POPULAR BANK

Guía de seguridad de la información
Pistas de Seguridad

GLOSARIO

ANCHO DE BANDA:
Se refiere a la cantidad de datos que se pueden transferir entre dos puntos de una red en un tiempo específico. Normalmente, el ancho de banda se mide en bits por segundo (bps) y se expresa como una tasa de bits; denota la capacidad de transmisión de una conexión y es un factor importante al determinar la calidad y la velocidad de una red.

AUTENTICACIÓN:
La autenticación es el proceso de detectar y comprobar la identidad de un usuario mediante la validación de las credenciales (usuario y contraseña, y consultando a una autoridad determinada).

AUTENTIFICACIÓN BIDIRECCIONAL:
Se refiere al proceso de reconocimiento automático y simultáneo que se efectúa entre un sistema y el usuario, a través de un dispositivo con microprocesador integrado. Es útil para legitimar las partes involucradas en transacciones de canales remotos.

BACK DOOR:
Programas maliciosos diseñados con la intención de abrir una puerta secreta “puerta trasera” en las computadoras, con la finalidad de permitirle al creador de este programa, acceder a estas sin ser detectado.

BLUE JACKING:
Es una técnica consistente en enviar información no solicitada entre dispositivos utilizando el Bluetooth. Por ejemplo, computadoras portátiles, tabletas o teléfonos móviles. Normalmente un bluejacker sólo envía mensajes de texto, aunque a través de los teléfonos inteligentes es posible enviar, también, imágenes, sonido y archivos. No intercepta información, pero sí puede ocasionar daños al sistema del dispositivo.

BOTNET:
Abreviatura de robot network o red robotizada, también se la conoce como ejército zombi. Se refiere a la red de computadoras conectadas a las internet vulnerables y sin ninguna protección, que son controladas remotamente por los spammers con el objeto de programarlas para enviar millones de correos electrónicos.

Después de escanear la internet y encontrar computadoras vulnerables, los *spammers* les instalan programas maliciosos (*malware*) o engañan al usuario para que descargue música o juegos gratuitamente.

BIT:
Contracción del término anglosajón dígito binario (*binary digit*), es la unidad básica de información para computadoras y telecomunicaciones; es la cantidad de información almacenada por un dispositivo digital o sistema físico que existe en uno de dos estadios posibles como serían, por ejemplo, dos niveles de corriente o de intensidad de la electricidad, dos posiciones en un interruptor, dos direcciones de polaridad, etc.
En el entorno de las computadoras, un bit es la variable con dos condiciones que, frecuentemente, se interpretan como dígitos binarios 0 y 1, la dualidad lógica Verdadero/ Falso, los signos algebraicos +/−, los modos de activación (encendido/apagado), entre otros.

BYTE:
En el entorno de las computadoras y las telecomunicaciones, es la unidad de información digital compuesta por ocho (8) bits. De ahí se desprenden kilobyte, megabyte, terabytes o petabit. Fue acuñado por el Dr. Werner Buchholz, durante la fase de diseño de la computadora IBM Strech, en julio de 1956.

CACHÉ:
Memoria temporal de las computadoras. Es la que sirve para almacenar la información suspendida antes de ejecutar cualquier acción definitiva con respecto a ella como, por ejemplo, cortar y pegar datos de un lugar a otro. Es la que almacena la secuencia de pasos previos que un usuario ha realizado en cualquiera programa y que se revierte con sólo pulsar la flecha o botón de deshacer (“*undo*”).

CADENA DE MENSAJES:
Son mensajes de correo electrónico en los que incentiva a reenviar dicho mensaje a más receptores para que éstos a su vez también lo reenvíen. Es una de las posibles fuentes de saturación del servicio con el correo electrónico, ya que a menudo llevan noticias falsas, pueden contener programas maliciosos, etc.

CERTIFICADO DIGITAL:
Es una firma autorizada que identifica una entidad válida. Estos son emitidos por entidades certificadoras, los cuales son utilizados para autenticar una entidad o personas. La seguridad del certificado está protegida por técnicas criptográficas del más alto nivel.

CIFRADO:
Codificación de datos mediante varias técnicas matemáticas que garantizan su confidencialidad y la integridad de la información durante el proceso de transmisión y almacenamiento.

CÓDIGO MALICIOSO:
Cualquier programa que se instala con intención de ocasionar daños o de robar información. Generalmente están diseñados para ejecutarse sin la intervención ni el consentimiento del usuario.

CONTRASEÑA O CLAVE SECRETA:
Conjunto de letras, números y símbolos utilizados para autenticar usuarios en un sistema informático. Para que sea efectiva, las mejores prácticas recomiendan componerla de forma tal que sea robusta y difícil de descifrar. Por ejemplo:
Nombre común –» Pez payaso
Nombre científico –» Amphiprion akallopisos
Contraseña fuerte –» @mph1pr10n@k@110p1505
(sustituye la letra “a” por @, la “i” por 1 y la “s” por 5)

COMPROMETIMIENTO DE DATOS (*DATA COMPROMISE*):
Se refiere al robo organizado de información de cajeros automáticos, tarjetas de débito o crédito principalmente de comercios, al detectar y aprovechar debilidades en los sistemas del comercio y de subcontratistas procesadores, o computadoras, dispositivos de almacenamiento o espionaje industrial fomentado por terceros.

COOKIES (GALLETAS):
Son pequeños ficheros de datos que el servidor de una página en Internet envía a la computadora que le visita, a través del navegador, y recupera posteriormente en cada nueva conexión. Éstos se almacenan en el disco duro de la computadora o del celular del internauta y permiten a la PER recuperar las características y/o preferencias de navegación de la sesión anterior.
Las que utiliza El Popular no son invasoras, malévolas ni nocivas y no recogen datos de índole personal. Sin embargo, si usted quiere, puede desactivarlas siguiendo las instrucciones del navegador. También puede eliminar de forma permanente las que tenga almacenadas en su computadora, o celular, accediendo al directorio correspondiente y seleccionando las opciones que la eliminan o no permiten su almacenamiento.

CORREO ELECTRÓNICO:
Escrito también Correos electrónico, es el sistema de comunicación personal por computadora vía las redes informáticas. A través de él se puede enviar, no solamente texto, sino todo tipo de documentos digitales.

CRACKER:
Abreviación del término en inglés criminal hacker, se refiere a una persona que usa su vasto conocimiento sobre sistemas, redes y computadoras, para lucrarse personalmente, irrumpiendo sin autorización en los sistemas de información de empresas, con el objetivo de evadir los sistemas de seguridad y destruir, exponer o sustraer su información.

CRIPTOGRAFÍA:
Disciplina que se ocupa de la seguridad de la transmisión electrónica y almacenamiento de la información.

DDOS:
Siglas para "*distributed denial of service*" o denegación del servicio. Consiste en el envío masivo, y simultáneo, de peticiones a los sistemas para bloquear o saturar el funcionamiento de los equipos e incapacitarlos para prestar el debido servicio a los usuarios.

DISPOSITIVO POS:
Aparato mediante el cual las transacciones de ventas pueden ser debitadas directamente a la cuenta bancaria o tarjeta de crédito de un cliente.
Se encuentran instalados en todos los establecimientos comerciales físicos y, a través de ellos, el comercio desliza las tarjetas de crédito y/o débito al momento de realizar un pago.
En el despliegue virtual, la salida de caja se realiza pidiéndole al internauta que digite los datos correspondientes a la dirección donde se remiten los estados de su tarjeta de crédito.

ENCRIPTACIÓN:
El proceso que convierte sus datos en un código cifrado antes de enviarlo a través de la Internet, previniendo a usuarios desautorizados su posterior lectura.

EXTENSIONES:
Se refiere a las últimas tres (3) letras después del punto en el nombre completo de un archivo. Son normalmente usadas por el sistema operativo para asociar ese archivo a un programa particular. Así, para:
Los documentos MS-Word la extensión es .doc o .docx,
Las hojas electrónicas MS-Excel con .wrk o .xls y
Las presentaciones MS-Powerpoint con .ppt o .pps

FILTRADO DE CONTENIDOS:
Son tecnologías que permiten establecer qué contenido se permite mostrar a un usuario cuando está navegando en la internet. También se aplica al filtrado de correos electrónicos con lo cual se evita la entrada de correos considerados no adecuados (spam, virus, material no ético, etc.)

FIRMA ELECTRÓNICA:
Información digital asociada a una operación en particular realizada en la Internet que, junto con los certificados, permite garantizar la identidad de los participantes en una transacción.

GUSANO (WORM):
Es un tipo de programa malicioso (*malware*), que tiene la capacidad de reproducirse a sí mismo y cuya función principal es causar denegación de servicio. Este tipo de programa, cuando se reproduce, utiliza espacio del disco y disminuye la velocidad de procesamiento del equipo.

HACKER:
Persona que tiene conocimientos de informática, a veces muy profundos, cuyo único objetivo es destacar su destreza para lograr infiltrarse en las redes de las empresas y pasar desapercibido por los filtros de seguridad, para acceder a sus sistemas de información.

HOAX:
Es un intento de hacer creer a un grupo de personas que algo falso es real. Es utilizado muy comúnmente enviando correos masivos.

INGENIERÍA SOCIAL:
Técnicas que intentan atacar la seguridad de los sistemas informáticos engañando a sus usuarios y a sus administradores utilizando la persuasión o utilizando una identidad falsa con la finalidad de obtener informaciones confidenciales.

INTERNAUTA:
Persona que accede a la Internet a través de una computadora con servicio de conexión y un programa de navegación, también conocido como navegador.

INTRUSIÓN:
Ataque informático en el cual el atacante obtiene un control completo sobre el equipo.
Durante una intrusión, el atacante puede obtener y alterar todos los datos del equipo, modificar su funcionamiento e incluso atacar nuevos equipos.

PER
Siglas para página o páginas en red, o en Internet; término castellano para definir web Page, web, website o site según la Fundación para un Español Urgente (*Fundeu*).

PARED DE FUEGO (*FIREWALL*):
Equipo o sistema de seguridad que permite controlar a qué equipos y a cuáles servicios se puede acceder dentro de una red. Puede tratarse de un equipo especializado de seguridad o de un programa instalado en un computador (*firewall personal*).

PIN (*PRIVATE IDENTIFICATION NUMBER*):
Números de identificación privado, por sus siglas en inglés.

PLUG-IN:
Módulo de programación que añade una funcionalidad específica al navegador de Internet. Los más comunes, por ejemplo, en formato Flash o HTML5, permiten visualizar videos o escuchar música.

PROGRAMA ANTI-ESPÍA:
Es un programa especializado, diseñado para proteger su computadora de ataques e instalación automática no autorizada de aplicaciones que recopilan y reenvían su información personal.

PROGRAMA ANTI-VIRUS:
Es un programa diseñado para detectar y prevenir la entrada de algún programa malicioso (*malware*) al computador, su posible esparcimiento e infección de otros computadores conectados en la misma red. Los programas maliciosos (*malware*), pueden propagarse rápidamente; por lo cual, usted deberá garantizar que su antivirus esté funcionando de modo regular y actualizado.

ROBO DE IDENTIDAD (*IDENTITY THEFT*):
Fraude que se perpetra usando los datos de otra persona sin su consentimiento, para comprometer servicios o establecer una nueva relación.

Algunos signos que le alertarán sobre posible robo de identidad son el que usted:

- Deje de recibir su estado de tarjeta(s) o cuenta(s),
- Reciba denegación de crédito sin ningún motivo,
- Tenga información inexacta en su reporte de crédito,
- Reciba aviso de cuentas abiertas, o deudas contraídas, sin pedirlas,
- Reciba tarjetas de crédito que usted no solicitó.

Minimice los riesgos de sufrir robo de su identidad:

- Revise regularmente los cargos en su(s) cuenta(s) o tarjeta(s) de crédito,
- Notifíquenos cualquier actividad sospechosa que usted detecte en su(s) cuenta(s) o tarjeta(s) de crédito a nuestras líneas de servicio al cliente: República Dominicana (809) 544-6970
- Panamá (507) 297-4100 Ext.:29935
- Escribiéndonos a las siguientes cuentas de correo electrónico: contactenos@popularbank.com.pa
- Reclame oportunamente cualesquier cargos que usted no reconozca haber realizado,
- Cierre su(s) cuenta(s) o tarjeta(s) de crédito si usted sospecha que ha sido vulnerada o expuesta.

RUPTURA DE LA PRIVACIDAD (*PRIVACY EVENT/BREACH*):
La ruptura de la privacidad es una situación en la cual la información sensible que controla Popular Bank Ltd. Inc. (o un tercero actuando a su nombre) se extravía, mal usa o divulga a terceras partes sin la debida autorización. La información podrá estar en cualquier forma, incluido papel impreso o cualquier formato electrónico o, bien, datos cifrados. La ruptura puede ocurrir dentro de la entidad financiera o en un proveedor que opere a su nombre.

SERVIDOR INTERMEDIARIO (*PROXY*):
Sistema informático cuya misión es hacer de intermediario entre un sistema y otro a través de Internet. Entre las misiones de un servidor intermediario están la de acelerar su acceso a la internet, filtrar los contenidos a los que se ha accedido y proteger los sistemas evitando su comunicación directa.

SPAMMER:
Persona que se dedica a enviar correos electrónicos con publicidad no solicitada por los usuarios.

SSL:
O “Secure Socket Layer” por sus siglas en inglés, significa Capas de Conexión Segura y se refiere a un protocolo de alto nivel de seguridad para las comunicaciones a través de la internet.
SSL proporciona una sesión cifrada entre el servidor y el navegador y ayuda a garantizar que la información sensible (datos personales o financieros) permanezca confidencial durante su transmisión.

TLS:
Transport Layer Security o TLS versión mejorada de SSL, funciona de un modo muy parecido a SSL, con la diferencia de que utiliza cifrado para proteger la transferencia de los datos e informaciones.

TROYANO:
Código malicioso camuflado dentro de otro programa, aparentemente útil e inofensivo, hasta que ejecutan las instrucciones de la persona que creó el código. Estos tienen la capacidad de mantenerse silentes e indetectables hasta activarse, utilizando funciones del sistema operativo como fecha, hora o el cumplimiento de algún otro tipo de evento en el equipo.

VULNERABILIDADES DE SEGURIDAD:
Se refiere a fallas, defectos o errores de programación los cuales pueden ser explotados por usuarios maliciosos sin autorización, para acceder a redes de computadoras o servidores. En la medida en que estas vulnerabilidades se dan a conocer, las empresas programadoras desarrollan parchos parches (“*patches*”), mejoras (“*updates*”) o arreglos (“*fixes*”) para corregir estas vulnerabilidades.

VIRUS:
Es la más conocida amenaza que enfrentan los servidores, navegadores, páginas en Internet y computadoras. Los virus son programas que se instalan en las computadoras, normalmente de forma oculta al usuario, con fines maliciosos (por ejemplo, destruir archivos, o el disco, propagarse a otras computadoras o provocar un mal funcionamiento en el equipo). Por lo general no actúan hasta que se ejecuta el programa que lo contiene o hasta que se cumple alguna condición (una fecha u hora específica).