instituto Español de Ciberseguridad:

Redes trampa

Las redes trampa son redes wifi falsas, esta es una práctica muy utilizada en la delincuencia electrónica y consiste en la creación de una red wifi gemela a otra legítima y segura, con un nombre igual o muy similar a la original, que crean utilizando software y hardware buscando configurar con los mismos parámetros que la original, esperando que la persona se conecte a esta. Este tipo de ataques suelen darse en lugares con una red wifi pública, con gran afluencia de usuarios. De modo que su red falsa pueda pasar desapercibida y engañe al mayor número de víctimas posible.

El objetivo es conseguir robar datos cuando se acceda a cuentas bancarias, redes sociales o correo electrónico, pensando que se está llevando a cabo una conexión segura. Además, el ciberdelincuente puede llegar a tomar control sobre nuestra navegación, accediendo a determinadas webs fraudulentas o muy similares a la original preparadas para el engaño o para la infección por malware. La mejor forma de prevenir este ataque es aprendiendo a identificar las redes wifi falsas:

- El primer indicativo es que existan dos redes con nombres iguales o muy similares. O, por ejemplo, que añadan la palabra “gratis”.
- Si las webs a las que accedes tras conectarte solo utilizan el protocolo http, detén tu actividad y desconéctate.
- Es probable que estas redes estén abiertas o que permitan introducir cualquier contraseña.

Otra medida preventiva es desconectar la función del dispositivo móvil para conectarse automáticamente a redes abiertas. Finalmente, como protección, no es recomendable utilizar este tipo de redes cuando vamos a intercambiar información sensible, como nuestros datos bancarios. En caso de necesidad, podemos recurrir a una VPN. (Instituto Nacional de Ciberseguridad, 2019)

Spoofing

Esta técnica consiste en el empleo de técnicas de hacking de forma maliciosa para suplantar nuestra identidad, la de una web o una entidad. Se basa en tres partes: el atacante, la víctima y el sistema o entidad virtual que va a ser falsificado. El objetivo de los atacantes es, mediante esta suplantación, disponer de un acceso a nuestros datos. Según el tipo de Spoofing, la suplantación y el engaño se llevarán a cabo de forma distinta. Como protección,

es fundamental que nos mantengamos alerta y sigamos las recomendaciones para una navegación segura.

IP Spoofing

En esta técnica el ciberdelincuente consigue duplicar o fingir la dirección IP y hacerla pasar por una dirección distinta. De este modo, consigue saltarse las restricciones del router del servidor empresarial o del nuestro y podría hacernos llegar un paquete con malware. Esto se consigue mediante software especializado que aprovecha debilidades del protocolo IP. El principal objetivo en estos casos es el acceso a redes que sirven para autenticar usuarios o que aplican permisos, restricciones y listas de acceso basados en IP y con esto robar información o credenciales. Suele utilizarse para ataques DDoS por lo que, si consigue infectar, podría tomar control de dispositivos para llevar a cabo un ataque de denegación de servicio.

Es recomendable llevar a cabo un filtrado de las direcciones IP para controlar las conexiones entrantes. Para ello, es necesario acceder a la configuración del router, ir al apartado Seguridad y acceder al Firewall. Desde aquí, es posible filtrar las direcciones IP aplicando normas y reglas de filtrado a los paquetes que entren al router. Una configuración segura del router protegerá el sistema de este y otros tipos de ataque.

Web e Email Spoofing

Este modelo de ataque consiste en la suplantación de una página web real por otra falsa, también se realiza por medio de correos electrónicos falsos. La web/correo electrónico falso es una copia del diseño de la original, llegando incluso a utilizar una URL muy similar. El atacante trata de hacernos creer que la web falsa es la original, para lo cual se basa en las técnicas de ingeniería social que han sido mencionadas con anterioridad. El objetivo de esta técnica es similar al anterior, ingresar a la información del empleado o persona y luego autenticarse en los ambientes oficiales para robar datos, dinero de cuentas, información y otros.

Para resguardarse hay que estar atentos a que al ser un ataque que suele llegar en forma de enlace se debe revisar con mucho cuidado la URL para identificar diferencias con la original. También habrá que desconfiar de las webs sin https ni certificados digitales y, en caso de tenerlo, comprobar que se trata de la web que dice ser. En el caso de los Email utilizar una firma digital o cifrado a la hora de enviar Emails nos permitirá autenticar los mensajes y prevenir suplantaciones. Si la organización con la que nos comunicamos dispone de firma digital, también será más sencillo identificar este tipo de ataques. Finalmente, analizando el contenido como si de un phishing se tratase, bastará para identificar el engaño.

Ataques DDOS

DDoS son las siglas en inglés de “Ataque distribuido denegación de servicio” y consiste en atacar un servidor web al mismo tiempo desde muchos equipos diferentes para que deje de funcionar al no poder soportar tantas peticiones, la propagación se lleva a cabo a partir de otro tipo de ataques con los que infectar dispositivos e ir aumentando la potencia del ataque. Las consecuencias son una pérdida de reputación, suspensión del servicio, así como

pérdidas económicas, además de las consecuencias de una brecha en su seguridad, como el robo de datos.

Las técnicas de protección contra este tipo de ataque:

- Monitorización continua: Existen herramientas para analizar la actividad del sitio web y detectar posibles ataques DDOS antes de que se conviertan en un problema. El firewall puede ayudarnos a detectar posibles intrusos o una actividad fuera de lo normal.
- Proveedor fiable: Elegir un proveedor que nos ofrezca garantías, como un servicio de prevención o una infraestructura sólida para aguantar un intento de ataque.
- Actualizaciones: Las actualizaciones de seguridad nos protegerán de posibles vulnerabilidades en el software.
- Conexión sólida: Un buen ancho de banda nos ayudará a reducir los efectos de un ataque DDOS y a reponernos antes.
- Reducir la superficie afectada: Una solución muy útil es limitar la infraestructura de nuestro servicio web que pueda ser atacada, por ejemplo, redirigiendo el tráfico directo de Internet. Fuente: (Instituto Nacional de Ciberseguridad, 2019)

Escaneo de puertos

En esta técnica, conocida como escaneo de puertos, o portscan, es el proceso en el que se analiza automáticamente los puertos de una máquina conectada a la red con la finalidad de analizar los puertos e identificar cuáles están abiertos, cerrados o cuentan con algún protocolo de seguridad. Igual que los modelos anteriores busca el robo de credenciales de acceso, datos bancarios o de sistemas internos, pero también ofrecen una entrada para controlar dispositivos conectados a una red.

Como medida de protección, el router tiene el papel protagonista a la hora de proteger los sistemas de la mayoría de los ataques a las conexiones. Es fundamental configurar correctamente, controlar las conexiones entrantes y los dispositivos conectados por medio de un filtrado MAC, mantener el firewall activado y controlar los puertos que tenemos abiertos. Y, como cualquier dispositivo, mantenerlo actualizado para protegerlo de posibles brechas de seguridad.

Defensa y seguridad en red

Con base en los puntos anteriores puede determinarse con precisión que uno de los elementos a proteger de vulnerabilidades es la red de datos de la organización, en este caso deben considerarse aspectos relevantes para la implementación de medidas de seguridad tales como la segmentación de redes (administrativa, datos, servicios, usuarios [correo, aplicaciones, notificaciones]), implementar proxies de comunicaciones, firewalls, sistemas de detección y prevención de intrusiones, esquemas de autenticación adecuados a la organización, entre otros, los cuales son requeridos para formar capas más externas respecto a los servidores, estaciones de trabajo y dispositivos de cómputo en general según

la infraestructura y arquitectura de servicios de la empresa. Además, acorde con lo que nos señala Romero Castro y otros *"no se debe delegar toda la defensa de los equipos a la protección perimetral, porque si se viese superada nada protegería a los equipos, es decir siempre se debe defender a distintos niveles de profundidad como se decía por capas, en resumen, en la seguridad de la red se basa en los siguientes puntos:*

- *Segmentación de redes*
- *Proxies*
- *Firewalls*
- *IDS e IPS"* (Romero Castro, y otros, 2018)

Todas las medidas de seguridad que se puedan aplicar son de suma relevancia sobre todo cuando la empresa u organización tiene alta dependencia de la red de comunicaciones como punto de acceso a aplicaciones y servicios de tecnología, tanto para la comunicación con los clientes como para el soporte de procesos internos y negocios electrónicos.

Teléfonos

Durante los análisis de riesgos y seguridad es importante verificar cómo la incorporación nuevos dispositivos a Internet, desde computadoras a teléfonos móviles, tablets, pockets, POS, y todos los aparatos comprendidos dentro del paradigma del Internet de las Cosas o IoT (Internet of Things por sus siglas en inglés), hace que los ataques y vulnerabilidades se aumenten y que ataques hacia estos dispositivos se realicen cada vez más o se intentan cada vez más buscando vulnerar los dispositivos mediante programas maliciosos y obtener con esto información personal e incluso empresarial.

Por tanto, se señala que debemos tomar en cuenta estos dispositivos de la misma forma y con las mismas medidas que analizamos PC o equipos portátiles, aunque considerando dos factores como lo son:

1. Los dispositivos móviles no contienen información crítica ni aplicaciones tan complejas aún, sin embargo, la computación en la nube está haciendo que se cierren las brechas.
2. Estos dispositivos son más sencillos de robar, por lo cual hay que considerar mecanismos de seguridad específicos, algunos ya incorporados como borrado remoto de información o bloqueo por intentos repetitivos de violentar el acceso.

Asociado al punto 2., otro aspecto de evaluación y establecimiento de políticas claras asociadas al uso de dispositivos móviles es que, en caso de robo, el terminal podría mantener registro de todos los datos de un empleado, que luego pueden ser usados en contra de la organización ya que estos terminales en la actualidad suelen contener números de teléfono internos de la empresa, datos sobre la empresa y en los casos más extremos, aplicaciones que contengan passwords de acceso a los sistemas o acceso pregrabados.

Por tanto, las políticas de la empresa deben solicitar a los empleados por norma, el no mantener datos importantes en este tipo de dispositivos, sobre todo passwords de acceso, y requerir también, por normativa que en caso de robo o pérdida se realice un informe donde

se indique que datos susceptibles de ser usados para hacking social o informático y que pudieran estar contenidos en el dispositivo. En la actualidad se han desarrollado mejoras al rendimiento de los algoritmos AES para su utilización en teléfonos móviles cerrando también las brechas de seguridad de estos dispositivos. Esta inclusión de los dispositivos móviles en la ecuación de seguridad de la información, requiere el estudio e incorporación un nuevo y amplio abanico de estrategias ofensivas, visto desde los intereses de una empresa, se vuelve estratégico el rol de la seguridad informática en la protección de los dispositivos y las redes que contengan información confidencial o sensible frente a los ataques de malware.

Guerra electrónica y de información

Tal cual se ha expuesto en los puntos anteriores, un elemento importante que debemos establecer es el contacto hacia las personas, lo cual también hace posible aplicar ataques por ingeniería social dirigidos a la persona, mediante mensajes de texto, texto sobre aplicaciones de mensajería y mediante llamadas telefónicas, en este sentido los ataques más usuales se conocen como: phishing, vhising y smishing. Sin embargo, también pueden ser utilizados para la creación de noticias falsas, expectativas empresariales e incluso para desestabilizar un gobierno mediante noticias falsas.

Phishing, Vhising y Smishing

- Son tres tipos de ataques basados en ingeniería social, muy similares en su ejecución dado su contacto con la persona que utiliza el dispositivo o que atiende el teléfono, en este escenario el ciberdelincuente enviará un mensaje suplantando a una entidad legítima, como puede ser un banco, una red social, un servicio técnico o una entidad pública, con la que nos sintamos confiados, para lograr su objetivo. Estos mensajes suelen ser de carácter urgente o atractivo, y muy acoplados a la realidad de cada país o al entorno social, para evitar que apliquen el sentido común y las personas víctimas piensen dos veces.
- Por su definición:
    - Phishing: Suele emplearse el correo electrónico, redes sociales o aplicaciones de mensajería instantánea.
    - Vhising: Se lleva a cabo mediante llamadas de teléfono.
    - Smishing: El canal utilizado son los SMS.
- Estos mecanismos buscan generar confusión y brindan enlaces sitios web fraudulentos, suplantando o bien fingiendo ser un enlace legítimo, o bien se trata de un archivo adjunto malicioso para infectarnos con malware. Cuando se trata de un ataque dirigido a una persona en concreto, se conoce como Spear phishing. Esta modalidad centra en una persona específica las técnicas de manipulación, recabando

información sobre ella previamente para maximizar las probabilidades de éxito a la hora de hacerse con su información o dinero.

- En estos casos el principal medio de propagación es el correo electrónico o email donde, fingiendo ser una entidad de confianza, el atacante lanza un cebo, que suele ser un mensaje urgente o una promoción muy atractiva, para motivarnos a hacer clic en el enlace o archivo adjunto, o a compartir los datos que el atacante pide en su mensaje. Siendo su objetivo es obtener datos personales y/o bancarios de los usuarios, haciéndonos creer que los estamos compartido con alguien de confianza. También pueden utilizar esta técnica para que sea descargado malware con el que infectar y/o tomar control del dispositivo.

EL PRINCIPAL CONSEJO ES SER PRECAVIDO Y LEER EL MENSAJE DETENIDAMENTE, ESPECIALMENTE SI SE TRATA DE ENTIDADES CON PETICIONES URGENTES, PROMOCIONES O CHOLLOS DEMASIADO ATRACTIVOS. ADEMÁS, OTRAS PAUTAS QUE PODEMOS SEGUIR PARA EVITAR SER VÍCTIMA DE UN PHISHING SON:

- DETECTAR ERRORES GRAMATICALES EN EL MENSAJE. Y, SI SE TRATA DE UN ASUNTO URGENTE O ACERCA DE UNA PROMOCIÓN MUY ATRACTIVA, ES MUY PROBABLE QUE SE TRATE DE UN FRAUDE.
- REVISAR QUE EL ENLACE COINCIDE CON LA DIRECCIÓN A LA QUE APUNTA. Y, EN CUALQUIER CASO, DEBEMOS INGRESAR LA URL NOSOTROS DIRECTAMENTE EN EL NAVEGADOR, SIN COPIAR Y PEGAR.
- COMPROBAR EL REMITENTE DEL MENSAJE, O ASEGURARNOS DE QUE SE TRATA DE UN TELÉFONO LEGÍTIMO.
- NO DESCARGAR NINGÚN ARCHIVO ADJUNTO Y ANALIZARLO PREVIAMENTE CON EL ANTIVIRUS. EN CASO DE VISHING, NO DEBEMOS DESCARGAR NINGÚN ARCHIVO QUE NOS HAYA SOLICITADO EL ATACANTE, NI CEDER EL CONTROL DE NUESTRO EQUIPO POR MEDIO DE ALGÚN SOFTWARE DE CONTROL REMOTO.
- NO CONTESTAR NUNCA AL MENSAJE Y ELIMINARLO. (Instituto Nacional de Ciberseguridad, 2019)

Acorde con la revista SAAB en foco, América Latina, sobre **Guerra Electrónica** nos señala que:

- *“Las operaciones militares se ejecutan en un entorno electromagnético cada vez más complejo: el espacio de maniobras operativas y el dominio de guerra de Guerra Electrónica (EW por sus siglas en inglés). El propósito de EW es, por lo tanto, usar y controlar el espectro electromagnético -señales como la radio, el infrarrojo o el radar- para detectar, proteger y comunicarse en apoyo de las operaciones militares. Al mismo tiempo, puede usarse para evitar que los enemigos interrumpan o utilicen estas señales. EW se puede aplicar desde el aire, el mar, la tierra y el espacio, y actúa sobre sistemas de comunicación y de radares. Implica el uso de la energía electromagnética para proporcionar una mejor comprensión del entorno operativo y para lograr efectos específicos en el campo de batalla moderno.*
- *La guerra electrónica se puede dividir en tres grandes grupos:*
    1. *Las **Medidas de Soporte Electrónico (ESM)** buscan detectar, interceptar, identificar, ubicar, registrar y/o analizar fuentes de energía electromagnética radiada, para el reconocimiento inmediato de amenazas o la planificación*

operacional a largo plazo. ESM ayudaría a las tropas, por ejemplo, a saber, si un radar de control de fuego se ha bloqueado en un vehículo de combate, barco o avión. El Soporte Electrónico proporciona información requerida para la decisión que involucra Protección Electrónica (EP), Ataque Electrónico (EA) otras fuerzas tácticas. Los datos de soporte electrónico se pueden usar para producir inteligencia de señales (SIGINT) e inteligencia de comunicaciones (COMINT). Las medidas de soporte electrónico recopilan inteligencia a través de la escucha pasiva de las radiaciones electromagnéticas. Esto proporciona detección inicial o conocimiento de sistemas extranjeros, a partir de los cuales se puede desarrollar una biblioteca de datos técnicos y operativos, e información táctica de combate utilizando esa biblioteca. Las plataformas de recolección de ESM pueden permanecer electrónicamente silenciosas, y detectar y analizar transmisiones de radar más allá del rango de detección debido a la mayor potencia del pulso electromagnético transmitido con respecto a un eco reflejado de ese pulso.

2. *Las **Medidas de Ataque Electrónico (EAM)**, también conocidas como contramedidas electrónicas (ECMI, involucran el uso de energía electromagnética para atacar sistemas de radar y afectar negativamente su desempeño y/o capacidad, para engañar al radar, el sonar y otros sistemas de detección como infrarrojos o láser. EAM puede usarse tanto ofensivamente como defensivamente para evitar ser objetivo de un enemigo. El sistema puede hacer que aparezcan muchos objetivos separados para el enemigo, o que el objetivo real desaparezca o se mueva de forma aleatoria. Se usa eficazmente para proteger aeronaves de misiles guiados. La mayoría de las fuerzas aéreas usan EAM para proteger sus aviones contra ataques. También ha sido desplegado en buques militares y recientemente en algunos tanques avanzados para engañar a misiles guiados por láser o IR. Un ejemplo de ECM ofensivas, ampliamente utilizado, es el jamming.*

3. *Las **Medidas de Protección Electrónica (EPM)**, también conocidas como contra-contramedidas electrónicas, tienen el propósito de proteger los activos de cualquier efecto de uso del espectro electromagnético que pueda degradar, neutralizar o destruir la capacidad de combate. En la práctica, EPM a menudo significa resistencia al jamming.*

4. *IDAS & CIDAS. El sistema de defensa propia para plataformas aéreas significa saber si alguien me está observando o si me está convirtiendo en un objetivo. Eso requiere hacer un seguimiento de cada tipo de señal que hay. La familia de sistemas de guerra electrónica IDAS / CIDAS. IDAS (Integrated Defensive Aids Suite), y la versión más compacta CIDAS, son un conjunto de sistemas avanzados que están diseñados para proporcionar protección a aviones y helicópteros contra MANPADS y misiles SAM. CIDAS es la variante pequeña y liviana con solo sensores electroópticos y un controlador más pequeño. Se puede configurar para advertencia láser y advertencia de aproximación de misiles. El sistema está completamente integrado con el sistema de*

> *dispensación de contramedidas ligeras. Por otro lado, IDAS, puede configurarse para ser el sistema de alto nivel con alerta laser, alerta de aproximación de misil, y un radar con capacidad de detección multiespectral. El sistema está completamente integrado con el dispensador de contramedidas"* (Bo, 2018)

Como puede observarse los dispositivos electrónicos y la seguridad de la información abarca también ámbitos externos al ambiente de las organizaciones y, por tanto, su estudio puede ampliarse a ámbitos empresariales, de gobierno, de seguridad nacional e incluso hasta aspectos militares, de esto existe mucha información sobre la que se puede profundizar.

Copyright y DRM

En principio las definiciones de Copyright y DRM (Digital Rights Management) son las siguientes:

- Copyright o derechos de autor, es, según la Real Academia Española: el "derecho que la ley reconoce al autor de una obra intelectual o artística para autorizar su reproducción y participar en los beneficios que esta genere." (Real Academia Española, 2021)
- DRM o Gestión de Derechos Digitales, se trata de una serie de tecnologías de protección aplicadas por las empresas que distribuyen contenidos digitales.

En referencia al tema Juan C. Calvi nos indica que en las últimas décadas los grandes grupos de empresas que controlan los sectores de producción y distribución de productos culturales tales como libros, discos, revistas, films, programas de radio y televisión, denominados grupos multimedia han constituido en el motor del proceso de expansión y globalización de la economía de mercado y el desarrollo económico de estos productos.

- *"El objetivo fundamental de este proceso de concentración fue posibilitar la explotación a escala mundial de amplias carteras de derechos (copyrights) sobre todo tipo de productos audiovisuales tales como discos, films, programas de televisión y vídeos, a través de múltiples medios y canales, tales como las redes de televisión por cable, satélite y digital terrestre, las redes de telecomunicaciones e Internet, y a través de nuevos soportes digitales como CD y DVD.*
- *No obstante, este complejo proceso, como todo proceso histórico, presenta diversas contradicciones. Por un lado, el desarrollo de nuevas tecnologías y redes digitales y su penetración creciente en los mercados domésticos es aprovechado por los grupos multimedia como nuevas redes, mercado de distribución y consumo de sus productos. Por otro, la penetración en los mercados domésticos de estas nuevas tecnologías digitales de reproducción y distribución de productos tales como las grabadoras de CD y DVD, los reproductores MP3, Internet y los sistemas denominados Peer to Peer (P2P), permiten, de una manera creciente, reproducir y distribuir «libremente» todo tipo de productos protegidos con copyright. En este sentido, como se sabe, los grupos multimedia han basado su poder de mercado en el monopolio de la reproducción, distribución y explotación comercial de un producto determinado, esto es, detentando*

el derecho exclusivo de su copyright. Y, en este contexto, vemos que ese derecho exclusivo está siendo seriamente cuestionado." (Calvi, 2005)

Es claro que las nuevas tecnologías, redes digitales, aplicaciones multiplataforma, por un lado, y los usos sociales que éstas permiten desarrollar, por otro, están cuestionando el derecho exclusivo de reproducción y distribución que los grupos multimedia intentan ejercer sobre la producción cultural. Aplicaciones como Spotify, Last.fm, Soundcloud, Shark music, Deezer, Youtube Music, a efectos del curso, es requerido conocer que se requieren establecer dos aspectos fundamentales:

1. El registro de derechos de la información, producción audiovisual, sistemas de información, apps, códigos fuentes, y todos aquellos aspectos que requieran el establecimiento de una propiedad intelectual de la organización.
2. Deben existir políticas claras para la adquisición y tenencia de contenido audiovisual, aplicaciones licenciadas o con derechos de autor, imágenes, audios, y otros para asegurar que las producciones internas cumplas con las regulaciones.

Esto mismo aplica para los licenciamientos llamados DRM (Digital Rights Management), ya que en ocasiones se comete el error de no verificar si las licencias gratuitas o las denominadas open source, software libre, también aplican para ambientes empresariales, lo cual es un concepto erróneo por cuanto el uso de licenciamiento, software libre y similares en aplicaciones para explotación comercial no es permitido, para esto por lo general el lucro implica un pago de licencia. Sobre estas implicaciones podemos mencionar:

1) Legislativa: a través de leyes como la Ley de Derechos de Autor o su versión europea: Directiva Europea para la Propiedad Intelectual (European Union Copyright Directive, EUCD, 2001), las cuales criminalizan el uso y el desarrollo de sistemas informáticos que infrinjan el copyright.
2) Tecnológica: a través de plataformas informáticas seguras y sistemas de encriptación como la llamada Alianza para una Plataforma Informática Segura (Trusted Computing Platform Alliance, TCPA, 1999) y los Sistemas de Protección Digital del Copyright (Digital Right Management, DRM, 1999), destinados a impedir el acceso, la distribución, el intercambio o la reproducción libre de productos con copyright.
3) Judicial: por medio de demandas a las empresas y desarrolladores de sistemas que infringen el copyright de los productos, a los proveedores de acceso a Internet y a los usuarios que los utilizan.

Haciendo balance

Conforme lo analizado, una organización puede desenfocar sus esfuerzos por la multiplicidad de dimensiones que debe cubrir en lo referente a las amenazas y vulnerabilidades de seguridad de la información, elementos técnicos a cubrir en la infraestructura y servicios de TI, posibilidad de intrusiones, virus, malware, seguridad en la red, phishing y técnicas de ingeniería social, entre otros elementos.

Sobre estos aspectos Baca Urbina nos señala que, una vez identificados los elementos de seguridad por cubrir y establecidas las alternativas *"sobre todo de tipo tecnológico, derivadas de las respuestas a éstas, el siguiente paso es determinar el costo de cada alternativa. Pero aquí no se trata de seleccionar la de menor costo, sino de hacer un balance entre el costo de la alternativa contra la protección que proporcionaría, lo cual depende del tipo de empresa."* (Baca Urbina, 2016)

Por lo tanto, el plan de seguridad debe incorporar estos elementos para garantizar que durante la identificación de riesgos y amenazas y la selección de alternativas se presente el mejor balance entre costo-protección contra las amenazas, donde el valor del activo para la empresa debe sopesarse para la implementación de contramedidas.

Otra recomendación es la segregación de funciones y la distribución de las funciones e implementación de normas en las distintas áreas de TI acorde con sus áreas de responsabilidad, por ejemplo, los departamentos de infraestructura deben aplicar las medidas y recomendaciones como parte de la administración de centros de datos e infraestructuras de almacenamiento, procesamiento, plataforma y respaldo, los expertos en comunicaciones deberán aplicar las medidas sobre los elementos de red, los departamentos de soporte sobre el entrenamiento y recomendaciones al usuario final, la áreas de desarrollo sobre las funciones y seguridad en la implementación de sistemas, entre otros, lo cual permite distribuir responsabilidades y cubrir mayores niveles de la arquitectura informática y el uso de los sistemas de información.

¿Vigilancia o privacidad?

Tal y como se ha planteado en los estudios anteriores los planes de seguridad y los sistemas de gestión de seguridad informática plantean a la organización acciones, salvaguardas y contramedidas que aportan una respuesta a las vulnerabilidades y amenazas de seguridad informática problema, proponiendo dentro de sus múltiples niveles el establecimiento de una arquitectura multinivel para cubrir distintos elementos dentro de la infraestructura y elementos que intervienen en la gestión de la información, desde capas físico lógicas donde se podrían incluir aspectos como la inclusión de sensores heterogéneos para detectar no sólo ataques tradicionales sino cambios en el contexto de la organización: modificaciones en pautas de uso de redes y sistemas, desviaciones de consumo eléctrico, incidentes de seguridad física y vídeo vigilancia, sensores ambientales, sensores de actividad en redes sociales, e incluso la caracterización de conflictividad laboral para anticipar posibles ataques internos de empleados descontentos, limitar el alcance del ataque lógico, mediante la implantación de un sistema de vigilancia de las cadenas estratégicas, muchos de estos elementos podrían llegar a considerarse al límite entre vigilancia y privacidad por parte de los funcionarios de una empresa, lo cual requiere el establecimiento de normativa y políticas de seguridad y conductuales adecuadas y acorde a los requerimientos de información y de la gestión de información empresarial.

En cuanto a la experiencia del país, Luis Paulino Mora señala en la Revista PROSIC, *"pueden citarse los siguientes delitos informáticos: violación de la privacidad, divulgación de material ilegal, sustracción de datos, modificación de los programas existentes o inserción*

de nuevos programas o rutinas (virus y gusanos), fraude bancario, espionaje informático e incluso ataques de naturaleza militar a las plataformas informáticas de un país (ciberguerra), etc." (Universidad de Costa Rica, 2010)

En este mismo análisis el autor nos señala*: "el tema de la invasión de la privacidad y manipulación de los datos personales en la red requiere la urgente atención de todos los sectores. Los usuarios deben tomar conciencia de que su vida y comportamiento están siendo estudiados para todo tipo de fines. Los dueños de los recursos invasivos deben entender que los límites son tan necesarios, como la información, y que el avasallamiento de los derechos de los usuarios puede terminar por volverse en su contra. Por eso me parece muy importante enfatizar en una publicación como la presente, -en la necesidad como democracia que somos-, en la obligación de garantizar el respeto a la seguridad e intimidad de los ciudadanos, valores que debemos sopesar siempre a la hora de desarrollar cualquier estrategia de lucha contra la criminalidad en cualquiera de sus formas."* (Universidad de Costa Rica, 2010)

En esta misma publicación Gabriela Barrantes nos señala sobre privacidad y seguridad:

- *"Este es un tema largo e importante, pero al menos debe quedar claro que ninguna conceptualización de la seguridad es completa sin tocar aspectos de protección de datos de los usuarios finales, y nuestro país tiene grandes lagunas legales y de concientización al respecto. Por ejemplo, el correo electrónico es totalmente "abierto" a menos que se cifre de punto a punto, pero muchos usuarios ignoran esto y lo usan como si fuera totalmente secreto con resultados a veces trágicos.*
- *Todos y todas debemos informarnos, informar a los demás, y mantenernos alertas sobre la tecnología que usamos, la protección de la que disponemos y sobre la visibilidad de nuestros datos en Internet."* (Universidad de Costa Rica, 2010)

Por último, Mavin Carvajal nos señala las siguientes conclusiones sobre ciberseguridad y privacidad:

- *"La implementación de reglas y procedimientos seguros en el acopio, almacenamiento y transferencia de datos personales repercute directamente en el respeto al derecho fundamental a la autodeterminación informativa.*
- *Podríamos concluir, a partir de lo que les he mencionado en estos minutos, que la implementación de normas y procedimientos seguros en el acopio, almacenamiento y transferencia de datos personales incide directamente en el respeto a un derecho de rango constitucional, como es el derecho a la autodeterminación informativa, reconocido por la Sala Constitucional en una muy basta doctrina jurisprudencial.*
- *Es sin duda alguna una preocupación que debe estar presente en aquellas bases de datos creadas para ofrecer informes al público, pero debe serlo en todas y cada uno de los ficheros que manejen información personal, puesto que de estas se alimentan las otras bases de datos para dar esos informes. Es decir, es una regla general del sistema que debemos tomar con el mismo cuidado que para administrar los fondos de una cuenta nuestra, con el mismo cuidado debe ser administrada la información personal que nos pertenezca y que obre en las bases de datos públicas y privadas.*

- *Esto es, sin duda alguna, un aspecto muy relevante de la autodeterminación informativa, un elemento muy relevante en la protección de datos que atañe a los derechos de la persona frente a este mundo tecnológico que avanza cada día más en ofrecernos nuevas alternativas de comunicación, nuevas alternativas de conectividad y por supuesto, nuevos riesgos de los cuales debemos protegernos con firmeza."* (Universidad de Costa Rica, 2010)

Conclusiones y recomendaciones

Se puede concluir a partir del estudio de las medidas de seguridad asociadas a las ingenierías de cifrado, ataques de red y defensas, teléfono y dispositivos móviles, guerra electrónica, derechos de autor, balances y privacidad, que los análisis de riesgos informáticos y la seguridad de la información son temas latentes, en alta demanda en las organizaciones que tan constantemente requieren migrar a modelos de negocios digitales en los cuales se requiere un abordaje consolidado e integral de los elementos de seguridad, estableciendo los planes de seguridad adecuados a la organización, a sus ingresos y a las prioridades definidas por el negocio, un abordaje escalonado e incremental suele ser una de las estrategias más exitosas que pueden aplicarse.

Adicionalmente es importante evaluar algunas tendencias del mercado y de la seguridad de la información que pueden ser aplicadas con éxito en las organizaciones y cuyos niveles de madurez están en crecimiento, tecnologías y técnicas tales como:

- Machine Learning
- Threat intelligence
- Analíticas de seguridad
- Automatización de tareas de seguridad
- Consolidación de consolas y dashboards de seguridad

Para mejorar los conceptos y tendencias podemos ampliar revisando lo siguiente:

- https://www.secureit.es/la-ciberseguridad-en-2019-balance-de-la-situacion-y-tendencias/
- Lectura 1 sobre el estándar del Gobierno Norteamericano NIST800-30.
- Lectura 2 sobre el modelo nacional de riesgo de seguridad del Gobierno de Colombia
- La guía de ciberataques de la Oficina de Seguridad del Internauta del Gobierno de España
- Referente Pensamiento Eje 3. ANÁLISIS DE RIESGOS INFORMÁTICOS. Pongamos en práctica

Referencias bibliográficas

- Alfaro Campos, J. C. (2017). *Metodología para la gestión de riesgos de TI basada en COBIT 5.* Cartago, Costa Rica: Instituto Tecnológico de Costa Rica.
- Baca Urbina, G. (2016). *Introducción a la Seguridad Informática* (Primera ed.). México: Grupo Editorial Patria. Obtenido de https://elibro.net/es/ereader/usanmarcos/40458
- Bo, T. (2018). Guerra electrónica. *SAAB EN FOCO. AMERICA LATINA*, 6-15. Obtenido de https://www.saab.com/globalassets/markets/colombia/saab-en-foco/saab-en-foco-2018-2.pdf
- Business Intelligent Limitada. (15 de Enero de 2020). *https://www.solucionesalnegocio.com/.* Obtenido de http://www.business-intelligent.com/cibercomercio.pdf
- Calvi, J. C. (2005). El copyright en la era digital. Nuevas estrategias de control y explotación de productos audiovisuales en Internet. *Anàlisi 32*, 25-31.
- CERT DE SEGURIDAD E INDUSTRIA. (2016). *ENSI_ARLI-CIB_01- Modelo de Análisis de Riesgos Ligero de Ciberseguridad en Sistemas de Control Industrial (ARLI-CIB).* España: Gobierno de España. Obtenido de https://www.incibe-cert.es/sites/default/files/paginas/publicaciones/ensi/ensi_arli-cib_01_metodologia-aarr_borrador.pdf
- Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT Versión 3.0. Metodología de análisis y gestión de riesgo de los sistemas de información.* Madrid: Gobierno de España.
- Editorial IT NOW. (29 de Abril de 2019). *Revista IT NOW.* Obtenido de https://revistaitnow.com/5-maneras-de-proteger-la-ciberseguridad-de-su-empresa/
- Garbarino Alberti, H. (2014). *Marco de Gobernanza de TI para empresas PyMEs - SMEsITGF.* Madrid: Universidad Politécnica Madrid.
- Instituto Nacional de Ciberseguridad. (2019). *Guía de Ciberataques.* Gobierno de España.
- ISACA IT RISK. (2009). *Marco de Riesgos de TI.* Estados Unidos de América: ISACA.
- ISACA®. (2012). *Cobit 5. Procesos Catalizadores.* Estados Unidos: ISACA.
- LaRepublica.Net. (20 de 02 de 2020). *LaRepublica.net*. Obtenido de https://www.larepublica.net/noticia/costa-rica-registro-casi-32-millones-de-intentos-de-ciberataques-en-primeros-tres-meses
- López, L. F. (2018). *Análisis de riesgos informáticos. Eje 1. Conceptualicemos.* Fundación Universitaria del Área Andina.
- Madrigal Chaves, W. (2019). *SUWA Universidad San Marcos, Repositorio.* Obtenido

de http://repositorio.usam.ac.cr/xmlui/

- Real Academia Española. (01 de 03 de 2021). *Diccionario de la Lengua Española*. Obtenido de https://dle.rae.es/
- Red Global de Conocimientos en Auditoría y Control Interno. (01 de 01 de 2021). *www.Auditool.com*. Obtenido de https://www.auditool.org/blog/auditoria-de-ti/3423-que-es-un-ciberataque
- Romero Castro, M. I., Figueroa Moran, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Alcoy - Alicante, España: Editorial Área de Innovación y Desarrollo,S.L. doi:http://dx.doi.org/10.17993/IngyTec.2018.46
- UNICEM. (22 de 12 de 2020). *El Modelo OSI*. Obtenido de http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf
- Universidad de Costa Rica. (2010). Ciberseguridad en Costa Rica. *PROSIC Programa Sociedad de la Información y Conocimiento*, 23-100.

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica