PARTE I: INTRODUCCION A LA SEGURIDAD INFORMÁTICA

Capítulo 1: INICIACIÓN A LA SEGURIDAD INFORMÁTICA

El concepto de la seguridad comienza desde nuestro PC, la seguridad a nivel local es lo primero que debemos cuidar. Un 90 % de los ataques vienen por las contraseñas. Es conveniente cambiarlas cada 15 días, o por lo menos una vez al mes.

Existen sistemas de fuerza bruta, "John the ripper", que consiste en un ataque a las contraseñas por medio de un programa que prueba palabras que están en un diccionario hasta que las descubre (normalmente un archivo de texto). Es decir, exploran combinaciones con el fin de hallar la contraseña. Pero en estos diccionarios no están todas las posibles claves, por lo tanto, lo adecuado es poner cosas que no estén en los diccionarios, por ejemplo, una contraseña

que no signifique nada, sin sentido, con caracteres ascii como ^y ~, y lo suficientemente larga.

Hay tres tipos de contraseñas que conviene no olvidar de poner en un PC si queremos que tenga una mínima seguridad. Se empieza " de abajo a arriba:

- La primera, la de la Bios. Esta es para que en el arranque no se pueda acceder a arrancar el SO (sistema operativo). Es muy conveniente hacerlo ya que hay muchas intrusiones a nivel "local", es el primer sitio que debemos cuidar. Si quitamos la pila de la Bios eliminaríamos la contraseña, esto implica un mayor trabajo en caso de un ataque.

- Después es importante poner también una contraseña de acceso al sistema (nos centramos en Windows). Dicha contraseña debe constar de, al menos, 8 caracteres para que sea algo segura. Procuraremos mezclar números, letras y también símbolos tipo la @ (pensad que en un ataque por fuerza bruta, una contraseña de menos de 15 caracteres es "rompible", pero tardaría tiempo).

- A continuación hay otra contraseña a tener en cuenta, el del salvapantallas de Windows. No lo descuidéis, en el trabajo hay verdaderos problemas con este tema, un descuido y podemos sufrir ataques rápidos fortuitos desde casa o el trabajo. Lo del salvapantallas no es una tontería, te vas al baño y...PC abierto, entonces te pueden colar un troyano, ver tus archivos, etc. Lo mejor es activar el salvapantallas con la opción de introducir contraseña para volver a tener acceso al PC.

NetBios

Veamos otro aspecto que está trayendo desde siempre muchos problemas: NetBios es uno de los quebraderos de cabeza de la seguridad y un coladero constante de problemas.

Netbios es un protocolo "invisible" para la mayoría, pero que esta ahí. Se usa para compartir archivos e impresoras vía Internet. Opera, normalmente, por el puerto el 139.

Realmente, a no se que estemos en una "Intranet" o "Extranet" no es necesario que esté habilitado. EN Windows XP Se quita desde PANEL DE CONTROL > CONEXIONES DE RED > COMPARTIR ARCHIVOS E IMPRESORAS EN RED. De ese modo evitaremos que, por un descuido y por compartir los archivos de nuestro disco, nos entren hasta la cocina.

Deshabilitar NetBios no afecta a otras cuentas de usuario, ya que éstas son individuales. Tampoco afecta para compartir archivos en programas P2P, sino que lo que hace es deshabilitar el compartir vía Web o mejor dicho, vía Internet. Es decir, podemos quitarlo y compartir archivos, creando grupos de trabajo, dominios, etc.

En el caso de que NetBios esté abierto, el uso de una contraseña evita que la intrusión sea tan fácil, porque si un intruso ve que tenemos el puerto abierto y netbios "open" intentará acceder. Pero si hay un contraseña la cosa se complica porque tendría que intentarlo por "fuerza bruta".

Correo electrónico

Hay dos tipos de correo: el correo POP y el correo Web. El POP se descarga al disco duro, el Web se ve por Internet (por ejemplo Hotmail).

Normalmente se usa el correo Web y eso no es muy recomendable porque es más fácil "romper" una cuenta de Hotmail que una de vuestro proveedor. La mayoría de las veces, el problema viene por la famosa pregunta-respuesta secreta. Puede sonar repetitivo pero no deben ponerse respuestas "previsibles", recordemos que el ataque suele ser de algún conocido que maneja datos nuestros. Además, puede intentar valerse de algún "exploit" para comprometer la seguridad del mismo. Por tanto es aconsejable usar el POP para lo importante y el correo Web para lo demás. El POP es mas fiable, seguro y tiene mas espacio.

Además, es recomendable un filtro "antispam" que lo que hace es comprobar las direcciones de los correos que entran con otras que están en listas de spammers. Y, si los detecta, las bloquea. Hay muchos programas anti pam, la mayoría funcionan bien; y es mas rápido que lo de "bloquear remitente".

Es muy importante que cada vez que nos bajemos un archivo o lo veamos sospechoso, le demos a "guardar destino como" y lo bajemos del Escritorio a una carpeta que podemos llamar "para escanear" y a continuación lo pasemos por el antivirus. A veces en las presentaciones tipo "PowerPoint" pueden venir virus adjuntos, también en las .src (extensión del salvapantallas), .pif, .bat, .com, etc.

La mayoría de infecciones vienen porque al abrir el correo, por ejemplo en el Outlook Express (se trata correo POP), no damos tiempo a que el antivirus esté actualizado.

Si utilizamos un gestor de correo electrónico debemos saber que si no esta activada la "vista previa" no se abre el correo ni se ejecutan archivos adjuntos si no lo decides tú, por lo tanto no te infectas (en VER > DISEÑO > desactivar MOSTRAR PANEL VISTA PREVIA). Independientemente de esta opción, también existe la posibilidad de "no permitir que se abran o guarden archivos adjuntos que puedan contener virus" (en HERRAMIENTAS > OPCIONES > pestaña SEGURIDAD > desactivar la casilla correspondiente).

Virus y troyanos

Podemos usar dos antivirus teniendo en cuenta que sean compatibles entre sí. Por ejemplo el KAV sólo para rastreos y el NOD como residente siempre activo. En el antivirus, el módulo activo controla todo lo que entra al PC y escanea constantemente en busca de virus.

El problema viene con los "virus durmientes": algunos virus no están activos, sino que esperan a una fecha y el módulo de

chequeo activo no lo detecta porque puede que el día de la "activación" del virus (por ejemplo, Viernes 13) nuestro antivirus no este activo o lo hayamos desactivado, por eso es importante hacer un escaneo semanal a todo el disco. Es decir, lo detectará en el caso de que hagamos el escaneo, puesto que por lo general en modo activo no lo suelen pillar.

Si nuestro antivirus tiene un buen motor heurístico, puede que detecte ese "virus durmiente" aunque éste no esté activo. Pero la heurística es una "ciencia" inexacta: se basa en el control del código y el modo de manifestarse de un posible virus. Hay veces en las que ni el antivirus con la heurística mas potente lo detectaría; por lo tanto, no hay que fiarse totalmente de la heurística aunque ayude bastante, porque mañana podría surgir un virus que ataque de modo "anormal" (como el Blaster) y nos infectaríamos.

Si se activara un virus durmiente, el módulo residente (suponiendo que lo tenga en su base de datos) lo detectaría en ese momento, aunque puede que también ataque al antivirus antes de que éste lo detecte, inutilizando el módulo y creándonos una falsa sensación de seguridad. Esto ocurre porque, a veces, va mas rápido el virus que el módulo porque utiliza menos recursos, consume menos memoria y es más rápido que el propio antivirus.

Una vez detectado y eliminado un virus (tanto de forma manual, por medio de un parche o por el propio antivirus) pueden ocurrir tres cosas:

- que esté eliminado completamente y ya no tengamos ningún problema.

- que esté eliminado pero hayan archivos que estén "corruptos".

- que el virus mute y ataque al antivirus.

Por esto último es recomendable arrancar el PC pulsando "F8" y elegir entrar en "modo seguro con funciones de red" para, de esta forma, escanearse con el antivirus Panda vía Web, por ejemplo.

Llegados a este punto, si hacemos este escaneo en Panda en modo normal en vez de hacerlo en modo seguro, podríamos temer que un posible virus atacase al mini módulo que instala el escáner del Panda y dicho escaneo fuese inútil. Esto no es muy probable ya que es de lo más resistente que hay para esos casos de infección.

Troyanos y antitroyanos

Además de los virus, están los troyanos: programas de código "malicioso" que se dedican a hacer de puente entre el PC de un atacante y nuestro ordenador. Los antivirus suelen fallar con los troyanos en muchos casos. El Kaspersky y el NOD 32 son de los mejores con ellos, pero lo mejor es tener un antitroyanos como por ejemplo el The Cleaner.

Si tenemos un troyano dentro y nos lo detectan, las entradas pueden ser interminables; es por eso que el uso de un firewall (muro virtual entre el ordenador y la red) se hace imprescindible, además de para otras muchas cosas. El firewall vigilará cualquier conexión entrante y saliente entre Internet y el PC.

Spyware y antispyware

El spyware o software espía instala como un "mini troyano" y se dedica a enviar información por un puerto previamente abierto, normalmente UDP (user datagram protocol, no necesita "envío-recibo" de conexión) a un servidor o máquina que recoge los datos de nuestros hábitos de navegación (paginas vistas, direcciones de e-mail, etc.), para luego spammear sin cesar a nuestra máquina. Además, puede cambiar la página de inicio del navegador y llevarnos a una dirección no deseada cada vez que se inicie el navegador web.

Algunos antivirus empiezan a tener dentro firmas de spyware pero no se ponen de acuerdo, es por ello que se recomienda el uso de softs tipo Ad-Aware o Spybot para eliminarlo.

Si el spyware es muy complejo puede abrir cualquier puerto y no dejar de recibir información y nuevas "cosas" para instalar en el PC (de ahí la importancia de tener un firewall). Diríamos que es como un troyano aunque sin intervención directa de otro usuario, pero en definitiva es todo un ataque contra la privacidad.

En resumen: el software espía es una violación de la privacidad, abre puertos que pueden ser explotados, puede instalar páginas de inicio no deseadas, ralentiza nuestra conexión y consume ancho de banda.

Dirección IP y privacidad

La IP es como el documento de identidad del PC, es algo que asigna nuestro proveedor de acceso a la red de forma aleatoria. Con la IP la seguridad se compromete en gran manera, porque para hacer un ataque es a por lo primero que se va, y el rastro que dejamos nos puede jugar una mala pasada.

Las hay de dos tipos: estáticas o dinámicas.

- Las estáticas o fijas, son por ejemplo las de un Server. Ese Server tiene una IP y por medio de las DNS resuelve que www.daboweb.com es la IP XXX (explicado en plan de andar por casa) y te lleva a la web correspondiente.

- La mayoría son dinámicas:

.....- Las que son por medio de módem cambian cada vez que te conectas, lo cual es muy bueno para la seguridad. Lo negativo es que con las IP de módem tradicional, por impulsos o

línea telefónica, nos pueden colar un dialer o programa que desvía la conexión a Internet a través de números de tarifa especial (más elevada que la conexión normal).

.....- Las de ADSL o cable cambian pero no tan a menudo, con lo cual, en el caso de que haya un ataque o troyano o fallo que hayan detectado desde fuera, nos intentarán atacar pero hasta que cambie la IP. La periodicidad con que se produce este cambio es aleatoria, depende del uso que haya en la red en ese momento.

Algo que puede complicarnos la vida en más de una ocasión es, por ejemplo, un foro que tenga las IP visibles. En ese caso, un hacker rastrea los foros de novatos, mira las preguntas que haces y ve la IP, empieza a escanear y te ataca. Tenemos entonces mayor peligro si tenemos ADSL o cable y la IP no cambia cada poco, por lo que se hace a veces indispensable el ocultarla por medio de proxies o webs de navegación anónima (ejemplo, proxomitron y www.anonymizer.com).

Aún así, no es imposible llegar hasta la IP de un usuario. Por ejemplo, para saber la de alguien que haya hecho una trastada, la policía puede solicitar saber quien se enrutó ese día y en ese momento. Luego contactan con el proveedor y éste les dará la información. Por tanto, la manera mejor manera de navegar anónimamente (y mas lenta) es hacerlo tras una cadena de proxies.

Autor: Dabo, webmaster de www.daboweb.com

Capítulo 2: LA SEGURIDAD INFORMÁTICA DE AQUELLO QUE ESTÁ ABIERTO

Uno de los problemas que está afectando a la seguridad de la información en nuestros PC es la falta de cuidado que los usuarios tenemos, con más frecuencia de la debida, respecto a dónde ponemos los datos y las informaciones que más nos interesan y cómo disponemos de las mismas en el momento de borrarlas o eliminarlas de un fichero o archivo. Curiosamente, todos somos conscientes de cómo funciona el sistema operativo de los PC cuando se borra un fichero, pero la inconsciencia surge cuando esto se nos olvida.

En estos breves comentarios voy a tratar estos dos aspectos que afectan al quehacer diario de todos nosotros.

Los datos y las informaciones normalmente los tenemos almacenados en el disco duro del PC que usamos a diario, y al cual, en principio, no tenemos acceso más que nosotros, tanto si se trata de un PC puramente personal, como si se trata de un PC corporativo de la organización para la que trabajamos. Claro que la situación es diferente si el PC es personal y lo tenemos en casa, o si es de la organización y lo tenemos en su sede conectado a una red. Veamos cuáles son las diferencias y las similitudes. Atención, parto de la base de que se dispone de un PC tipo fijo o portátil, (es lo mismo) con los últimos avances como Wifi, puerto infrarrojo, puerto bluetooth, puertos USB y conexión a Internet vía red interna o vía módem.

El primer problema es el de analizar si los datos y las informaciones que tenemos en nuestro disco duro son importantes y por tanto deberíamos cifrarlas para impedir a cualquier intruso tener acceso a su contenido. Hoy en día hay sistemas de cifrado de variada complejidad, pero incluso el PGP es lo suficientemente robusto para tener una protección adecuada en la mayoría de los casos.

La segunda etapa del análisis a realizar son los mecanismos de acceso al PC, es decir, accedemos normalmente mediante el teclado y la pantalla, pero esto no nos interesa, sino los mecanismos por medio de los cuales podemos extraer los datos y las informaciones y llevarlas a otro lugar utilizando el correspondiente soporte electrónico. Aquí es donde entran en juego los distintos sistemas de puertos del PC que lo ponen en comunicación con el exterior. Ya hace años, para el transporte de informaciones de un lugar a otro se utilizaban los disquetes, pero estos alcanzaron una capacidad máxima de 1,4 megabytes, lo cual no da mucho de sí (existían algunos disquetes del doble de capacidad). A pesar de esta limitación de capacidad ha habido organizaciones que impusieron la supresión de las disqueteras, entre otros motivos para evitar la entrada de virus en los PC, pues los disquetes eran una de las vías de infección por virus más frecuentes, sin perjuicio de que también

se utilizaban para transportar programas, no necesariamente legales y ficheros pirateados. Una de las maneras de prevenirlo fue precisamente la supresión de las unidades de disquetes cuando los PC estaban conectados a redes desde las que se podía comunicar y compartir la información y los programas.

En la actualidad nos encontramos con tres tipos de unidades de almacenamiento que pueden resultar harto peligrosas para la seguridad de la información si no se manejan y se administran con el cuidado debido. Me refiero a las unidades de disquetes de gran capacidad (llegan hasta más de 200 megabytes), los denominados discos duros portátiles y los dispositivos de memoria. Y todos estos dispositivos se conectan mediante los puertos USB del PC. Aquí es donde verdaderamente tenemos el problema de seguridad. Es difícil pensar en los momentos actuales llegar a disponer PC sin puerto USB, pero los dispositivos que a estos puertos se pueden conectar para extraer datos e informaciones requieren una clara supervisión por parte de los responsables de seguridad de las organizaciones, so pena de incurrir en riesgos que podrían no resultar aceptables para la organización. Lo mismo que, por otros motivos, ya se ha comenzado a prohibir entrar en determinados lugares con teléfonos móviles dotados de cámara fotográfica. Habría que llegar a prohibir el uso de los citados dispositivos portátiles de almacenamiento masivo de información en las organizaciones si no están controlados debidamente por quien sea responsable de la seguridad de la información. Sobre todo los problemas se plantean con el uso de los dispositivos de memoria flash por sus reducidas dimensiones y la facilidad de ocultarlos.

El siguiente problema nos lo plantea el dispositivo Wifi, el puerto infrarrojo y el puerto o dispositivo bluetooth de los PC portátiles, ya que si este dispositivo está permanentemente abierto y operativo, no es nada difícil que un pirata se nos cuele en nuestro PC y nos cause estragos. Si, por ejemplo, se colocan dos PC portátiles próximos y alguno de los dispositivos mencionados está simultáneamente operativo en ambos equipos, muy fácilmente se sintonizarán y estarán dispuestos para comunicarse entre los dos. Por ello resulta muy recomendable el que estos dispositivos estén

normalmente cerrados e inoperativos, y solo se habiliten cuando sea necesario y tomando las correspondientes precauciones.

Por último está el tema del borrado de ficheros. Supongo que habrá alguien que se acuerde de aquella película británica de los años 60 en que un ingenioso empresario consigue convencer a las mujeres de la limpieza de unas oficinas de un agente de bolsa londinense para que al terminar su trabajo acudieran a una reunión con él y con todo el papel que habían recogido de las papeleras de las oficinas. De repente, se ponían a investigar el contenido de las informaciones que aparecían en aquellos trozos de papel u hojas hechas pelotillas que se estiraban convenientemente. Aquellos "ficheros" "borrados" contenían tanta información valiosa que todos los allí presentes, mujeres de la limpieza y empresario, en la película, se hacían ricos. Pues con nuestros PC hacemos normalmente lo mismo que aquellos que tiraban a la papelera las notas de sus transacciones de bolsa, es decir, aparentemente destruimos los ficheros, los borramos; pero en realidad el sistema de borrado lo único que hace es alterar el primer carácter del nombre del fichero y así, con el programita de turno, es fácilmente recuperable cada fichero y por lo tanto aprovechable. Si queremos realmente eliminar un dato o una información en un disco duro o memoria flash, lo que hay que hacer es pasar el correspondiente programa de destrucción (que no borrado) de ficheros. Los hay de muy buenos, que repiten la operación varias veces, y los hacen realmente irrecuperables, incluso para los expertos en la ciencia forense informática.

Y esto es sólo la punta del iceberg, algunos de los problemas de seguridad que se soslayan con facilidad en el día a día del trabajo. Espero que cuando menos sirva para capacitar y reflexionar sobra la seguridad informática esencial.

Autor: Fernando Piera Gómez

fpiera@ati.es

Capítulo 3: ETIMOLOGÍA DE FOO

Aproximadamente 212 RFCs, alrededor del 7% de los RFCs, comenzando con el [RFC269], contienen los términos `foo', `bar', o `foobar', utilizados como variables metasintácticas sin ningún tipo de explicación o definición. Esto puede parecer trivial, pero un gran número de iniciados, especialmente aquellos cuya lengua nativa no es el inglés, han tenido problemas para comprender el origen de dichos términos.

Definición y Etimología

bar /bar/ n. [JARGON]

1. La segunda variable metasintáctica, después de foo y antes de bar. "Supongamos que tenemos dos funciones: FOO y BAR. FOO llama a BAR..."

2. A menudo añadida a foo para formar foobar.

foo /foo/ [JARGON]

1. Interjección. Expresión de asco.

2. Utilizada generalmente como un nombre de ejemplo para absolutamente cualquier cosa, especialmente programas y archivos sobre todo archivos scratch).

3. La primera de la lista estándar de variables metasintácticas utilizadas en ejemplos de sintaxis (bar, baz, qux, corge, grault, garply, waldo, fred, plugh, xyzzy, thud).

Cuando se utiliza en conexión con `bar' generalmente hace referencia al acrónimo de la II Guerra Mundial FUBAR (`Jodidos Sin Remedio`, Fucked Up Beyond All Repair`), posteriormente modificado a foobar. Las primeras versiones del Archivo Jargon [JARGON] interpretaron este cambio como una moderación posguerra, pero parece ser que FUBAR se derivó de `foo', tal vez influenciado por el alemán `furchtbar', (terrible) - puede que incluso `foobar' haya sido la forma original.

Por lo que parece, la palabra `foo' tiene una historia preguerra en viñetas de cómics y dibujos animados. En 1938, los dibujos de "Daffy Doc", una versión inicial del Pato Duffy, de la Warner Brothers y dirigidos por Robert Clampett, sostenía un letrero que decía "EL SILENCIO ES FOO" (SILENCE IS FOO). `FOO' y `BAR' también aparecen en las viñetas de Pogo, de Wall Kelly. Las primeras utilizaciones documentadas aparecen en el cómic surrealista "Smokey Stover", de Bill Holman, que trata sobre un bombero. Esta tira aparece en varios cómics americanos añadiendo "Everybody's" entre 1930 y 1952. Es frecuente poner la palabra "FOO" en las matrículas de los coches, o en expresiones sin sentido que hacen referencia a otras conocidas, como "El que foo el último foo mejor"

("He who foos last foos best"), o "Muchos fuman, pero foo mascan" ("Many smoke but foo men chew"), además Smokey decía "Donde hay foo hay fuego" ("Where there's foo, there's fire").

Bill Holman, el autor de la tira, lo llenó de bromas extrañas y chistes personales, incluyendo frases como "Notary Sojac", y "1506 nix nix". Coincidiendo con La Compañía de Dibujos Animados Warner Brothers [WBCC], Holman aseguraba haber encontrado la palabra "foo" en el fondo de una figurita china. Esto es plausible, ya que las estatuillas chinas suelen tener inscripciones con carácter apotropaico (de protección o amuleto), y tal vez a éstas pertenezca la palabra china `fu' (algunas veces interpretada como `foo'), que puede significar "felicidad" cuando se pronuncia con el tono adecuado (los leones-perro guardianes que aparecen a los lados de la entrada de muchos restaurantes chinos reciben el nombre de "perros fu") [PERS]. Sin duda alguna, la aceptación de la palabra sin sentido `foo' por los angloparlantes fue influenciada por el término hebreo `feh' y las palabras inglesas `fooey'y `fool'. [JARGON, FOLDOC]

El protagonista de las viñetas de Holman era un camión de bomberos llamado Foomóvil, que se desplazaba sobre dos ruedas. Esta tira de cómic fue tremendamente popular a finales de los 30, y existe incluso una leyenda sobre un fabricante de Indiana que construyó una versión funcional del Foomóvil de Holman [EAC]. Según la Enciclopedia de Cómics Americanos [EAC], la fiebre del `Foo' se extendió por América, en canciones populares y creando más de 500 'clubs del Foo'. La moda dejó referencias a `foo' dentro de la cultura popular (incluyendo un par de apariciones en dibujos de la Warner Brothers entre 1938 y 1939), pero sus orígenes se perdieron rápidamente. [JARGON]

Un lugar donde se sabe que permaneció fue en el ejército de los Estados Unidos durante los años de la Segunda Guerra Mundial. Entre 1944 y 1945, el término `cazadores de foo' (foo fighters) [FF] fue utilizado por los operadores de radar para designar a las apariciones misteriosas o rastros extraños que posteriormente serían denominados OVNI (Objeto Volador No Identificado) (el término antiguo reapareció en América en 1995 a través del nom-

bre de uno de los mejores grupos musicales de grunge-rock [BFF]). Los informadores relacionaron el término con la viñeta de Smokey Stover [PERS]

Los militares británicos y americanos a menudo utilizaron términos de su jerga durante la guerra. Las fuentes periodísticas señalaron que `FOO' se convirtió en un sujeto semilengendario de los graffitis de la II Guerra Mundial, equiparable al Kilroy americano [WORDS]. Allá donde fueron las tropas británicas aparecieron pintadas del tipo "Foo estuvo aquí", o similares. Muchos diccionarios de jerga aseguran que FOO probablemente se originó por Oficial de Observación Avanzada (Forward Observation Officer), pero esto (al igual que el contemporáneo "FUBAR") fue probablemente una palabra regular hecha acrónimo [JARGON].

Cuarenta años después, EL excelente libro de Paul Dickson "Words" [WORDS] siguió el rastro de "Foo" hasta una revista naval Británica de 1946 sin especificar, que decía lo siguiente:

"Mr. Foo es un misterioso producto de la Segunda Guerra Mundial, mezclado con omnisciencia amarga y sarcasmo".

Las primeras versiones del Archivo Jargon sugirieron la posibilidad de que los hackers lo utilizasen realmente extraído de "FOO, Sátiras y Parodias", el título de un libro de cómics editado por primera vez el Septiembre de 1958, un proyecto conjunto de Charles y Robert Crumb. A pesar de que Robert Crumb (por entonces en la mitad de su adolescencia) posteriormente se convirtiese en uno de los artistas más influyentes de los cómics underground, este proyecto no tuvo éxito; de hecho, los hermanos quemaron la mayor parte de las copias existentes por el disgusto. El título FOO fue escrito con letras grandes en la portada. Sin embargo, muy pocas copias de este cómic circularon realmente, y los estudiantes de la obra de Crumb han determinado que este título era una referencia a los cómics anteriores de Smokey Stover. Los Crumb pudieron ser influenciados también por una revista canadiense, de corta vida, denominada `Foo' publicada entre 1951 y 1952. [JARGON]

Un antiguo miembro señaló que en 1959 el "Diccionario del Lenguaje del TRMC", compilado en el TRMC (Tech Model Railroad

Club en el MIT) tenía una entrada para Foo. La versión actual en Internet, en la que "Foo" es la única palabra escrita en rojo, contiene lo siguiente [TRMC]:

Foo: La sílaba sagrada (FOOO MANI PADME HUM); solo puede ser dicha bajo obligación para comunicarse con la Deidad. Nuestra primera obligación es mantener los Contadores Foo girando.

Esta definición utilizaba el término sin sentido de Bill Holman, entonces con sólo dos décadas de antigüedad, y se puede demostrar que aún perdura en la jerga y en la cultura popular, para hacer una analogía "ha ha seria" con el esoterismo Budismo Tibetano. Los hackers actuales encontrarían difícil resistirse a hacer alguna broma del mismo estilo, y probablemente no eran menos susceptibles en 1959. [JARGON]

4. [EF] El Príncipe Foo fue el último emperador de Pheebor y dueño del Timón Phee alrededor de 400 años antes del reinado de Entharion. Cuando Foo fue decapitado por alguien que él denominó "fop del este" de Borphee, la era gloriosa de Pheebor terminó, y Borphee alcanzó la importancia que ahora disfruta.

5. [OED] Término utilizado entre los siglos 13 y 16 para designar al demonio o a cualquier otro enemigo. La primera cita que aparece es del año 1366, Chaucer A B C (84): "Lat not our alder foo [demonio] make his bobance [ostentación]". El "Foo" al que Chaucer hace referencia está asociado probablemente al término inglés actual "foe".

6. Raza poco común de perro. Un perro de raza spitz redescubierto después de haber sido considerado como extinto durante mucho tiempo, el perro chino Foo, o también Perro Sagrado de Sinkiang, su origen pudo ser el cruce de los perros cazadores del Norte de Europa con el antiguo perro Chow Chow de Mongolia, o bien ser el eslabón perdido entre el Lobo Chino y el Chow Chow. Su nombre deriva probablemente de foochow, el estilo predominante en Foochow, o bien provenir de la ciudad de Foochow (ahora Minhow) en el sureste de China. [DOG]

foobar n.

[JARGON] Una variable metasintáctica muy utilizada; ver foo para etimología. Probablemente difundida a través de los manuales de los sistemas DEC de Digital Equipment Corporation (DEC) en los años 60 y principio de los 70; en este aspecto las pruebas se remontan hasta 1972. Los hackers no suelen utilizar esto para hacer referencia a FUBAR. Se ha sugerido que "foobar" se extendió entre los primeros ingenieros informáticos en parte debido a FUBAR y en parte a que ,en el lenguaje técnico utilizado en electrónica, "foo bar" se considera una señal "foo" invertida.

foo-fighter (cazador de foo) n.

Término de la Segunda Guerra Mundial para designar a los Objetos Voladores No Identificados (OVNIs), observados tanto por los alemanes como por los ingleses. Ver [FF] y entrada superior a "foo".

Acrónimos

La información siguiente se ha obtenido directamente de las compilaciones de la University Cork College <http://www.ucc.ie/acronyms> y del Buscador de Acrónimos <http://www.AcronymFinder.com> generalmente utilizado para uso informático.

Bar

Extensión genérica de archivo que no refleja nada acerca del tipo de archivo que representa

BAR: Registro de Dirección Base (Base Address Register) Registro de Dirección de Buffer (Buffer Address Register)

FOO: Observador de Observación Avanzada (Forward Observation Observer).

FOO de Oberlin: Una organización cuyo nombre es un acrónimo recursivo. Apodo: The FOO, the FOO, the Proud (el Orgullo). Ver <http://cs.oberlin.edu/students/jmankoff/FOO/home.html>. Archivo Abierto para Salida. Un código de error NFILE [RFC1037].

FOOBAR: Operaciones FTP en Grandes Registros de Direcciones [RFC1639]. (Particularmente apropiado ya que el primer RFC que uso "foo", [RFC269], trataba sobre transferencias de archivos).

FUBAR: Registro de Dirección UniBus Errónea - en una VAX, de Digital Equipment Corporation Engineering. Jodidos Sin Remedio - De la Armada de los Estados Unidos en la II Guerra Mundial. Algunas veces corregido a "Arruinados...".

FUBARD: Forma pasada de FUBAR.

Texto completo de este documento:

http://www.rfc-es.org/getfile.php?rfc=3092

Texto original de Donald E. Eastlake, Carl-Uno Manros y Eric S. Raymond

Traducción al español del RFC: Rubén Alfonso Francos

Capítulo 4: LISTA DE ESTÁNDARES DE SEGURIDAD INTERNACIONALES

Este documento lista los estándares internacionales relacionados con seguridad informática que se consideran importantes en la actualidad o por su importancia histórica. Están clasificados en seis clases de estándares: para administración de seguridad de la información, para evaluación de seguridad en sistemas, para desarrollo de aplicaciones, para servicios financieros, para riesgos y para autenticación.

Porque a ver... ¿alguien sabe en qué consiste el estándar ISO 17799? ¿Cuáles son sus repercusiones? ¿Cómo se debe aplicar? En este informe desvelamos esta ISO y otras relacionadas con la seguridad informática.

- RFC 2196

La Internet Engineering Task Force (IETF) elaboró el RFC2196 Site Security Handbook, que ofrece una guía práctica para quienes intentan asegurar servicios e información. Se puede conseguir en http://www.ietf.org/rfc/rfc2196.txt

- BS 7799 (Reino Unido)

El estándar británico BS 7799 es un estándar aceptado ampliamente que ha sido utilizado como base para elaborar otros estándares de seguridad de la información, incluyendo el ISO 17799. Fue desarrollado por el British Standards Institute (http://www.bsi-global.com). En la página BSI Catalogue (http://bsonline.techindex.co.uk) se puede buscar el estándar 7799.

La versión actual del estándar tiene dos partes:

o BS7799-1:1999 Information Security Management. Code of Practice for Information Security Management

o BS7799-2:1999 Information Security Management. Specification for Information Security Management Systems

El BSI ha implementado un esquema de certificación para el BS 7799 a través del C:Cure program. Más información está disponible en http://www.c-cure.org

- Manual de protección de IT (Alemania)

La Agencia Federal Para Seguridad en Información en Alemania ha generado el IT Baseline Protection Manual. Este docu-

mento presenta un conjunto de métricas de seguridad recomendadas o safeguards, como se denominan en el manual, para sistemas IT típicos. La versión ms á reciente es de octubre de 2000. Más información puede ser encontrada en http://www.bsi.bund.de/gshb/english/menue.htm

• Guías OECD

OECD Guidelines for the Security of Information Systems, están disponibles http://www.oecd.org/dsti/sti/it/secur/prod/e_secur.htm

Otros estándares para evaluación de seguridad en sistemas...

• ISO 15408 (Common Criteria)

La International Organization for Standardization (ISO) ha elaborado el estándar IS 15408. Este estándar, The Common Criteria for Information Technology Security Evaluation v2.1 (ISO IS 15408) es una mezcla mejorada deITSECl , el Canadian criteria, y el US Federal Criteria.

Se encuentra en http://csrc.nist.gov/cc/ccv20/ccv2list.htm

• Serie Arco Iris - Rainbow Series- (Orange Book) (EE.UU.)

Una importante serie de documentos es la Rainbow Series, que delinea una serie de estándares de seguridad desarrollados en los EE.UU. Esta serie está disponible en http://www.radium.ncsc.mil/tpep/library/rainbow

Quizá el libro ms importante de esta serie esá el Trusted Computer System Evaluation Criteria (TCSEC, o Orange Book). Aunque este estándar, de 1985, ha sido superado por otros estándares (como los mencionados antes en este documento) sigue siendo un documento útil. De forma adicional, el US Federal

Criteria, fue elaborado como borrador a comienzos de los años 90, aunque nunca fue adoptado.

TCSEC puede ser encontrado en http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

• Information Technology Security Evaluation Criteria (ITSEC) (Reino Unido)

El Reino Unido elaboró el Information Technology Security Evaluation Criteria (ITSEC) a comienzos de los años 90, y es ot ro estándar históricamente importante.

Fue elaborado, en algunos aspectos, basándose en el Orange Book, pero con una mayor granularidad.

Detalles sobre este esquema pueden ser encontrados en http://www.itsec.gov.uk/

Lista de estándares de seguridad internacionales...

Estándares para desarrollo de aplicaciones

• Capability Maturity Model (CMM)

El Software Engineering Institute lideró el desarrollo del Capability Maturity Model, que es un motodo para garantizar mé adurez en procesos. Detalles sobre el modelo pueden encontrarse en http://www.sei.cmu.edu/cmm/cmms/cmms.html

• System Security Engineering Capability Maturity Model (SSE-CMM)

Un derivado del CMM es el System Security Engineering Capability Maturity Model. Detalles están disponibles en http://www.sse-cmm.org

Estándares para servicios financieros

ISO 11131 (Banking and Related Financial Services; Sign-on Authentication)

ISO 11131:1992 Banking and Related Financial Services; Sign-on Authentication

ISO 13569 (Banking and Related Financial Services -- Information Security Guidelines)

ISO 13569:1997 Banking and Related Financial Services -- Information Security

Estándares para riesgo

• Acquisition Risk Management (EE.UU.)

El Software Engineering Institute tiene algunos documentos sobre Acquisition Risk Management. Los detalles están disponibles en http://www.sei.cmu.edu/arm/index.html

Estándares para autenticación

ISO 11131 (Banking and Related Financial Services; Sign-on Authentication)

ISO 11131:1992 Banking and Related Financial Services; Sign-on Authentication

¿Qué es la ISO 17799?

En la actualidad las empresas son conscientes de la gran importancia que tiene para el desarrollo de sus actividades el hecho de proteger de forma adecuada la información que poseen y especialmente aquella que les sirve para realizar correctamente su actividad de negocio. El poder gestionar bien la seguridad de la información que manejan no sólo permitirá garantizar, de cara a la propia organización, que sus recursos están protegidos -asegurando la confidencialidad, integridad y disponibilidad de los mismos- sino que de cara a los posibles clientes les aportará un grado de confianza superior al que puedan ofrecer sus competidores, convirtiéndose en un factor más de distinción en el competitivo mercado en el que comercia la empresa.

Debido a la necesidad de securizar la información que poseen las organizaciones era precisa la existencia de alguna normativa o estándar que englobase todos los aspectos a tener en consideración por parte de las organizaciones para protegerse eficientemente frente a todos los probables incidentes que pudiesen afectarla, ante esta disyuntiva apareció el BS 7799, o estándar para la gestión de la seguridad de la información, un estándar desarrollado por el British Standard Institute en 1999 en el que se engloban todos los aspectos relacionados con la gestión de la seguridad de la información dentro de la organización. Esta normativa británica acabó desembocando en la actual ISO/IEC 17799:2000 – Code of practice information security management.

En un principio se consideraba por parte de las empresas que tenían que protegerse de lo externo, de los peligros de Internet, pero con el paso del tiempo se están percatando de que no sólo existen este tipo de amenazas sino que también hay peligros dentro de la organización y todos éstos deberían ser contemplados a la hora de securizarse. La aparición de esta normativa de carácter

internacional ha supuesto una buena guía para las empresas que pretenden mantener de forma segura sus activos.

La ISO/IEC 17799:2000 considera la organización como una totalidad y tiene en consideración todos los posibles aspectos que se pueden ver afectados ante los posibles incidentes que puedan producirse. Esta norma se estructura en 10 dominios en los que cada uno de ellos hace referencia a un aspecto de la seguridad de la organización:

Política de seguridad

Aspectos organizativos para la seguridad

Clasificación y control de activos

Seguridad del personal

Seguridad física y del entorno

Gestión de comunicaciones y operaciones

Control de accesos

Desarrollo y mantenimiento de sistemas

Gestión de continuidad del negocio

Conformidad legal

En resumen esta norma pretende aportar las bases para tener en consideración todos y cada uno de los aspectos que puede suponer un incidente en las actividades de negocio de la organización.

Esta norma es aplicable a cualquier empresa, sea cual sea el tamaño, la actividad de negocio o el volumen del mismo, esto es lo que se denomina el principio de proporcionalidad de la norma, es decir que todos los aspectos que aparecen en la normativa deben ser contemplados y tenidos en cuenta por todas las organizaciones a la hora de proteger sus activos, y la diferencia radicará en que

una gran organización tendrá que utilizar más recursos para proteger activos similares a los que puede poseer una pequeña organización. De la misma forma, dos organizaciones que tengan actividades de negocio muy diferentes, no dedicarán los mismos esfuerzos a proteger los mismos activos/informaciones. En pocas palabras, esta norma debe tenerse como guía de los aspectos que deben tener controlados y no quiere decir que todos los aspectos que en ella aparecen tienen que ser implementados con los últimos avances, eso dependerá de la naturaleza de la propia organización.

Como hemos comentado la ISO/IEC 17799:2000 es una guía de buenas prácticas, lo que quiere decir que no especifica como se deben proteger los aspectos que aparecen indicados en ella, ya que estas decisiones dependerán de las características de la organización. Es por ello que en la actualidad no es posible que las organizaciones se puedan certificar contra este estándar, ya que no posee las especificaciones para ello.

Por el contrario, la precursora de esta norma, el BS 7799 sí que posee estas dos partes, una primera que representa el código de buenas prácticas y una segunda que los las especificaciones para la gestión de la seguridad de los sistemas de información, y es contra esta segunda parte contra la que las organizaciones que lo deseen pueden certificarse. La ISO (Internacional Organization for Standardization) en la actualidad está trabajando para confeccionar esta segunda parte del ISO/IEC 17799 con el objetivo de que las organizaciones puedan certificarse contra esta norma de carácter internacional.

Así mismo esta normativa internacional ha servido a su vez como precursora para otras de carácter nacional y en el caso de España, en noviembre de 2002 ya surgió la normativa UNE-ISO/IEC 17799 Código de buenas prácticas para la Gestión de la Seguridad de la Información elaborada por AENOR y que a su vez está desarrollando la segunda parte de esta normativa para que las empresas de ámbito nacional puedan certificarse contra ella.

Como conclusiones se puede decir que la normativa ISO/IEC 17799:2000 debe ser utilizada como un índice de los puntos que pueden provocar algún tipo de incidente de seguridad

en una organización para que éstas se puedan proteger de los mismos, sin olvidarse aquellos que puedan parecer más sencillos de controlar hasta llegar a los que pueden suponer un mayor dispendio de recursos a las organizaciones.

Más información:

The ISO 17799 Service & Software Directory

http://www.iso17799software.com

Diez preguntas y respuestas sobre ISO 17799

http://www.angelfire.com/la2/revistalanandwan

Software de conformidad BS7799 / ISO17799 en español

http://www.callio.com.es

Autor: Universidad Nacional de Colombia y esCERT Universidad Politécnica Catalunya

Capítulo 5: GUÍA PARA LA ELABORACIÓN DE POLÍTICAS DE SEGURIDAD EN LA EMPRESA

Esta metodología es potencialmente útil para el desarrollo, implementación, mantenimiento y eliminación de un conjunto completo de políticas – tanto de seguridad como en otras áreas

Es frecuente que las personas involucradas con seguridad informática tengan una visión estrecha de lo que significa desarrollar las políticas de seguridad, pues no basta con escribirlas y pretender ponerlas en práctica. En ocasiones se incluye la asignación de responsables, se realizan actividades para dar a conocerlas y, quizá, se supervise su cumplimiento; pero esto tampoco basta.

Muchas políticas de seguridad informática fallan ya que se desconoce lo que implica realmente desarrollarlas.

Es importante resaltar que una política de seguridad tiene un ciclo de vida completo mientras esta vigente. Este ciclo de vida incluye un esfuerzo de investigación, la labor de escribirla, lograr que las directivas de la organización la acepten, conseguir que sea aprobada, lograr que sea diseminada a través de la empresa, concienciar a los usuarios de la importancia de la política, conseguir que la acaten, hacerle seguimiento, garantizar que esté actualizada y, finalmente, suprimirla cuando haya perdido vigencia. Si no se tiene en cuenta este ciclo de vida se corre el riesgo de desarrollar políticas que sean poco tenidas en cuenta, incompletas, redundantes, sin apoyo pleno por parte de los usuarios y las directivas, superfluas o irrelevantes.

Este documento presenta algunos punttipo de os que deben tenerse en cuenta al desarrollar algún política de seguridad informática.

¿Por qué tener políticas escritas?

Existen varias razones por las cuales es recomendable tener políticas escritas en una organización La siguiente es una lista de algunas de estas razones.

Para cumplir con regulaciones legales o técnicas

Como guía para el comportamiento profesional y personal

Permite unificar la forma de trabajo de personas en diferentes lugares o momentos que tengan responsabilidades y tareas similares

Permiten recoger comentarios y observaciones que buscan atender situaciones anormales en el trabajo

Permite encontrar las mejores prácticas en el trabajo

Permiten asociar la filosofía de una organización (lo abstracto) al trabajo (lo concreto)

Definición de política

Es importante aclarar el término política desde el comienzo. ¿Qué queremos dar a entender cuando decimos POLITICA o ESTÁNDAR o MEJOR PRÁCTICA o GUÍA o PROCEDIMIENTO? Estos son términos utilizados en seguridad informática todos los días, pero algunas veces son utilizados correctamente, otras veces no.

Política. Declaración general de principios que presenta la posición de la administración para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías. Las políticas deben ser pocas (es decir, un número pequeño), deben ser apoyadas y aprobadas por las directivas de la empresa, y deben ofrecer direccionamientos a toda la organización o a un conjunto importante de dependencias. Por definición, las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción.

Estándar. Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares sirven como especificaciones para la implemen tación de las políticas: son diseñados para promover la implementación de las políticas de alto nivel de la organización antes que crear nuevas políticas.

Mejor práctica. Es una regla de seguridad específica a una plataforma que es aceptada a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad con-

creta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la organización.

Guía. Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son, esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento. Los procedimientos definen específicamente cómo las políticas, estándares, mejores prácticas y guías serán implementados en una situación dada. Los procedimientos son dependientes de la tecnología o de los procesos y se refieren a plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada a dicho proceso o sistema específico.

Generalmente los procedimientos son desarrollados, implementados y supervisados o del sistema. Los procedimientos por el dueño del proceso seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.

El cuadro anterior, además de presentar una definición de los términos utilizados en la enunciación e implementación de políticas, muestra una jerarquía entre las definiciones.

Un ejemplo de los requerimientos de seguridad interrelacionados podría ser:

1. En el nivel más alto, se puede elaborar una POLÍTICA, para toda la organización, que obligue a "garantizar seguridad en el correo electrónico cuyo contenido sea información confidencial".

2. Esta POLÍTICA podría ser soportada por varios ESTÁNDARES, incluyendo por ejemplo, que los mensajes de este

tipo sean enviados utilizando criptografía con algún sistema de aprobado por la empresa y que sean borrados de manera segura después de su envío.

3. Una MEJOR PRÁCTICA, en este ejemplo, podría estar relacionada sobre la manera de configurar el correo sobre un tipo específico de sistema (Windows o Linux) con el fin de garantizar el cumplimiento de la POLÍTICA y del ESTÁNDAR.

4. Los PROCEDIMIENTOS podrían especificar requerimientos para que la POLÍTICA y los ESTÁNDARES que la soportan, sean aplicados en una dependencia específica, por ejemplo la Oficina de Control Interno.

5. Finalmente, las GUÍAS podrían incluir información sobre técnicas, configuraciones y secuencias de comandos recomendadas que deben seguir los usuarios para asegurar la información confidencial enviada y recibida a través del servicio de correo electrónico.

Nótese que, en muchas ocasiones, el término "política" es utilizado en un sentido genérico para aplicarlo a cualquiera de los tipos de requerimientos de seguridad expuestos. En este documento se llamará política, de manera genérica, a todos los requerimientos de seguridad mencionados antes y POLÍTICA (en mayúsculas) a las políticas propiamente dichas.

Hay varias etapas que deben realizarse a través de "la vida" de una política. Estas etapas pueden ser agrupadas en 4 fases.

1. Fase de desarrollo: durante esta fase la política es creada, revisada y aprobada.

2. Fase de implementación: en esta fase la política es comunicada y acatada (o no cumplida por alguna excepción).

3. Fase de mantenimiento: los usuarios deben ser concientes de la importancia de la política, su cumplimiento debe ser monitoreado, se debe garantizar su cumplimiento y se le debe dar mantenimiento (actualizarla)

4. Fase de eliminación: La política se retira cuando no se requiera más.

Creación: Planificación, investigación, documentación, y coordinación de la política

El primer paso en la fase de desarrollo de una política es la planificación, la investigación y la redacción de la política o, tomado todo junto, la creación. La creación de una política implica identificar por qué se necesita la política (por ejemplo, requerimientos legales, regulaciones técnicas, contractuales u operacionales); determinar el alcance y la aplicabilidad de la política, los roles y las responsabilidades inherentes a la aplicación de la política y garantizar la factibilidad de su implementación. La creación de una política también incluye la investigación para determinar los requerimientos organizacionales para desarrollar las políticas (es decir, que autoridades deben aprobarla, con quién se debe coordinar el desarrollo y estándares del formato de redacción), y la investigación de las mejores prácticas en la industria para su aplicabilidad a las necesidades organizacionales actuales. De esta etapa se tendrá como resultado la documentación de la política de acuerdo con los procedimientos y estándares de la empresa, al igual que la coordinación con entidades internas y externas que la política afectará, para obtener información y su aceptación. En general, la creación de una política es la función más fácil de entender en el ciclo de vida de desarrollo de una política.

Revisión: Evaluación independiente de la política

La revisión de la política es la segunda etapa en la fase de desarrollo del ciclo de vida. Una vez la documentación de la política ha sido creada y la coordinación inicial ha sido iniciada, esta debe ser remitida a un grupo (o un individuo) independiente para su evaluación antes de su aprobación final. Hay varios beneficios de la revisión independiente: una política más viable a través del escrutinio de individuos que tienen una perspectiva diferente o más vasta que la persona que redactó la política; apoyo más amplio

para la política a través de un incremento de involucrados; auento en el número de credibilidad en la política gracias a la información recibida de diferentes especialistas del grupo de revisión. Propio de esta etapa es la presentación de la política a los revisores, ya sea de manera formal o informal, exponiendo cualquier punto que puede ser importante para la revisión, explicando su objetivo, el contexto y los beneficios potenciales de la política y justificando por qué es necesaria. Como parte de esta función, se espera que el creador de la política recopile los comentarios y las recomendaciones para realizar cambios en la política y efectuar todos los ajustes y las revisiones necesarias para obtener una versión final de la política lista para la aprobación por las directivas.

Aprobación: Obtener la aprobación de la política por parte de las directivas

El paso final en la fase de desarrollo de la política es la aprobación. El objetivo de esta etapa es obtener el apoyo de la administración de la empresa, a través de la firma de una persona ubicada en una posición de autoridad.

La aprobación permite iniciar la implementación de la política. Requiere que el proponente de la política haga una selección adecuada de la autoridad de aprobación, que coordine con dicho funcionario, presente las recomendaciones emitidas durante la etapa de revisión y haga el esfuerzo para que sea aceptada por la administración. Puede ocurrir que por incertidumbre de la autoridad de aprobación sea necesaria una aprobación temporal.

Comunicación: Difundir la política

Una vez la política ha sido aprobada formalmente, se pasa a la fase de implementación. La comunicación de la política es la primera etapa que se realiza en esta fase. La política debe ser

inicialmente difundida a los miembros de la comunidad universitaria o a quienes sean afectados directamente por la política (contratistas, proveedores, usuarios de cierto servicio, etc.). Esta etapa implica determinar el alcance y el método inicial de distribución de la política (es posible que deban tenerse en cuenta factores como la ubicación geográfica, el idioma, la cultura y línea de mando que será utilizada para comunicar la política). Debe planificarse esta etapa con el fin de deterinmar los recursos necesarios y el enfoque que debe ser seguido para mejorar la visibilidad de la política.

Cumplimiento: Implementar la política

La etapa de cumplimiento incluye actividades relacionadas con la ejecución de la política. Implica trabajar con otras personas de la empresa, vicerrectores, decanos, directores de departamento y los jefes de dependencias (de división o de sección) para interpretar cuál es la mejor manera de implementar la política en diversas situaciones y oficinas; asegurando que la política es entendida por aquellos que requieren implementarla, monitorearla, hacerle seguimiento, reportar regularmente su cumplimiento y medir el impacto inmediato de la política en las actividades operativas. Dentro de estas actividades está la elaboración de informes a la administración del estado de la implementación de la política.

Excepciones: Gestionar las situaciones donde la implementación no es posible

Debido a problemas de coordinación, falta de personal y otros requerimientos operacionales, no todas las políticas pueden ser cumplidas de la manera que se pensó al comienzo. Por esto, es probable que se requieran excepciones a la política para permitir a ciertas oficinas o personas el no cumplimiento de la política. Debe establecerse un proceso para garantizar que las solicitudes de excepciones son registradas, seguidas, evaluadas, enviadas para aprobación o desaprobación, documentadas y vigiladas a través del periodo de tiempo establecido para la excepción. El proceso tam-

bién debe permitir excepciones permanentes a la política al igual que la no aplicación temporal por circunstancias de corta duración.

Concienciación: Garantiza la concienciación continuada de la política

La etapa de concienciación de la fase de mantenimiento comprende los esfuerzos continuos realizados para garantizar que las personas están concientes de la política y buscan facilitar su cumplimiento. Esto es hecho al definir las necesidades de concienciación de los diversos grupos de audiencia dentro de la organización (directivos, jefes de dependencias, usuarios, etc.); en relación con la adherencia a la política, determinar los métodos de concienciación más efectivos para cada grupo de audiencia (es decir, reuniones informativas, cursos de entrenamiento, mensajes de correo, etcétera); y desarrollo y difusión de material de concienciación (presentaciones, afiches, circulares, etc.). La etapa de concienciación también incluye esfuerzos para integrar el cumplimiento de la política y retroalimentación sobre el control realizado para su cumplimiento.

Monitoreo: Seguimiento y reporte del cumplimiento de la política

Durante la fase de mantenimiento, la etapa de monitoreo es realizada para seguir y reportar la efectividad de lo esfuerzos en el cumplimento de la política. Esta información se obtiene de la observación de los docentes, estudiantes, empleados y los cargos de supervisión, mediante auditorias formales, evaluaciones, inspecciones, revisiones y análisis de los reportes de contravenciones y de las actividades realizadas en respuesta a los incidentes.

Esta etapa incluye actividades continuas para monitorear el cumplimiento o no de la política a través de métodos formales e informales y el reporte de las deficiencias encontradas a las autoridades apropiadas.

Garantía de cumplimiento: Afrontar las contravenciones de la política

La etapa de garantía de cumplimiento de las políticas incluye las respuestas de la administración a actos u omisiones que tengan como resultado contravenciones de la política con el fin de prevenir que sigan ocurriendo. Esto significa que una vez una contravención sea identificada, la acción correctiva debe ser determinada y aplicada a los procesos (revisión del proceso y mejoramiento), a la tecnología (actualización) y a las personas (acción disciplinaria) involucrados en la contravención con el fin de reducir la probabilidad de que vuelva a ocurrir. Se recomienda incluir información sobre las acciones correctivas adelantadas para garantizar el cumplimiento en la etapa de concienciación.

Mantenimiento: Asegurar que la política esté actualizada

La etapa de mantenimiento esta relacionada con el proceso de garantizar la vigencia y la integridad de la política. Esto incluye hacer seguimiento a las tendencias de cambios en la tecnología, en los procesos, en las personas, en la organización, en el enfoque del negocio, etcétera, que puede afectar la política; recomendando y coordinando modificaciones resultado de estos cambios, documentándolos en la política y registrando las actividades de cambio. Esta etapa también garantiza la disponibilidad continuada de la política para todas las partes afectadas por ella, al igual que el mantenimiento de la integridad de la política a través de un control de versiones efectivo. Cuando se requieran cambios a la política, las

etapas realizadas antes deben ser revisitadas, en particular las etapas de revisión, aprobación, comunicación y garantía de cumplimiento.

Retiro: Prescindir de la política cuando no se necesite más

Después que la política ha cumplido con su finalidad y no es necesaria (por ejemplo, la empresa cambió la tecnología a la cual aplicaba o se creó una nueva política que la reemplazó) entonces debe ser retirada. La etapa de retiro corresponde a la fase de eliminación del ciclo de vida de la política, y es la etapa final del ciclo. Esta función implica retirar una política superflua del inventario de políticas activas para evitar confusión, archivarla para futuras referencias y documentar la información sobre la decisión de retirar la política (es decir, la justificación, quién autorizó, la fecha, etcétera).

Estas cuatro fases del ciclo de vida reúnen 11 etapas diferentes que deben seguirse durante el ciclo de vida de una política específica. No importa como se agrupen, tampoco importa si estas etapas son abreviadas por necesidades de inmediatez, pero cada etapa debe ser realizada. Si en la fase de desarrollo la empresa intenta crear una política sin una revisión independiente, se tendrán políticas que no estarán bien concebidas ni serán bien recibidas por la comunidad universitaria. En otras circunstancias, y por falta de visión, puede desearse omitir la etapa de excepciones de la fase de implementación, pensando equivocadamente que no existirán circunstancias para su no cumplimiento. También se podría descuidar la etapa de mantenimiento, olvidando la importancia de mantener la integridad y la vigencia de las políticas. Muchas veces se encuentran políticas inoficiosas en los documentos de importantes organizaciones, indicando que la etapa de retiro no está siendo realizada.

No sólo se requiere que las once etapas sean realizadas, algunas de ellas deben ser ejecutadas de manera cíclica, en particular

mantenimiento, concienciación, monitoreo, y garantía de cumplimiento.

Algunas prácticas recomendadas para escribir una política

Sin importar que una política se enuncie formal o informalmente, esta debe incluir 12 tópicos:

1. La declaración de la política (cuál es la posición de la administración o qué es lo que se desea regular)

2. Nombre y cargo de quien autoriza o aprueba la política

3. Nombre de la dependencia, del grupo o de la persona que es el autor o el proponente de la política

4. Debe especificarse quién debe acatar la política (es decir, a quién está dirigida) y quién es el responsable de garantizar su cumplimiento

5. Indicadores para saber si se cumple o no la política

6. Referencias a otras políticas y regulaciones en las cuales se soporta o con las cuales tiene relación

7. Enunciar el proceso para solicitar excepciones

8. Describir los pasos para solicitar cambios o actualizaciones a la política

9. Explicar qué acciones se seguirán en caso de contravenir la política

10. Fecha a partir de la cual tiene vigencia la política

11. Fecha cuando se revisará la conveniencia y la obsolescencia de la política

12. Incluir la dirección de correo electrónico, la página web y el teléfono de la persona o personas que se pueden contactar en caso de preguntas o sugerencias

Otras prácticas que se recomiendan seguir son:

1. Uso de lenguaje sencillo (evitar lenguaje técnico hasta donde sea posible)

2. Escribir la política como si fuese a utilizarse siempre

3. Debe escribirse de tal forma que pueda ser entendida por cualquier miembro de la empresa

4. Se debe evitar describir técnicas o métodos particulares que definan una sola forma de hacer las cosas

5. Cuando se requiera, hacer referencia explicita y clara a otras dependencias de la organización

6. Utilizar la guía para la presentación de documentos escritos de la empresa

Referencias

Fites, Philip and Martin P.J. Kratz., Information Systems Security: A Practitioner's Reference, London: International Thomson Computer Press, 1996.

Hutt, Arthur E., Seymour Bosworth, and Douglas B. Hoyt. Computer Security Handbook, 3rd ed., John Wiley & Sons, New York, 1995.

National Institute of Standards and Technology, An Introduction to Computer Security: The NIST Handbook , Special Publication 800-12, October 1995.

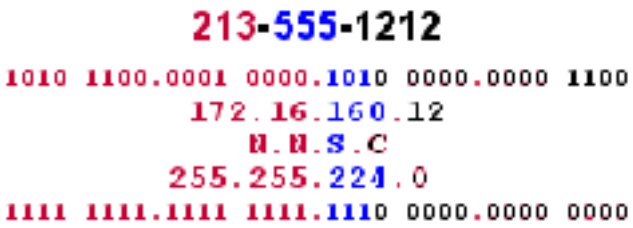
Peltier, Thomas R., Information Security Policies and Procedures: A Practitioner's Reference, Auerbach Publications, New York, 1999.

Tudor, Jan Killmeyer, Information Security Architecture: An Integrated Approach to Security in the Organization,Auerbach Publications, New York, 2001.

Texto traducido y adaptado de "The Security Policy Life Cycle: Functions and Responsibilities" de Patrick D. Howard, Information Security Management Handbook, Edited by Tipton & Krause, CRC Press LLC, 2003.

Autor: Universidad Nacional de Colombia

Capítulo 6: PRINCIPIOS BÁSICOS DE LAS SUBREDES



Todos sabemos, más o menos, que las redes sirven para que varios ordenadores puedan conectarse entre sí. En un mundo hipotético, todos los ordenadores podrían tener una IP distinta y pertenecer a la misma red.

Es decir, dos ordenadores, uno en China y otro en Cabo Verde podrían tener dos IP (194.223.0.25) y (123.456.789.001). Ambos ordenadores podrían verse en esa red sin ningún problema (de hecho en este caso, y sin firewalls por el medio, deberían poder verse).

Pero esto, aparte de no ser seguro, no tiene ningún sentido práctico. No me pondré a explicar el por qué las empresas necesitan rangos privados ni por qué se han definido unos estándares al respecto.

En una subred, todos los equipos comparten tres características comunes:

La dirección de red.

La dirección de broadcast.

Parte de sus direcciones IP son idénticas.

Toda subred necesita una dirección de red (que ayude a definir dicha subred), una dirección de broadcast (para mensajes a toda la red) y un rango de direcciones IP que puedan asumir los ordenadores y dispositivos que pertenecen a dicha subred. Esos ordenadores y dispositivos podrán verse entre sí de forma directa (esto es, sin necesidad de gateways, ni routers ni proxies).

Las direcciones IP de red y broadcast NO SON direcciones válidas para asignar a ordenadores ni dispositivos. Son necesarias para la existencia de la propia subred, por así decirlo.

La dirección de red es la primera del rango. La de broadcast la última. Todas las que quedan entre ambas son las que pueden asignarse a los equipos que formen parte de esa subred.

De acuerdo, tenemos un principio y un final, pero... ¿qué nos marca ese principio y ese final? ¡La máscara! Uniendo la máscara a la dirección de red obtenemos el rango de IP que conforma esa subred.

Por la forma en que se forman las máscaras, las subredes sólo pueden estar formadas por rangos que sean potencia (positiva) de 2. Sabiendo esto, y conociendo lo que hemos dicho anteriormente, sabemos que la subred viable más pequeña será de rango 4. ¿Por qué? Porque una de rango 2 tendrá sus IP copadas por la dirección de red y la de broadcast (no quedaría ninguna IP válida para asignar a ningún equipo). Por supuesto nos queda la subred de rango 1 (2 elevado a 0)... Eso NO es una subred, obviamente. Pero nos sirve para indicar que hablamos de UN ÚNICO ordenador (tema importante en tablas de enrutado).

Dicho esto, veamos las notaciones de las subredes. Vamos a poner los ejemplos para redes de clase C y menores. Luego se podrán extrapolar a redes de cualquier tamaño.

Comencemos con las notaciones. Primero veamos el estilo XXX.XXX.XXX.XXX para la máscara (el que más conoceréis alguno.. ¿os suena 255.255.255.0? Una máscara que define una subred de clase C).

La máscara se debe ver en binario, para entenderla bien, teniendo en cuenta que los 1 son los bits que deben coincidir y los 0 son las posibles variaciones. Cada subred tiene una IP (la más alta) como direccion de broadcast y otra (la mas baja) como dirección de red.

Recordemos que un byte son 8 bits y que una dirección IP (en IPv4) está formada por 4 bytes.

En los siguientes ejemplos omitiré los primeros 3 bytes en binario. Puesto que vamos a practicar con ejemplos para clases C los primeros 3 bytes serán 11111111.11111111.11111111. (= 255.255.255.)

Ejemplos:

- 255.255.255.240 = 16 posibilidades (14 IPs válidas) => 240 = 128+64+32+16 => 11110000 => 4 ceros => 2^4 posibilidades (=16)

Aquí vemos que, si disponemos de una clase C para repartir en subredes, con una máscara como la expuesta podemos construir 16 subredes de 16 IP cada una..

Por ejemplo:

192.168.0.0 - 192.168.0.15 (Dir. Red = 192.168.0.0; Dir. Broadcast = 192.168.0.15; Rango válido: 192.168.0.1 - 192.168.0.14).

La siguiente empezaría donde acabó la primera.

192.168.0.16 - 192.168.0.31 (Dir. Red = 192.168.0.16; Dir. Broadcast = 192.168.0.31; Rango válido: 192.168.0.17 - 192.168.0.30).

Y así continuaríamos hasta completar las 16 subredes independientes que podemos hacer con nuestra clase C (que en este caso es 192.168.0.0/255.255.255.0).

Otro ejemplo:

- 255.255.255.192 = 64 posibilidades (62 IPs válidas) => 192 = 128+64 => 11000000 => 2^6

Esto nos permitiría, siempre con nuestra clase C, construir 4 subredes con 64 IP cada una. Probad a definirlas.

Y así seguiríamos... Veámoslo:

- 0 = 256 posibilidades (254 IP) -> Clase C
- 128 = 128 posibilidades (126 IP)
- 192 = 64 posibilidades (62 IP)
- 224 = 32 posibilidades (30 IP)
- 240 = 16 posibilidades (14 IP)
- 248 = 8 posibilidades (6 IP)
- 252 = 4 posibilidades (2 IP)
- 254 = 2 posibilidades (ninguna IP) <- Obviamente NO es válida...

- 255 = 1 ordenador (no hay subred posible)

Por otro lado, tenemos la otra notación /xx (CIDR)

Esta se traduce como que usamos el número de bits detrás de la / para indicar el número de bits a "1" de la máscara... Es decir:

/24 = 24 bits a 1 => 3 bytes a 1 (255.255.255) => un byte a 0 => => 256 direcciones (254 IP válidas) -> Clase C

Obviamente si aumentamos un número a /24 (o sea, /25) significará que tenemos 25 bits a 1... sólo nos quedan 7 bits a 0... o sea, es lo mismo que

255.255.255.128 (o 128 posibilidades, justo la mitad => 126 IP válidas)

Nuestra correlación sería:

- /24 = 0 = 256 posibilidades (254 IP) -> Clase C
- /25 = 128 = 128 posibilidades (126 IP)
- /26 = 192 = 64 posibilidades (62 IP)
- /27 = 224 = 32 posibilidades (30 IP)
- /28 = 240 = 16 posibilidades (14 IP)
- /29 = 248 = 8 posibilidades (6 IP)
- /30 = 252 = 4 posibilidades (2 IP)
- /31 = 254 = 2 posibilidades (ninguna IP) <- Obviamente NO es válida...
- /32 = 255 (un ordenador y ninguna subred posible).

Lo mismo es válido si tenemos en cuenta una subred de más de 256 equipos. Simplemente iremos construyendo la máscara en función del número de bits (y siempre como potencia de 2).

- /23 = 254.0 = 2^9 = 512 posibilidades (510 IP válidas)
- /22 = 252.0 = 1024 posibilidades
- /21 = 248.0 = 2048 posibilidades
- /20 = 240.0 = 4096 posibilidades
- ...
- ...
- /16 = 255.255.0.0 = 2^16 = 65.536 -> Clase B
- ...
- ...
- /8 = 255.0.0.0 = 2^24 = 16.777.216 -> Clase A

Como véis, resulta ser de lo más simple.

Por cierto, un último apunte:

/0 = 0.0.0.0 = ¡Toda Internet!

Autor: Moebius para los foros de HackXcrack

Capítulo 7: EL MUNDO DE LA INFORMÁTICA FORENSE

La ciencia forense es sistemática y se basa en hechos premeditados para recabar pruebas para luego analizarlas. La tecnología, en caso de análisis forense en sistemas informáticos, son aplicaciones que hacen un papel de suma importancia en recaudar la información y pruebas necesarias. La escena del crimen es el ordenador y la red a la cual éste está conectado. Gran cantidad de documentos son elaborados digitalmente en ordenadores para ser a continuación impresos.

Las nuevas leyes sobre delitos informáticos y la de firmas electrónicas y mensajes de datos abren procesalmente y definitiva-

mente los medios probatorios informáticos. Las operaciones comerciales tienden claramente a reducir costos y ampliar mercados a través de las redes informáticas.

Ya se han producido algunas experiencias en Venezuela y otros países de habla hispana uno de los más destacados es España, en las cuales se ha solicitado la determinación de la autenticidad e integridad por ejemplo de mensajes de e-mail pudiéndose relacionar con un remitente, dirección de correo, ordenador y hasta con una persona determinada e inclusive la relación entre estos elementos y los datos anexos (adjuntos) que se encontraban en el e-mail almacenado previamente en el equipo.

Es posible investigar (aún cuando Internet permite el anonimato y el uso de nombres falsos) quién es el dueño de sitios web, quiénes son los autores de determinados artículos y otros documentos enviados a través de redes o publicados en la misma. El rastreo depende en sí de quien y como realizó el ataque o cualquier otra acción, es posible buscar atacantes exteriores de sistemas e incluso se conocen casos donde se ha determinado la autoría de virus.

Son igualmente investigables las modificaciones, alteraciones y otros manejos dolosos de bases de datos de redes internas o externas, así como de cualquier sistema de redes, ataques internos. Por supuesto, para realizar esta tarea se debe poseer un conocimiento sólido (normalmente quienes hacen de informáticos forenses han realizados ataques anteriormente o conocen el uso de herramientas, dispositivos y software de incursión en redes; por lo que tienen una idea de las posibles intrusiones por parte de terceros en un sistema).

La destrucción de datos y la manipulación de los mismos también pueden rastrearse. Los hábitos de los usuarios de los ordenadores y las actividades realizadas pueden ayudar a la reconstrucción de hechos, siendo posible saber de todas las actividades realizadas en un ordenador determinado.

Los archivos informáticos pueden guardar información sobre su autor, la compañía, fecha y otros datos de interés jurídico. Esta información es almacenada a espaldas del usuario, pudiendo

determinarse en algunos casos en qué ordenador/estación fue redactado el archivo (esto es poco fiable, ya que cualquier otra persona pudo trabajar con el PC, falsificando la identidad del usuario propietario de la estación, pero es usado como base del procedimiento).

Las imágenes digitales y otros medios audiovisuales pueden estar protegidos no solo por derechos de autor (copyright) sino por las llamadas marcas de agua digitales que servirían para determinar el origen del archivo, aunque hayan sido modificados para disfrazarlos y darle una apariencia distinta.

Ya son frecuentes las inspecciones judiciales sobre páginas Webs y archivos, tendientes a la fijación de hechos que ocurren dentro del vasto mundo electrónico digital.

La promoción, evacuación y control de estas experticias informáticas es especial y bajo las normas de naciente, pero desarrollada informática forense que se pone al servicio inmediato del derecho para afrontar nuevas tareas probatorias y lo más importante es que ya se puede contar en Venezuela y en otros países con este tipo de pericias útiles en los procesos judiciales del presente y del futuro.

El objetivo de un análisis forense informático es realizar un proceso de búsqueda detallada y minuciosa para reconstruir a través de todos los medios el log de acontecimientos que tuvieron lugar desde el mismo instante cuando el sistema estuvo en su estado integro hasta el momento de detección de un estado comprometedor.

Esa labor debe ser llevada acabo con máxima cautela y de forma detallada, asegurándose que se conserva intacta, en la medida de lo posible, la información contenida en el disco de un sistema comprometido, de forma similar a los investigadores policiales que intentan mantener la escena del crimen intacta, hasta que se recogen todas las pruebas posibles.

Juan Carlos Guel, jefe del Departamento de Seguridad en Cómputo de la Dirección General de Servicios de Cómputo Académico y Coordinador del Equipo de Respuesta a Incidentes en Seguridad en Cómputo UNAM-CERT (no estoy al tanto que aún

posea este cargo), señala: "*informática o cómputo forense es un conjunto de técnicas especializadas que tiene como finalidad la reconstrucción de hechos pasados basados en los datos recolectados, para lo cual se procesa la información que pueda ser usada como evidencia en un equipo de cómputo*".

Es decir, el cómputo forense opera diversas herramientas informáticas para determinar el estado de un sistema luego que sus medidas de seguridad han sido sobrepasadas y vulneradas, con la finalidad de encontrar evidencias que permitan definir, con toda certeza, los mecanismos que los intrusos utilizaron para acceder a ella, así como de desarrollar las mejoras y/o técnicas que deben seguirse para evitar futuras incursiones ajenas en el sistema.

En una entrevista realizada por virusprot al Doctor Jeimy J.Cano, Ingeniero de Sistemas y Computación Universidad de los Andes (Colombia) en el año 2002, y cito textualmente la pregunta:"*¿Cuánto se puede tardar en reunir las suficientes pistas que den con el autor de un ataque?*", éste respondía:

"*Es una pregunta complicada de responder, pues muchas veces el informático forense debe prepararse para fallar en la identificación de la persona real que cometió el ataque. Pues la versatilidad que ofrece Internet para enmascarar direcciones IP, correos electrónicos, entre otros aspectos, sugiere un gran conocimiento técnico y paciencia por parte de los atacantes, los cuales también consideran estrategias "anti-forenses" que limiten las investigaciones y la efectividad de las mismas. Luego, la recolección de pista puede ser demorada; algunos casos pueden llevar años en esta labor.*"

Las herramientas que utilizan los peritos forenses en materia de cómputo para dar con los intrusos, y saber a ciencia cierta qué hicieron en el sistema, se han desarrollado al paso del tiempo, para que nos ayuden en cuestiones de velocidad y faciliten identificar lo que realmente le pasó al sistema y qué es lo que le puede suceder; en su contraparte igualmente se han desarrollado herramientas bastantes sofisticadas en contra de los análisis forenses (herramientas y técnicas que intentan no dejar rastros, camuflarlos o borrarlos, de tal manera que se dificulte una posterior investigación.), tal como lo indica el Dr. Jeimi Cano.

De allí el personal que trabaje en la informática forense deberá poseer sólidos conocimientos técnicos y prácticos y conocer las herramientas de uso, estar al día en bugs (vulnerabilidades) de sistemas (Sistemas operativos, software y hardware)

El campo de la seguridad informática es inmensamente heterogéneo e interesante. Analizar un entorno atacado y comprometido es un desafiante ejercicio de aplicación de ingeniería inversa, para el cual es necesario tener gran conocimiento del funcionamiento de los sistemas involucrados, las técnicas de ataque y los rastros que dejan las mismas.

Se puede leer en diferente sitios web notas similares a estas: "*Espero que los nuevos empleados tengan un mínimo de conocimientos de informática y software forense antes de que lleguen a la puerta*", apunta Marc Kirby, detective inspector para la sección de informática forense de la británica Unidad Nacional de Crimen de Alta Tecnología (NHTCU). Saque sus conclusiones de ese párrafo.

Debemos tener en cuenta que la prioridad es preservar lo más íntegramente posible las evidencias del crimen en un estado íntegro. Eso significa colocar el sistema fuera de servicio (offline) cuando todos los usuarios del sistema están presionando para volver a ponerlo on-line.

Si el sistema, por parte del administrador, fue forzado a seguir funcionando, eliminando las posibles vulnerabilidades o cualquier otra supuesta vía de acceso al servidor, la investigación forense no podrá seguir el rumbo correcto ya que:

1. Se eliminaría cualquier posibilidad de persecución del intruso en un futuro, ya que se modifica la "escena del crimen" y no se podría calcular los daños estimados con un grado elevado de certeza.

2. Hay muchas posibilidades de que se pase algo importante por alto al administrador y el intruso (o intrusos) sigan teniendo acceso al sistema. Por lo tanto es mejor sufrir un "downtime" de red, mientras que se realiza el análisis forense del sistema.

Se tiene que establecer una prioridad entre:

(a) Funcionamiento inmediato, teniendo presente que las huellas dejadas por el/los intruso(s) pueden haberse eliminado por descuido del administrador y su equipo, y que el servidor pueda seguir teniendo puertas traseras bien ocultas. Esta opción permite estar operativo en poco tiempo.

(b) Investigación forense detallada. Esta opción supone un mayor tiempo de permanencia offline sí no existen planes de contingencia y procedimientos para el backup del servicio.

Bases de la Informática Forense:

Experticias, Auditoria e Inspecciones en ordenadores y Páginas Web.

Ubicación de origen de correos anónimos y archivos anexos.

Determinación de propietarios de Dominios .com .net .org y otros.

Pruebas de violación de derechos de autor.

Control preventivo y restricción de uso de ordenadores e Internet.

Protección de información y derechos de autor.

Recuperación de data y archivos borrados intencionalmente o por virus.

Recuperación y descifrado de las claves.

Al realizar un análisis de informática forense es necesario tomar notas de lo que se hace con el disco duro, y a qué hora, almacenándolo en una ubicación segura como por ejemplo una caja fuerte. Es recomendable que siempre que se trabaje con el medio original esté acompañado por un colega, para que conste a los efectos legales y el testimonio pueda ser confirmado por alguien con un nivel de conocimientos similar.

Las copias deben ser hechas bit-por-bit, es decir será necesario hacer imágenes del disco. La investigación debe ser llevada sobre una copia y nunca sobre el disco original. Se debe hacer tres copias del disco duro original. Sobre todas las copias y original se debe llevar a cabo una verificación criptográfica - un checksum. En lo posible realizar dumps de memoria y almacenarlos al igual que los discos.

Es importante que todos los hechos pertinentes al caso durante la preparación, recuperación y análisis de las pruebas sobre un ataque sean anotados para poder desarrollar un informe detallado de incidencia que se debe preparar una vez terminado el análisis. Este documento deberá servir como una prueba del incidente o compromiso. Siempre que se realiza cualquier apunte al cuaderno, el asistente debe tener completo conocimiento y entendimiento de lo que ha sido apuntado.

Antes de apagar el sistema, será útil recoger algunos ejemplos de aquella información que posiblemente no ha sido cambiada por los intrusos, como la organización de sistema de ficheros logs, el nombre del host, su dirección IP del fichero e información de algunos dispositivos.

El análisis de la comunicación de datos es realmente importante. Allí se trabajaran en dos actividades:

1. Intrusión en una red de ordenadores o mal uso de la misma.

2. Interceptación de datos.

La intrusión en una red de ordenadores o mal uso de la misma es la actividad de la informática forense principal cuando el análisis se hace sobre estructuras de esta naturaleza. Consiste en las funciones siguientes:

a) Detección de la intrusión.

b) Detectar la evidencia, capturarla y preservarla; y

c) Reconstrucción de la actividad específica o del hecho en sí

El descubrimiento de la intrusión generalmente involucra la aplicación de software especializado y en algunos casos hardware, para supervisar la comunicación de los datos y conexiones a fin de identificar y aislar un comportamiento potencialmente ilegal.

Este comportamiento incluye el acceso no autorizado, modificación del sistema en forma remota y la monitorización no autorizada de paquetes de datos.

La captura de la evidencia y su preservación, generalmente tiene lugar después del descubrimiento de una intrusión o un comportamiento anormal, para que la actividad anormal o sospechosa pueda conservarse para el posterior análisis.

La fase final, la reconstrucción de la intrusión o comportamiento anormal, permite un examen completo de todos los datos recogidos durante la captura de la evidencia.

Para llevar a cabo con éxito estas funciones, el investigador forense debe tener experiencia en comunicación de datos y el apoyo de ingenieros y/o técnicos de software.

Antes de realizar un análisis se debe tener en cuenta la siguiente información:

sistema operativo afectado.

inventario de software instalado en el equipo

tipo de hardware del equipo

accesorios y/o periféricos conectados al equipo

si posee firewall

si esta en el ámbito del DMZ (Zona desmilitarizada)

conexión a Internet

configuración

parches y/o actualizaciones de software

políticas de seguridad implementadas

forma de almacenamiento de la información (cifrada o no)

personas con permisos de acceso al equipo

el PC esta dentro del DMZ

existe IDS

cuántos equipos en red

Recomiendo como lectura interesante a:

Sistemas de Detección de Intrusiones de Diego González Gómez

http://www.dgonzalez.net/pub/ids/html/

Interesante artículo enviado por Antonio Javier G.M.

http://www.analisisforense.net/SIC59_074-084.pdf

Algunos Software/herramientas aplicables en la informática forense:

. F.I.R.E.: Destaca dentro de las distribuciones linux específicas para informática forense

Sitio web: http://biatchux.dmzs.com

. WinHex: Software para informática forense y recuperación de archivos, Editor Hexadecimal de Archivos, Discos y RAM

Sitio web: http://www.x-ways.net (shareware)

. Encase: Herramienta propietaria, la cual ha demostrado ser un dispositivo útil a los peritos forenses en diferentes casos.

sitio web: http://www.guidancesoftware.com/

. Snort Herramienta libre por excelencia una de las mejores

Sitio web: http://www.snort.org

. Ossim: Herramienta de monitorización

Sitio web:http://www.ossim.net

. Ettercap: Excelente sniffer de redes

Sitio web: http://ettercap.sourceforge.net/

. NMap: Potente localizador de vulnerabilidades

Sitio web: http://www.insecure.org/nmap/

. Nessus: Otro proyecto para scanear vulnerabilidades

Sitio web: http://www.nessus.org

. Ethereal: Otro potente sniffer

Sitio web: http://www.ethereal.com

.Fport: Identifica puertos abiertos y aplicaciones asociadas a ellos.

Sitio web: http://foundstone.com/

. putty: Escelente cliente SSH

Sitio web:
http://www.chiark.greenend.org.uk/~sgtatham/putty/

. Stunnel: Programa que cifra las conexiones TCP bajo SSL

Sitio web: http://www.stunnel.org/

. AirSnort: Herramienta wireless para recuperar claves cifradas

Sitio web: http://airsnort.shmoo.com/

. Aircrack: sniffer y WEP craqueador de wireless

Stio web: http://www.cr0.net:8040/code/network/

. Achilles: Herramienta para testear la seguridad de las aplicaciones web

sitio web: http://www.mavensecurity.com/achilles

. NetStumbler Localizador de los puntos de acceso wirless
(debes poseer tarjeta wirless para que funcione)

Sitio web: http://www.stumbler.net/

.Dsniff: sniffer

Sitio Web: http://www.datanerds.net/~mike/dsniff.html

.VNC Administrador remoto

Sitio web: http://www.realvnc.com/

.The Autopsy: Browser para la informática forense

Sitio web: http://www.sleuthkit.org

.PyFlag: Herramienta para recuperar discos en RAID

Sitio web: http://pyflag.sourceforge.net/

Herramientas Microsoft:

. Promqry 1.0 (linea de comandos, 113 KB):

http://download.microsoft.com/download/b/b/6/bb6ea193-2880-43c3-b84b-b487a6454a17/promqrycmd.exe

. PromqryUI 1.0 (interfaz gráfico, 255 KB):

http://download.microsoft.com/download/7/2/6/7262f637-81db-4d18-ab90-97984699d3bf/promqryui.exe

Sitios web de seguridad (recomendados)

http://www.kb.cert.org

http://www.securityfocus.com

http://www.sqlsecurity.com

http://www.secunia.com

http://www.securitytracker.com

http://www.forensicfocus.com/

http://www.frsirt.com

http://www.hispasec.com

http://www.seguridad0.com

http://www.forensic-es.org

http://www.synacksecurity.com

Fuentes consultadas:

tecnoiuris.com

informaticaforense.com

criptored.upm.es

loquefaltaba.com

grafotecnica.com

virusprot.com

obm.corcoles.net

dgonzalez.net

vnunet.es

unam-cert.unam.mx

alfa-redi.org

ausejo.net

symantec.com

pandasoftware.com

monografias.com

criminalista.net

delitosinformaticos.com

hispasec.com

synacksecurity.com

unmanarc.synacksecurity.com

Autor: Xombra, www.xombra.com

Capítulo 8: LA IMPORTANCIA DE UNA BUENA CONTRASEÑA

Las claves o contraseñas, de un tipo u otro, forman parte de nuestra vida cotidiana. Las utilizamos para nuestro móvil, alarma de casa y oficina, sacar dinero de cajeros, y en el tema que nos aplica: correo electrónico, FTP, cuentas bancarias, etcétera . Muchas veces la contraseña es la única vía de acceso a los servicios.

Al referirnos a poner una contraseña 'fuerte', expresamos cuál es la dificultad que ofrece ésta ante alguien (o algo) que está intentando descubrirla. Una contraseña será más fuerte cuando ofrezca mayores dificultades para que el atacante la identifique. Por el contrario, será más débil cuando sea relativamente simple descubrirla. Será mucho más difícil localizar una clave como 'jz7iit16' , que una palabra común como 'gato'.

Algo análogo sería poner un candado pequeño o grande para nuestra puerta.

Una buena forma de demostrar la necesidad de utilizar contraseñas fuertes es mostrar la facilidad con que las contraseñas débiles pueden ser identificadas. La mayoría de los usuarios no tienen ni idea de la existencia de herramientas para descubrir contraseñas, ni de lo realmente fáciles y eficientes que son (y en muchos casos, incluso totalmente gratuitas). Es realmente un ejercicio muy aleccionador obtener una copia de la SAM de un dominio de Windows, pasarla por una herramienta de análisis y ver cómo, instantáneamente, obtenemos la contraseña de una gran cantidad de usuarios.

Evidentemente el problema de la calidad de las contraseñas no es exclusivo de Windows, sino que puede aplicarse a cualquier entorno en donde se utilice este tipo de autenticación.

Objetivo: mejorar la calidad de las contraseñas

La política de seguridad existente en cada organización debe fijar los requerimientos para que una contraseña se considere aceptable dentro del ámbito de la misma. No obstante, me permito sugerir una serie de valores que son comunmente aplicados:

Todas las cuentas de usuario, sin excepción, deben de tener asociada una contraseña.

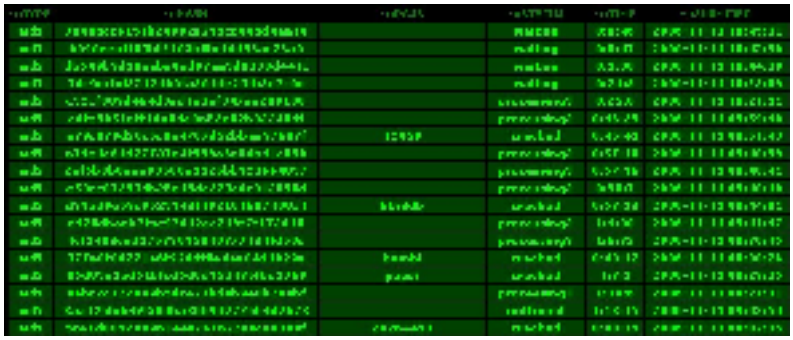
- El usuario, en su primera conexión a la red, debe ser forzado a cambiar de contraseña.
- La longitud de las contraseñas no debe ser inferior a los siete caracteres.
- Las contraseñas deben estar formadas por una mezcla de caracteres alfabéticos (donde se combinen las mayúsculas y las minúsculas) y números.
- La contraseña no debe contener el identificador o el nombre del usuario.

- Las contraseñas deben caducar, como máximo, cada noventa días. El período mínimo de validez de una contraseña debe ser un día.
- Cuando se realice un cambio de contraseña, ésta debe ser diferente de las utilizadas anteriormente por el mismo usuario.
- Periódicamente debe realizarse una auditoría para verificar que se cumple con los requerimientos de la política de seguridad.

Como conclusión, en contra de lo que pueda parecer, la seguridad informática está siendo olvidada por la mayoría de empresas, hasta que ocurre algo indeseado. No son las máquinas las que fallan, sino las personas que efectuamos prácticas incorrectas (dejar la contraseña visible en la oficina, dejarnos sesiones abiertas, etcétera). Con las recomendaciones aportadas podemos evitar estos errores. Como conclusión hay que añadir que si se cierra la puerta cuando se sale de casa, lo mismo se debe hacer al usar sistemas y servicios en Internet.

Autor: Josep Pocalles

Capítulo 9: ¿QUÉ ES Y CÓMO FUNCIONA LA INTEGRIDAD MD5?



MD5 es un algoritmo que se suele utilizar para realizar la comprobación de la integridad de ficheros binarios, siendo muy utilizado para, por ejemplo, la posterior verificación de imágenes ISO o programas descargados de Internet.

Realmente es muy utilizado por su sencillez de uso, potencia y popularidad, siendo relativamente sencillo el comprobar si un determinado archivo se ha descargado correctamente o por el contrario ha ocurrido algún problema y el programa o imagen ISO es inutilizable. Así, en el mundo Linux, es muy habitual encontrar las sumas de control MD5 de todos los paquetes que componen la distribución.

Veamos lo anterior en forma de ejemplo. Supongamos que tengo el fichero pepe.zip y quiero distribuirlo en Internet. Como se supone que es un archivo bastante grande y quiero facilitar que cualquiera lo pueda descargar, lo que puedo hacer es añadir un

pequeño fichero de texto (o dejarlo en la web desde la que se produce la descarga) con el resultado de la ejecución del comando md5sum (o en algunos sistemas simplemente md5) sobre el archivo en cuestión. Y añado este archivo a la distribución del fichero.

Ahora, si alguien descarga pepe.zip, para verificar la integridad del fichero simplemente tendrá que comprobar la suma de control obtenida: el md5. Si coincide la suma md5 con el contenido del fichero de texto que contiene el resultado md5 incluido por el autor, es que la integridad del fichero es buena. Nos podemos fiar.

md5sum suele venir incluido dentro del paquete GNU textutils (ftp://ftp.gnu.org/gnu/textutils/). En Windows no viene utilidad alguna por defecto. Sin embargo, se puede localizar un programa llamado wxChecksums que verifica y calcula ficheros md5 en http://wxchecksums.sourceforge.net/. Aquí hay un manual donde se detalla cómo verificar mútiples archivos: http://wxchecksums.sourceforge.net/manual/en/manual.html y la creación de los mismos.

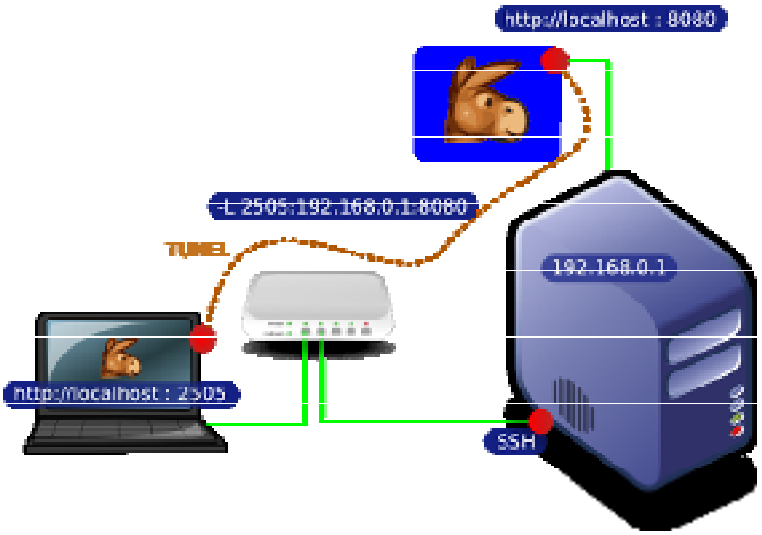
md5 se utiliza también por motivos de seguridad. De forma que permite saber si un determinado fichero ha sido fraudulentamente modificado.

Enlaces de interés:

rfc1321: The MD5 Message-Digest Algorithm

http://www.ietf.org/rfc/rfc1321.txt

Capítulo 10: INTRODUCCIÓN AL SSH



Secure Shell (ssh) es un programa que permite realizar conexiones entre máquinas a través de una red abierta de forma segura, así como ejecutar programas en una máquina remota y copiar archivos de una máquina a otra. Tal y como se explica en el RFC de Secure Shell:

"SSH(Secure Shell) es un programa para conectarse a otros equipos a través de una red, para ejecutar comandos en una máquina remota y para mover archivos de una máquina a otra. Proporciona una exhaustiva autenticación y comunicaciones seguras en redes no seguras".

Ssh provee fuerte autenticación y comunicación segura sobre un canal inseguro y nace como un reemplazo a los comandos telnet, ftp, rlogin, rsh, y rcp, los cuales proporcionan gran flexibili-

dad en la administración de una red, pero sin embargo, presenta grandes riesgos en la seguridad de un sistema. Adicionalmente, ssh provee seguridad para conexiones de servicios X Windows y envío seguro de conexiones arbitrarias TCP.

Secure Shell admite varios algoritmos de cifrado entre los cuales se incluyen:

- Blowfish
- 3DES
- IDEA
- RSA

La ventaja más significativa de ssh es que no modifica mucho las rutinas. En todos los aspectos, iniciar una sesión de ssh es tan sencillo como (y similar a) iniciar una sesión de telnet. Tanto el intercambio de llaves, la autenticación, así como el posterior cifrado de sesiones son transparentes para los usuarios.

¿ De qué Previene Secure Shell?

Debido a la promiscuidad de la interfaz ethernet, se genera una problemática sobre los siguientes servicios de red usados en la actualidad, tales como:

- telnet
- ftp
- http

- rsh
- rlogin
- rexec

Ello nos representa un problema importante, ya que, incluso en un entorno de red cerrado, debe existir como mínimo un medio seguro para poder desplazar archivos, hacer copia de archivos, establecer permisos, ejecutar archivos, scrips, etc, a través de medios seguros.

Por ello para evitar que determinadas personas capturen el trafico diario de la red, es conveniente instalar el Secure Shell(SSH).

Entre los ataques más comunes que nos previenen Secure Shell están:

- Sniffering(Captura de trafico)
- IP Spoofing
- MACpoofing
- DNS Spoofing
- Telnet Hickjacking
- ARP Spoofing
- ARP Spoofing
- IP Routing Spoofing
- ICMP Spoofing

Protocolos de Secure Shell

Existen actualmente dos protocolos desarrollados sobre ssh:

SSH1: La última versión de ssh cliente/servidor para Unix que soporta este protocolo es la 1.2.31, esta puede ser utilizada libremente para propósitos no comerciales y es ampliamente usada en ambientes académicos.

SSH2: Provee licencias más estrictas que SSH1 ya que es de carácter comercial. La última versión de ssh cliente/servidor para Unix con este protocolo es la 2.4.0 y puede ser utilizada libremente respetando la licencia expresa.

OpenSSH es una versión libre de los protocolos SSH/SecSH bajo licencia BSD y es totalmente compatible con los protocolos SSH1 y SSH2.

¿Dónde obtener el Secure Shell?

Secure Shell cliente/servidor para sistemas Unix

Sitio FTP de Secure Shell

http://ftp.ssh.com/pub/ssh

Sitio FTP de OpenSSH

http://www.openssh.com/ftp.html

Secure Shell cliente para sistemas Windows

Putty

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

WinSCP

http://winscp.sourceforge.net/eng/

Tunnelier:

http://www.bitvise.com/tunnelier.html

Secure Shell servidor para sistemas Windows

WinSSHD

http://www.bitvise.com/winsshd.html

Instalación de servidor WinSSHD

http://www.bitvise.com/winsshd-users-guide.html

Artículo original completo:

Departamento de Seguridad en Cómputo UNAM
http://www.ipicyt.edu.mx/cns/ManualUsoSecureShellDGSCA-UNAM.htm