POLITICA DE SEGURIDAD

Por: Alejandro Corletti (acorletti@hotmail.com)

La RFC 1244 se refiere a los distintos aspectos a tener en cuenta para la confección de la política de seguridad de una red. A través de este texto se tratará de llevar a la práctica los aspectos fundamentales de la misma e incluir la mecánica a seguir para la elaboración de las distintas actividades referidas a seguridad, no expresadas en la RFC.

Como introducción, fuera de lo que especifica la norma, se tratará de establecer una diferencia básica que se tiene en cuenta en Administración y Conducción. Al tratar todo tipo de problemas, se establece una gran diferencia entre el marco estratégico y el de planeamiento y ejecución. El marco estratégico es quién define las políticas a seguir en líneas generales, es el enfoque macro. Los elementos de Conducción y ejecución sí son los que efectivizan el detalle planificando y ejecutando las acciones.

Siguiendo este lineamiento es que a lo largo de este texto se tratará de diferenciar claramente la Política de seguridad (Estrategia) del Plan de seguridad (Ejecución).

Para iniciar esta actividad, es necesario entonces comprender que los responsables de la creación del plan y política de seguridad son los responsables de la toma de decisiones y el personal técnico que las llevarán a cabo. Una vez definidos todos sus pasos, pasarán también a ser responsables la totalidad de los usuarios de la Organización, por quienes pasan la masa de los puntos claves y deberán conocer sus derechos y obligaciones al respecto.

1. Política de seguridad:

El primer paso entonces es definir la estrategia que se desea para la seguridad de la Organización. Para esta actividad, el Directorio deberá tener en cuenta lo siguiente:

- Grado de exposición al que se desea llegar:
- Cantidad de información que se desea exponer:
- Metodología de trabajo en el sistema informático de la Organización:
- Grado de acercamiento con otras entidades:
- Importancia de la seguridad dentro de la Organización:
- Presupuesto que se desea invertir para esta tarea:
- Personal que se dedicará al tema:
- Grado de compromiso del más alto nivel:

Luego del análisis de cada uno de estos Item y con las pautas claras al respecto es cuando puede comenzar a elaborarse el Plan de seguridad, el cual deberá realimentar muchas de las decisiones tomadas en la Política, generando con esto un Feedback permanente, característico de todo proceso dinámico.

2. Plan de Seguridad:

2.1. Análisis de riesgo:

La primera actividad para la implementación del Plan es determinar que es lo que se necesita proteger y cómo hacerlo. Este es el proceso de analizar todos los riesgos y clasificarlos acorde a algún tipo de prioridad. Existen dos tipos de elementos que se deben identificar en este análisis:

2.1.1. Identificación de recursos:

Son los elementos físicos que se necesitan proteger, estos deben contener:

- Hardware: CPU, terminales, workstations, PC, discos, líneas de comunicaciones, Servidores, Hub, Switch, Router, etc.
- Software: Programas fuente y objeto, utilitarios, sistemas operativos, programas de comunicaciones, etc.
- Datos: Durante la ejecución, Almacenamiento en línea y fuera de línea, backups, registros de auditorías, bases de datos, información en tránsito.
- Personas: Usuarios, personal necesario para la ejecución de sistemas, programadores, etc.
- Documentación: De programas, de hardware, de sistemas, procedimientos.
- Auxiliares: papeles, formularios, medios magnéticos, CD, etc.

2.1.2. Identificación de actividades:

En estas se puede determinar qué potencial de pérdida puede existir.

- Accesos no autorizados: Autorización de empleo de cuentas de usuarios por otras personas, uso de recursos sin autorización.
- Desbloqueo de información: La modificación de permisos sobre recursos es el más común.
- Negación de servicio: Esta actividad se puede presentar de distintas formas y afectará a los distintos usuarios de manera diversa.

2.2. Lineamiento del plan:

Una vez analizados los riesgos es importante trazar los primeros lineamientos generales del plan, aquí se especificarán los problemas globales a considerar, en general estos son:

2.2.1. Quién está autorizado a usar los recursos?

En este punto se inicia el análisis de los distintos niveles de acceso a recursos, dando el enfoque inicial a los futuros grupos de acceso a recursos.

2.2.2. Cuál es el uso correcto de recursos?

Se trata aquí de especificar un guía de acceso a los diferentes tipos de usuarios, aclarando fehacientemente qué es lo correcto y lo incorrecto, definiendo cuáles son los límites de cada uno, debe quedar sumamente claro las responsabilidades de las acciones llevadas a cabo. Un detalle a tener en cuenta también es el alcance legal del copiado de Software, acorde a la política de licencias de la Organización

En redes con buena capacidad de administración, se puede fomentar la actividad de investigación de vulnerabilidades, esto quiere decir que usuarios autorizados pueden desarrollar actividades de "Hackers" para colaborar con la administración de seguridad, detectando fallas tempranamente. Si se desea llevar a cabo esta actividad, es imprescindible dedicar varios apartados del Plan para dejar claramente especificado que se debe y que no se debe hacer, hasta dónde se puede llegar y los procedimientos ante cada uno de los avances. En estos casos, una buena medida es aislar segmentos de red para estas tares, con la finalidad de poder testearlos e identificar los "propios de los ajenos"

2.2.3. Quién está autorizado a crear usuarios y conceder accesos?

Si no se tiene control sobre quién autoriza los accesos, no se podrá controlar sobre quienes usan el sistema. Es una muy buena medida especificar procedimientos para la creación de cuentas y asegurarse que el personal que lo realiza conozca bien estas normas.

El garantizar el acceso a usuarios es una de las vulnerabilidades más grandes de un sistema. Un detalle importante a tener en cuenta es la metodología de selección de contraseñas (este tema se tratará más adelante)

Se plantea aquí uno de los puntos claves de seguridad:

Se centralizarán los accesos o existirán múltiples puntos ?

Siempre cuanto más centralizado sean los mismos, más seguro será el sistema.

2.2.4. Quiénes pueden tener privilegios administrativos?

Esta es una decisión de suma importancia, pues inevitablemente se deberá designar a un cierto grupo de personas para poseerlos.

2.2.5. Cuáles son las responsabilidades de los administradores del sistema?

En particular se deben tener en cuenta los aspectos relacionados a la información propietaria de los distintos usuarios de la red como así también el análisis de trafico o correo electrónico, el acceso a bases de datos, etc.

2.2.6. Qué hacer con la información sensible?

Se planifican aquí las distintas estrategias de resguardo y recuperación de información en diferentes modos (Discos, tape, CD, etc).

2.2.7. Que sucede si el plan es violado?

Existen distintos tipos de violaciones al plan, cada una de las cuales deberá ser tratada de manera diferente, esta pueden ser por:

- Negligencia individual:
- Accidente:
- No haber sido correctamente informado de las medidas de seguridad:
- No entendimiento del plan:

Lo importante es la rápida reacción y la determinación de cómo y por qué se produjo. Se deberá determinar la respuesta a la violación.

2.2.8. Proceder ante incidentes:

Existen dos estrategias básicas a tener en cuenta ante un incidente de seguridad:

- Proteger y proceder: La premisa de esta es la preservación de los componentes del sistema, el gran problema es que si el intruso no pudo ser identificado, este podrá regresar por la misma puerta o por algún otra.

  Qué premisas se deben tener en cuenta para implementar esta estrategia?

  * Si los recursos no están bien protegidos.
  * Si existe un riesgo económico de magnitud al continuar la intrusión.
  * Si no existe la posibilidad de perseguir al intruso.
  * Si los usuarios no poseen conciencia de seguridad y sus recursos peligran.
  * Si los recursos no están claramente establecidos.

- Seguir y perseguir: Se permite al intruso continuar sus actividades hasta identificarlo y evidenciar las vulnerabilidades del sistema que fueron aprovechadas. Se requiere aquí conocimiento en el manejo de incidentes y herramientas adecuadas pues se está arriesgando demasiado. La gran ventaja de este proceder es que es la única forma eficiente de llegar a las causas del problema para que este no vuelva a repetirse.

  Qué premisas se deben tener en cuenta para implementar esta estrategia?

  * Si los recursos y sistemas están bien protegidos.

* Si se dispone de buenos backup.

* Si la frecuencia de ataques es considerable.

* Si el acceso de intrusos puede ser controlado.

* Si se posee la capacitación suficiente para enfrentar un ataque.

* Si existen contactos con otros organismos que puedan prestar apoyo ante ataques.

* Si existe soporte legal en la organización para responder ante estos casos.

2.2.9. Publicación del plan:

La última actividad que se debe considerara es cómo se difunde el plan a los usuarios del sistema, para esta actividad se deben tener en cuenta varios aspectos referidos al dinamismo de las actualizaciones, al carácter reservado del plan, al acuse recibo de su lectura, a las correcciones, al cumplimiento y control, etc.

3. Análisis de detalle:

Habiendo definido ya qué necesita ser protegido, qué es lo más importante y cuáles son sus prioridades, es el momento de diseñar **cómo** hacerlo. Esta actividad es la que se tratará en este punto.

3.1. Identificación de problemas reales:

Acorde a lo especificado en el análisis de riesgo, se comienzan ahora a determinar las vulnerabilidades reales del sistema.

3.1.1. Puntos de acceso:

Todo usuario de la organización para poder acceder a la misma deberá hacerlo a través de uno de una interfaz que conecte físicamente su estación de trabajo a la red. Se debe diferenciar aquí los accesos vía LAN, los cuales se realizarán en general a través de vínculos propios y "bajo cierto control físico" (Si se respeta la seguridad a nivel físico) por parte de la Organización; y por otro lado los accesos remotos a esta red que es desde donde puede ingresar en general un usuario ajeno a la Empresa.

Los puntos de acceso de la LAN deben quedar claramente especificados en los planos de red, incluidos en la documentación de red, dentro de esta carpeta se establecerán las medidas de seguridad a los ductos, gabinetes de comunicaciones, locales de ubicación de hardware de comunicaciones, etc.

Los puntos de acceso WAN, pueden ser dial-up, punto a punto, multipunto, o a través de acceso a una red pública de datos. En este ítem se deberá detallar al máximo la totalidad

de los accesos, sin dejar de considerar todos los equipos que poseen módem y lo emplean para salir a la red de telefonía pública, pues es aquí donde generalmente se abren puertas no tenidas en cuenta.

3.1.2. Configuración de sistemas:

Se deberá detallar aquí las distintas medidas adoptadas para la configuración de los sistemas, teniendo especialmente en cuenta aquellos detalles referidos a la transmisión de información y al acceso a recursos. Este punto es tenido en cuenta pues por defecto existe mucho software que viene por defecto con detalles de configuración que facilitan ciertas actividades para beneficio de los instaladores del mismo, como así también medidas que deben ser adoptadas para facilitar accesos o ruteos a determinados usuarios pero que pueden ser causa de vulnerabilidades. A continuación se detalla una lista de referencia:

- Tipos de servicios.
- Rutas en host.
- activación de tareas dinámicas (DHCP, WINS, RIP, OSPF, etc).
- Cuentas invitado o Anonymous .
- Puertos abiertos.
- Protocolos de comunicaciones.
- Directorios con permisos de control total.
- Cuentas o contraseñas que no respetan los procedimientos normales.
- Relaciones de confianza.
- Fronteras.
- Puertas traseras.

3.1.3. Bugs de software:

Todo Software posee bugs, los cuáles provocan inconvenientes en los sistemas, muchos de estos son aprovechados para vulnerar medidas de seguridad. Al ser detectados por los fabricantes, van generando los parches necesarios a los mismos. La segunda causa de los ataques de seguridad (después de los usuarios internos) es provocada por estas falencias. Por lo tanto en este punto se debe especificar todas las actualizaciones de Software que fueron introducidas en el sistema, con el mayor grado de detalle posible. También se plantean los problemas descubiertos y aún no solucionados.

Aparece aquí una gran reflexión: MANTENERSE PERMANENTEMENTE ACTUALIZADO, es una de las herramientas más importantes que posee un Administrador de sistemas. Con sólo leer los diarios, aparecen cotidianamente evidencias de ataques producidos por bugs en sistemas que ya fueron resueltos pero que aún no fueron actualizados en esa Empresa, y como corresponde fue aprovechado por un intruso que seguramente sí está actualizado.

3.2. Medidas de protección:

3.2.1. Protección de recursos:

- Control sobre recursos: Se deben .definir qué tipos de recursos deben ser auditados y sobre estos qué detalles auditar. La regla básica es que si se desea auditar TODO, luego NADA se mira. Por lo tanto es sin duda más eficiente definir sólo lo fundamental (poco), y sobre esto sí incrementar el control.
- Estrategias múltiples de protección: Suele ser más seguro emplear varias medidas simples que pocas sofisticadas. Las combinaciones de medidas cruzadas son de común empleo en seguridad, se ponen en evidencia en las estrategias de resguardo de información o en el acceso a recursos con monitoreo y auditoría en simultáneo.

3.2.2. Seguridad física:

Si el acceso a las estaciones de trabajo, servidores, periféricos, dispositivos y canales de comunicaciones no es seguro, a partir de allí no se puede sustentar un plan de seguridad. Por lo tanto se debe aquí establecer la totalidad de las normas de seguridad en los accesos a cada uno de estos elementos.

3.2.3. Reconocimiento de actividad no autorizada:

Para esta actividad se pueden emplear distintas herramientas, muchas de estas ya vienen incorporadas con el software de los sistemas, y otras son adicionales. En este punto se deberá establecer el conjunto de ellas y regular su empleo.

3.2.3.1. Monitoreo de los sistemas en uso:

Esta es la actividad de control sobre los distintos recursos, se deberá realizar en forma agendada y aleatoria, analizándola y luego guardando los registros.

La clave aquí son los registros que se hayan decidido establecer, **su revisión constante es la primera barrera de seguridad**, pues con ellos se determinará usuarios en horarios no frecuentes, reiteración de accesos negados, modificación de archivos y permisos, actividad no concordante, consulta o apertura de puertos de uso no común, archivos nuevos no conocidos, etc.

3.2.3.2. Analizadores de protocolos:

Estas herramientas permiten analizar el tráfico de un red, y por lo tanto desarmar todo su contenido. A través de estos se puede determinar direcciones fuente y destino tanto de

hardware como de software, exceso de tráfico en la red, protocolos que se están empleando, tipo de información que circula, establecimiento y cierre de sesiones.

A través de este punto se dejará registrado la mecánica de trabajo de estas herramientas y los archivos de lo examinado, con las conclusiones obtenidas.

3.2.4. Comunicación del plan de seguridad:

Se debe definir una metodología de información permanente del plan de seguridad y sus actualizaciones y verificar su correcta interpretación en todos los niveles de la Organización.

3.2.4.1. Educación de usuarios:

Deben tener claro que es lo correcto y lo incorrecto en todos sus procederes, y a su vez cómo deben proteger sus propios recursos. Una actividad importante es el monitoreo de sus recursos, cuenta y contraseñas, pues un ataque común es tomar posesión de los recursos de un determinado usuario de la red, y hacer uso de sus privilegios. La persona más indicada para detectarlo es el mismo usuario, por notar cambios en sus propios archivos, performance del equipo, capacidad de disco, actividad en horarios diferentes, etc. Ante estas eventualidades, debe poder reconocerlas y tener perfectamente claro dónde informarlas.

3.2.4.2. Educación de administradores:

Dentro de una red no podrá existir en la práctica un sólo administrador, sino que esta actividad deberá ser implementada por distintas personas que desempeñarán tareas diferentes. Si bien poseerán muchos privilegios similares, no todos deben ostentarán los mismos permisos ni tendrán las mismas atribuciones. En base a los distintos grupos de administración que se definan, es aquí donde se debe instruir respecto al correcto uso de sus cuentas.

3.2.5. Procedimientos de resguardo y recuperación:

Nunca es suficiente el énfasis que se puede hacer sobre las medidas a adoptar para l resguardo de la información. Esta si bien puede ser contemplada dentro de otras actividades, es también una actividad de seguridad por excelencia, pues de esta depende la capacidad de restaurar cualquier información dañada o perdida.

En este apartada es donde se debe volcar todas las actividades que se llevan a cabo para el resguardo de la información y los registros de lo realizado, especificando la periodicidad (diario, semanal mensual), el tipo (Normal, copia, diferencial o incremental) y la información resguardada.

Existen muchos métodos para verificar la integridad de los backup, los cales deben realizarse pues guardar información corrupta, de nada sirve.

3.3. Recursos para prevención de ataques:

3.3.1. Conexiones de red, modems, routers, proxys y Firewalls:

Se deben detallar aquí todas las implementaciones de barreras físicas colocadas y sus reglas de control. se analizará cada dispositivo en cada una de sus interfaces, confeccionando un cuadro con lo que está permitido y denegado en cada una de ellas. El mismo deberá coincidir con lo configurado en estos dispositivos, y es una de las metodologías de control cruzado, la comparación de este documento con la realidad.

3.3.2. Confidencialidad:

La confidencialidad es la acción de restringir el acceso a la información a ciertas categorías de usuarios. Se presentan tres puntos en los cuales la información puede perder esta cualidad:

- Cuando la información está almacenada sobre un host.
- Cuando la información está en tránsito.
- Cuando la información se encuentra almacenada en dispositivos de backup.

Por lo tanto es necesario centrar la atención en este tipo de información acorde a la clasificación que se la haya impuesto, y especificar aquí todos los detalles.

3.3.2.1. Criptografía:

Esta actividad consta en convertir información interpretable, a un formato bajo el cual no se la pueda interpretar. Existen distintas formas de realizarla, tanto por software como por hardware, y se debe prestar especial atención, justamente sobre la que se encuentra en tránsito que es dónde en general presenta más flancos.

Se deben especificar aquí las técnicas empleadas y en que momento se las emplea.

Un detalle común en casi todas las recomendaciones de seguridad es NO DEJAR ESCRITO LAS CLAVES. Este último punto es común para contraseñas de usuarios, recursos o claves públicas y privadas de criptografía.

3.3.2.2. Privacidad en el correo electrónico:

El correo electrónico tiene la característica de transferir información como texto puro. Por lo tanto es común en las distintas organizaciones, separar el correo interno del de Internet. Esta actividad es aconsejable realizarla a través de distintos servidores, los cuales se deben encontrar en zonas de distinta clasificación de seguridad. Si bien la integración o sincronización de los mismos es llevada a cabo, se debe tener muy especialmente en cuenta que el correo interno viajará por vínculos propios mientras que el de Internet dará la vuelta al mundo. Este detalle hace que el tipo de información que se maneje en cada uno de ellos sea diferente.

En ambos casos, acorde al tipo de Organización, se puede implementar privacidad en la transferencia de correo electrónico. Existen varios productos para esta tarea e inclusive también una serie de RFC (1113, 1114 y 1115) que proponen un estándar para privacidad en correo electrónico.

3.3.3. Autenticación:

Aquí se trata de garantizar que "quien dice ser , realmente lo sea". El sistema primario es a través de la creación de la cuenta de usuario con su contraseña correspondiente. En un sistema seguro, en especial al tratar las cuentas de acceso es conveniente ampliar esta medida a través de algún mecanismo adicional de autenticación. Existen de varios tipos, a continuación se detallan algunas posibilidades:

- Kerberos: Fue desarrollado por el MIT y emplea una combinación de criptografía y comparación en una base de datos distribuida, incrementando las medidas de autenticación/
- Tarjetas Inteligentes: Estos dispositivos poseen una clave que va cambiando permanentemente acorde a una secuencia pseudoaleatoria que se encuentra sincronizada con el servidor de acceso, y al coincidir las mismas, autentica al usuario.

Si se emplea algún método adicional, se debe aclarar aquí, acorde a la metodología que se haya definido.

3.3.4. Integridad de la Información:

La Integridad de la Información se refiere al estado completo, correcto y sin cambios desde la última vez que haya sido verificada. Esta actividad se lleva a cabo mediante el control de accesos sobre la misma. La masa de los sistemas permiten llevar registros sobre el acceso a la información y realizar las comparaciones pertinentes.

Esta es la actividad que se debe detallar aquí, el análisis de estos registros y las conclusiones obtenidas.

3.3.5. Fuentes de información:

Como mantenerse actualizado es la medida más importante a tener en cuenta, en este apartado se mencionarán las distintas opciones que se pueden consultar y las relaciones que hayan sido establecidas con el grado de participación logrado, detallando toda actividad desarrollada. Las opciones que se presentan a continuación son algunas de estas:

- Listas de correo: Permiten suscribirse y participar de noticias o debates sobre temas en particular.
- Equipos de repuesta: Son equipos que asesoran y recaban información sobre distintos incidentes referidos a seguridad.

- Vendedores: El soporte técnico sobre los productos adquiridos es parte de la actividad comercial de los productores de software y hardware, por lo tanto se debe tener bien claro dónde recurrir en caso de incidentes en los cuales la causa es identificada con un producto.

4. Procedimientos normales:

En este apartado se tratará de definir las distintas actividades en forma normalizada:

4.1. Actividades agendadas:

En este punto se debe realizar un calendario de actividades, detallando las tareas a realizar diariamente, semanalmente y mensualmente. Cuál es el objetivo de las mismas y contra qué confrontarlas para obtener conclusiones.

4.2. Test de procedimientos:

Se trata aquí de verificar el correcto funcionamiento del plan de seguridad, esta es uno de los puntos más dinámicos pues cotidianamente aparecerán nuevos empleos, desde la restauración de los backup, la creación de cuentas, verificar accesos, consultar usuarios, o realizar auditorías completas. Lo importante de este paso es anotar todo lo nuevo que se implemente, pues seguramente será reusado con posterioridad. Si se detectaran fallas, esto generará modificaciones al plan que realimentarán todo el proceso. Al lanzar algún tipo de test es importante poder definirlo unívocamente, para evitar confusiones acerca de la actividad que se está realizando, pues puede ser aprovechada o solapada con alguna intrusión real.

4.3. Procedimientos para la administración de cuentas:

La creación de las cuentas de usuarios es una tarea que cuánto más estandarizada esté, más eficiente será la organización de este servicio y más clara será la identificación de cualquier anomalía. Sobre esta actividad es importante considerar los siguientes aspectos:

- Quiénes están autorizados a crear o modificar cuentas?
- Quiénes pueden tener cuentas en el sistema?
- Cuánto tiempo durará la asignación de una cuenta, y cómo se renegocia?
- Cómo serán removidas y cuándo caducan las cuentas obsoletas?
- Las cuentas se crean centralizadamente o se puede distribuir su administración?
- Quiénes pueden crear o modificar grupos?
- Quiénes pueden formar parte de los distintos grupos?

- Quiénes pueden ser usuarios remotos?
- Quiénes incrementan el nivel de validación? (En caso de existir)
- Se restringirá el acceso por equipo, usuario, horarios ,etc ?
- Se permite a más de un usuario usar el mismo equipo?
- Cuál es la lógica de nombres de cuentas?

4.4. Procedimientos para la administración de contraseñas:

De manera similar a la administración de cuentas, el tema de las contraseñas se debe tomar con cuidado, pues tratar de romperlas o crackearlas es una de las primeras actividades que desea realizar un intruso. Un buen test es ejecutar programas de Crack y luego informarle al usuario cuánto tiempo tardó en descubrir su contraseña, para que este sea consciente de la importancia que revista. Sobre esta actividad es importante considerar los siguientes aspectos:

- Los usuarios pueden dar su contraseña a otros usuarios?
- Cómo se implementa la contraseña inicial?
- Tendrán fecha de caducidad?
- Qué cantidad mínima de dígitos se permitirá?
- Se guardará historia de cambios?, cuántas?
- Los usuarios pueden cambiar sus contraseñas?

4.4.1. Selección:

Guía de detalles a tener en cuenta: para la selección de una contraseña:

- NUNCA emplear las contraseñas por defecto.
- NUNCA dejar por escrito listas de contraseñas.
- NO USAR nombres de usuarios como contraseñas (ni en inverso, mayúsculas, duplicados, etc).
- NO USAR nombres, apellidos, etc.
- NO USAR nombres de esposa/o, hijos, parientes cercanos.
- NO USAR información de fácil obtención, como ser : Nro documento, fechas, teléfono, patente de automóvil, etc.
- NO USAR Contraseñas de todas letras o todos números, mucho menos repetición de los dígitos.
- NO USAR palabras contenidas en diccionarios.
- NO USAR contraseñas menores a 6 dígitos.
- USAR mezclas de números y letras.
- USAR caracteres de puntuación, matemáticos, lógicos , etc.

- USAR contraseñas fáciles de recordar.
- USAR contraseñas que se puedan escribir rápidamente sin mirar el teclado.

4.4.2. Cambios:

Un detalle a aclarar aquí es la metodología de verificación del usuario que solicita un cambio de contraseña, pues es inclusive un reporte de varios CERT el hecho de solicitar esta actividad para obtener acceso por parte de intrusos. Por lo tanto para esta actividad se deberán extremar las medidas de control.

5. Procedimientos ante incidentes:

En general este es un apartado al cual se le dedica muy poca atención y el resultado es que cuando se produce un incidente, las decisiones son tomadas sobre la marcha, provocando muchas veces daños por falta de previsión. Es por esta razón que se tiene en cuenta esta actividad, y se plantea el desarrollo del plan contra incidentes, el cual eliminará muchas ambigüedades.

Este plan será el resultado de todas las tareas realizadas anteriormente, es por esta razón que no se puede definir con anterioridad, ni puede apartarse de todas las regulaciones que ya fueron establecidas dentro de la Política y el Plan de seguridad.

Como referencia se detallan a continuación los aspectos que se deben considerar en el plan:

- Asegurar l a integridad de los sistemas críticos.
- Mantener y restaurar datos.
- Mantener y restaurar servicios.
- Determinar cómo sucedió.
- Detener escalamiento o futuros incidentes.
- Detener la publicidad negativa.
- Determinar quién lo hizo.
- Penalizar a los atacantes.

5.1. plan contra incidentes:

La primer medida del plan consiste en la determinación de prioridades, las cuales se detallan a continuación como referencia:

- Prioridad 1: Proteger vidas o seguridad de personas.
- Prioridad 2: Proteger datos clasificados.
- Prioridad 3: Proteger otros datos.
- Prioridad 4: Prevenir daños a los sistemas.
- Prioridad 5: Minimizar anomalías en los sistemas.

5.2. Determinación del problema (Evaluación):

Es esto real ?

Este es el primer interrogante, pues a menudo se puede confundir una intrusión con virus, falla de un sistema o un test que se está ejecutando. Existen varios indicadores que se pueden tener en cuenta, como por ejemplo:

- Ruptura de sistemas.
- Nuevas cuentas de usuarios, o actividad en cuentas que hace tiempo no se empleaban.
- Nuevos archivos, en general con extraños nombres.
- Discrepancia en cuentas respecto a lo establecido en el plan.
- Cambios en la longitud de los archivos o datos (en clientes, se pone de manifiesto en general por el crecimiento de archivos ".exe" desconocidos).
- Intentos de escritura en sistemas.
- Modificación o borrado de datos.
- Negación de servicios.
- Bajo rendimiento de sistemas, host o red.
- Numerosos intentos de validación.
- Numerosos intentos de inicio de sesión en puertos no habilitados.
- Nombres ajenos al sistema.
- Direcciones IP o MAC ajenas al sistema.
- Modificación de rutas en dispositivos de comunicaciones.
- Alarmas.

5.3. Alcance:

Se detallan aquí un conjunto de criterios que permiten delimitar el problema:

- El incidente está acotado a este sitio o es multi-sitio?
- Cuántos host están afectados?
- Existe información sensible involucrada?
- Cuál es el punto de entrada del incidente?
- Tomó participación la prensa?
- Cuál es el daño potencial del incidente?
- Cuál es el tiempo estimado para solucionar el incidente?
- Qué recursos serán requeridos para controlar el incidente?

5.4. Notificaciones:

Al saber fehacientemente que un incidente se ha provocado, se debe comenzar a notificar a aquellos que deban tomar participación en el hacho. Para mantener el hecho bajo control es importante saber a quiénes es necesario hacerlo. A continuación se tratarán ciertos aspectos que se deben tener en cuenta.

5.4.1. Información explícita:

Toda notificación que se curse dentro o fuera del sitio deberá ser explícita, esto quiere decir que la misma deberá ser clara, concisa y completa. El tratar de enmascarar el hecho o decir parte de la verdad, sólo sirve para crear más confusión.

5.4.2. Información verídica:

Si el hecho ya está difundido, el tratar de brindar explicaciones que no son estrictamente ciertas, sólo empeorará paso a paso el problema.

5.4.3. Elección del lenguaje:

La elección del lenguaje puede tener un efecto muy importante en las notificaciones. Si se usa un lenguaje emocional o inflamatorio, crecerán las expectativas sobre el incidente. Otro detalle del lenguaje son las expresiones no técnicas que se empleen para dirigirse a la masa del personal, pues es más difícil explicar hechos en este lenguaje pero es dónde realmente se están esperando las notificaciones.

5.4.4. Notificaciones a individuos:

Este último aspecto debe quedar definido para dejar claramente sentado a quien se debe notificar y por qué medios. Se estila contar aquí con una cadena de comunicaciones.

- Personal técnico.
- Administradores.
- Relaciones públicas.
- Personal directivo.
- Equipos de respuesta (CERT).
- Personal legal.
- Vendedores.
- Service Provider.

5.4.5. Aspectos generales a tener en cuenta par las notificaciones:

- Mantener un nivel técnico bajo. Si un alto grado de detalle es difundido, puede facilitar las actividades de intrusión.
- No difundir especulaciones.
- Trabaje con personal legal, para determinar qué evidencias deberán o no ser difundidas.
- Trate de no ser forzado a divulgar información antes de estar listo a brindarla..
- No permita que las presiones por brindar información desvíen el control del incidente.

5.5. Respuestas:

Este es el punto central del tratamiento de incidentes, la respuesta caerá en alguna o varias de los procedimientos que se detallan a continuación:

5.5.1. Contención:

Se trata de limitar la extensión del ataque. Varias medidas pueden quedar aquí establecidas, como apagar ciertos servidores, desactivar servicios, desconectar segmentos de red, activar rutas de contención, etc.

5.5.2. Erradicación:

Una vez contenido el incidente, es momento de erradicar las causas que lo provocaron. detectar programas troyanos, virus, limpiar backup, etc.

5.5.3. Recuperación:

La recuperación consta de retornar el sistema a su estado normal. Para esta actividad se deberá instalar los parches correspondientes, recuperar la información dañados, restituir los servicios negados, etc.

5.5.4. Seguimiento:

Este que es uno de los procedimientos más importantes, es también el más dejado de lado. Este el punto de partida para luego desarrollar las "Lecciones Aprendidas". Se lo suele llamar el "Análisis Post mortem", se deben analizar los siguientes aspectos:

- Exactamente qué sucedió.
- En que horario y fecha?
- Cómo respondió el personal involucrado al incidente?
- Qué clase de información se necesitó rápidamente?

- Cómo se obtuvo esa información?
- Qué se debería hacer diferente la próxima vez?
- Cómo fue la cronología de eventos?
- Que impacto monetario se estima que causó (Software, archivos, recursos, hardware, horas de personal, soporte técnico, etc)?

5.6. Registros:

Al determinar un incidente, es imprescindible detallar todos los eventos posibles, por lo tanto se deben registrar con el mayor grado de precisión todos los pasos y acciones tomadas por personal propio y por intrusos. Como mínimo se debe registrar:

- Todos los eventos.
- Todas las acciones tomadas y detectadas.
- Todas las conversaciones telefónicas y notificaciones.

La mejor manera de realizarlo es llevar un libro de registros.

6. Procedimientos post incidentes

6.1. introducción:

Luego de superado el incidente, es aconsejable realizar también una serie de actividades para permitir justamente la realimentación del plan de seguridad:

- Determinación final de los cómo fueron afectados los recursos.
- Las lecciones aprendidas deberán replantear el plan de seguridad.
- Un nuevo análisis de riesgo debería ser realizado.
- Si dentro del plan está contemplado, se deberá lanzar una investigación y tomar las medidas legales pertinentes.

6.2. Remover vulnerabilidades y depuración de sistemas:

Esta es una tarea muchas veces dificultosa, desde ya que es necesario haber podido determinar cuál fue la brecha, y es frecuente tener que remover todos los accesos o funcionalidades para restituirlas a su estado original. Si no se poseía líneas de base en la configuración de los sistemas, se incrementará el nivel de dificultad. Debería existir un plan de limpieza de los sistemas.

6.3. Lecciones aprendidas:

Basado en el seguimiento y registros realizados, es prudente escribir un reporte que describa el incidente, métodos de descubrimiento, procedimientos de recuperación, procedimientos de monitoreo, y por último el sumario de las lecciones aprendidas.

6.4 Actualización de políticas y planes:

Se dejará aquí asentado, los cambios que provocó este incidente en la Política y Plan de seguridad. Es de especial interés tener en cuenta que si el incidente se produjo por una pobre Política o Plan, a menos que estos sean modificados, seguramente se repetirá.