Procedimiento de manejo de incidentes

1.0 INTRODUCCIÓN

Este documento proporciona algunas pautas y procedimientos generales para tratar incidentes de seguridad informática. El documento está destinado a proporcionar al personal de soporte de UTREEE algunas pautas sobre qué hacer si descubren un incidente de seguridad. El término incidente en este documento se define como cualquier evento irregular o adverso que ocurra en cualquier parte de la NPSN. Algunos ejemplos de posibles categorías de incidentes incluyen: compromiso de la integridad del sistema; denegación de recursos del sistema; acceso ilegal a un sistema (ya sea una penetración o una intrusión); uso malicioso de los recursos del sistema, o cualquier tipo de daño a un sistema. Algunos escenarios posibles para incidentes de seguridad son:

* Ves un proceso extraño ejecutándose y acumulando mucho tiempo de CPU.

* Ha descubierto un intruso que ha iniciado sesión en su sistema.

* Ha descubierto que un virus ha infectado su sistema.

* Ha determinado que alguien de un sitio remoto está tratando de penetrar en el sistema.

Los pasos involucrados en el manejo de un incidente de seguridad se clasifican en cinco etapas: protección del sistema, identificación del problema, contención del problema, erradicación del problema, recuperación del incidente y análisis de seguimiento. Las acciones tomadas en algunas de estas etapas son comunes a todos los tipos de incidentes de seguridad y se analizan en la sección 2. La sección 3 analiza los procedimientos específicos para tratar los incidentes de gusanos/virus y los incidentes de hackers/crackers.

1.1 TÉRMINOS

Algunos términos utilizados en este documento son:

ISO - Oficial de seguridad de la instalación

CSO - Oficial de Seguridad Informática

CSA - Analista de Seguridad Informática

LSA - Analista Principal de Sistemas

CERT - Equipo de Respuesta a Emergencias Informáticas

CIAC - Capacidad de asesoramiento sobre incidentes informáticos

1.2 ÁREAS DE RESPONSABILIDAD

En muchos casos, las acciones descritas en esta guía no serán realizadas por una sola persona en un solo sistema. Muchas personas pueden estar involucradas durante el curso de un incidente de seguridad activo que afecta a varios de los sistemas UTREEE al mismo tiempo (es decir, un ataque de gusano). El CSA de UTREEE siempre debe participar en la investigación de cualquier incidente de seguridad.

El ISO de UTREEE Eminel Alcon, el CSO de UTREEE Antonio Reyes y el CSA de UTREEE Harry Ferreras actuarán como el equipo de coordinación de incidentes para todos los incidentes relacionados con la seguridad. En incidentes menores, solo estará involucrada la CSA. Sin embargo, en incidentes más graves, los tres pueden estar involucrados en el esfuerzo de coordinación. El equipo de coordinación de incidentes será responsable de asignar personas para trabajar en tareas específicas del proceso de manejo de incidentes y coordinará el proceso general de respuesta a incidentes. Todas las personas involucradas en

la respuesta y limpieza de incidentes son responsables de proporcionar cualquier información necesaria a los miembros del equipo de coordinación de incidentes.

Cualquier directiva dada por un miembro del equipo de coordinación de incidentes reemplazará este documento.

1.3 CONSIDERACIONES IMPORTANTES

Un incidente de seguridad informática puede ocurrir en cualquier momento del día o de la noche. Aunque la mayoría de los incidentes de piratas informáticos / piratas informáticos ocurren durante las horas libres cuando los piratas informáticos no esperan que los administradores de sistemas estén vigilando a sus rebaños. Sin embargo, los incidentes de gusanos y virus pueden ocurrir en cualquier momento del día. Por lo tanto, las consideraciones de tiempo y distancia al responder al incidente son muy importantes. Si la primera persona de la lista de llamadas a la que se debe notificar no puede responder en un plazo razonable, se debe llamar a la segunda persona además de a la primera. Será responsabilidad de las personas en la lista de llamadas determinar si pueden responder dentro de un plazo aceptable.

Los medios de comunicación también son una consideración importante. Si alguien de los medios de comunicación obtiene conocimiento sobre un incidente de seguridad, intentará recopilar más información de un sitio que actualmente responde al incidente. Proporcionar información a las personas equivocadas podría tener efectos secundarios indeseables. La sección 2.3 analiza la política sobre divulgación de información.

2.0 PROCEDIMIENTOS GENERALES

En esta sección se describen los procedimientos que son comunes para todos los tipos de incidentes de seguridad.

2.1 MANTENGA UN LIBRO DE REGISTRO

El registro de información es fundamental en situaciones que eventualmente pueden involucrar a las autoridades federales y la posibilidad de un juicio penal. Las implicaciones de cada incidente de seguridad no siempre se conocen al comienzo o incluso durante el curso de un incidente. Por lo tanto, se debe mantener un registro escrito de todos los incidentes de seguridad que se están investigando. La información debe registrarse en una ubicación que no pueda ser alterada por otros. Los registros escritos manualmente son preferibles ya que los registros en línea se pueden modificar o eliminar. Los tipos de información que deben registrarse son:

* Fechas y horas de las llamadas telefónicas relacionadas con incidentes.
* Fechas y horas en que se descubrieron u ocurrieron eventos relacionados con incidentes.
* Cantidad de tiempo dedicado a trabajar en tareas relacionadas con incidentes.
* Personas con las que ha contactado o se ha puesto en contacto con usted.
* Nombres de sistemas, programas o redes que se han visto afectados.

2.2 INFORMAR A LAS PERSONAS ADECUADAS

Informar a las personas adecuadas es de suma importancia. Hay algunas acciones que solo pueden ser autorizadas por la ISO o CSO de UTREEE. UTREEE también tiene la responsabilidad de informar a otros sitios sobre un incidente que pueda afectarlos. A continuación se proporciona una lista de contactos. La sección 3 analiza a quién se debe llamar y cuándo para cada tipo de incidente de seguridad.

Los números de teléfono de las personas a continuación se pueden obtener en el Manual de operaciones de UTREEE en la sala de control de UTREEE. Además, los analistas de la sala de control pueden ser de ayuda cuando se trata de contactar a las personas adecuadas.

Lista de contactos

UTREEE ISO – Eminel Alcon

Suplente – Rebeca Jiménez

UTREEE CSO – Antonio Reyes

Suplente – Lady Jiménez

UTREEE CSA - Harry Ferreras

Suplente – Teodosio Rodríguez

Oficina de Seguridad/Deber de Ames – TBD

2.3 DIVULGACIÓN DE INFORMACIÓN

El control de la información durante el transcurso de un incidente de seguridad o la investigación de un posible incidente es muy importante. Proporcionar información incorrecta a las personas equivocadas puede tener efectos secundarios indeseables, especialmente si los medios de comunicación están involucrados. Toda divulgación de información debe ser autorizada por la ISO de UTREEE o por otras personas designadas por la ISO de UTREEE. Todas las solicitudes de comunicados de prensa deben enviarse a nivel de rama o división. Además, la información específica del incidente, como las cuentas involucradas, los programas o los nombres de los sistemas, no debe proporcionarse a ninguna persona que llame y afirme ser un oficial de seguridad de otro sitio. Todas las solicitudes sospechosas de información (es decir, solicitudes realizadas por personas que llaman que afirman ser CSA para otro sitio) deben enviarse al CSO o al nivel de sucursal de UTREEE. Si tiene alguna duda sobre si puede divulgar una información específica, comuníquese con UTREEE CSO o UTREEE ISO.

2.4 ANÁLISIS DE SEGUIMIENTO

Una vez que un incidente se ha manejado por completo y todos los sistemas se restauran a un modo normal de operación, se debe realizar un análisis postmortem de seguimiento. La etapa de seguimiento es una de las etapas más importantes para manejar un incidente de seguridad. Todas las partes involucradas (o un representante de cada grupo) deben reunirse y discutir las acciones que se tomaron y las lecciones aprendidas. Todos los procedimientos existentes deben evaluarse y modificarse, si es necesario. Todas las copias en línea de archivos infectados, código de gusano, etc., deben eliminarse del sistema. Si corresponde, se debe presentar un conjunto de recomendaciones a los niveles de gestión apropiados. Un informe de incidente de seguridad debe ser escrito por una persona designada por la ISO de UTREEE y distribuido a todo el personal apropiado.

3.0 PROCEDIMIENTOS ESPECÍFICOS DEL INCIDENTE

En esta sección se describe el procedimiento para controlar los incidentes de virus, gusanos y hackers/crackers.

3.1 INCIDENTES DE VIRUS Y GUSANOS

Aunque los incidentes de virus y gusanos son muy diferentes, los procedimientos para manejar cada uno son muy similares, aparte del aislamiento inicial del sistema y la criticidad del tiempo. Los virus no se autorreplican y, por lo tanto, los incidentes de esta naturaleza no son tan críticos como los incidentes de gusanos o piratas informáticos. Los gusanos se autorreplican y pueden propagarse a cientos de máquinas en cuestión de minutos, por lo tanto, el tiempo es un factor crítico cuando se trata de un ataque de gusano. Si no está seguro del tipo de ataque, proceda como si el ataque estuviera relacionado con gusanos.

3.1.1 Aislar el sistema

Aísle los sistemas infectados de la red UTREEE restante lo antes posible. Si se sospecha de un gusano, se debe tomar la decisión de desconectar el UTREEE del mundo exterior. El aislamiento de red es un método para detener la propagación de un gusano, pero el aislamiento también puede dificultar el esfuerzo de limpieza, ya que UTREEE se desconectará de los sitios que pueden tener parches. La ISO de UTREEE debe autorizar el aislamiento de la red UTREEE del mundo exterior.

Registre todas las acciones.

No apague ni reinicie los sistemas que puedan estar infectados. Hay algunos virus que destruirán los datos del disco si el sistema se apaga y se reinicia. Además, reiniciar un sistema podría destruir la información o evidencia necesaria.

3.1.2 Notificar a las personas apropiadas

Notifique a UTREEE CSA lo antes posible. Si no puede comunicarse con él / ella dentro de los 10 minutos, comuníquese con la persona de respaldo. El CSA de UTREEE será responsable de notificar a otro personal apropiado. **NOTA -** A continuación, se indican diferentes tiempos para sospecha de ataque de gusanos y para sospecha de ataque de virus.

- El CSA de UTREEE notificará al CSO de UTREEE lo antes posible. Si no puede comunicarse con él dentro de una hora (10 minutos para un ataque de gusano), se contactará a su persona de respaldo.

- El CSA o CSO de UTREEE notificará a la ISO de UTREEE dentro de las dos horas (una hora para un ataque de gusano). La ISO de UTREEE escalará a un nivel superior de gestión si es necesario.

- La sala de control o UTREEE CSA debe notificar a todos los LSA involucrados dentro de las cuatro horas (dos horas para un ataque de gusano).

3.1.3 Identificar el problema

Intente identificar y aislar los archivos y procesos relacionados con virus o gusanos sospechosos. Antes de eliminar cualquier archivo o eliminar cualquier proceso, se debe tomar y guardar una instantánea del sistema. A continuación se muestra una lista de tareas para hacer una instantánea del sistema:

1) Guarde una copia de todos los archivos de registro del sistema. Los archivos de registro generalmente se encuentran en /usr/adm.

2) Guarde una copia del archivo de historial raíz, */.history*.

3) Guarde copias de los *archivos /etc/utmp* y */etc/wtmp*. A veces, estos archivos se encuentran en el directorio */usr/adm*.

4). Capture toda la información del estado del proceso en un archivo usando el comando ps -awwxl > nombre de archivo para sistemas BSD y ps -efl > nombre de archivo para sistemas SYSV.

Si se pueden identificar archivos específicos que contienen código de virus o gusano, mueva esos archivos a un lugar seguro o archívelos en cinta y luego elimine los archivos infectados. Además, obtenga una lista de todas las conexiones de red activas. Un analista de la sala de control puede brindar asistencia para obtener información instantánea sobre el sistema.

Ejecute el comprobador de seguridad de la policía en los sistemas infectados para identificar otros posibles problemas, como archivos del sistema alterados, nuevos programas suid o archivos especiales ocultos. Puede ser necesario instalar una versión limpia de policías de cinta.

Si otros sitios han estado involucrados en este punto, pueden tener información útil sobre el problema y posibles soluciones a corto plazo. Además, cualquier información útil obtenida sobre el virus o gusano debe transmitirse a los sitios de Internet CERT, después de la aprobación de UTREEE ISO. Registre todas las acciones.

3.1.4 Contener el virus o gusano

Todos los procesos sospechosos ahora deben detenerse y eliminarse del sistema. Haga un volcado completo del sistema y guárdelo en un lugar seguro. Las cintas deben etiquetarse cuidadosamente para que no sean utilizadas por personas desprevenidas en el futuro. A continuación, elimine todos los archivos o códigos de gusanos sospechosos de estar infectados. En el caso de un ataque de gusano, puede ser necesario mantener el sistema aislado del mundo exterior hasta que todos los sistemas UTREEE hayan sido inoculados y/o los otros sitios de Internet hayan sido limpiados e inoculados. **Registre todas las acciones.**

3.1.5 Inocular el sistema o sistemas

Implemente correcciones y/o parches para inocular los sistemas contra nuevos ataques. Antes de implementar cualquier corrección, puede ser necesario evaluar el nivel de daño al sistema. Si se ha analizado el código del virus o gusano, las tareas de evaluación del daño no son muy difíciles. Sin embargo, si no se ha analizado el código ofensivo, puede ser necesario restaurar el sistema a partir de cintas de copia de seguridad. Una vez que el sistema vuelve a un modo seguro, se deben implementar y probar los parches o correcciones. Si es posible, el virus o gusano debe soltarse en un sistema aislado que haya sido inoculado para garantizar que los sistemas ya no sean vulnerables. **Registre todas las acciones.**

3.1.6 Volver a un modo de funcionamiento normal

Antes de volver a poner los sistemas en modo de funcionamiento completo, debe notificar al mismo grupo de personas que fueron notificadas en la primera etapa. También se debe notificar a los usuarios que los sistemas están volviendo a un estado completamente operativo. Puede ser prudente solicitar a todos los usuarios que cambien sus contraseñas. Antes de restaurar la conectividad con el mundo exterior, verifique que todas las partes afectadas hayan erradicado con éxito el problema e inoculado sus sistemas. **Registre todas las acciones.**

3.1.7 Análisis de seguimiento

Realice un análisis de seguimiento como se describe en la sección 2.4.

3.2. INCIDENTES DE HACKERS/CRACKERS

Responder a incidentes de piratas informáticos / crackers es algo diferente a responder a un incidente de gusano o virus. Algunos piratas informáticos son muy sofisticados y llegarán a grandes profundidades para evitar la detección. Otros son jóvenes estudiantes ingenuos que buscan emociones. Un hacker también

puede ser alguien en el interior que participa en actividades ilícitas del sistema (es decir, el descifrado de contraseñas). Cualquier incidente de hacker/cracker debe abordarse como una amenaza real para la NPSN.

Los incidentes de piratas informáticos se pueden dividir en tres tipos: intentos de obtener acceso a un sistema, una sesión activa en un sistema o eventos que se han descubierto después del hecho. De los tres, una sesión activa de hacker/cracker es la más grave y debe tratarse lo antes posible.

Hay dos métodos para lidiar con un incidente activo de hacker / cracker. El primer método consiste en bloquear inmediatamente a la persona del sistema y restaurar el sistema a un estado seguro (consulte la sección 3.2.2). El segundo método consiste en permitir que el hacker/cracker continúe su sondeo/ataque e intente recopilar información que conduzca a una identificación y posible condena penal (véase la sección 3.2.3). El método utilizado para manejar un incidente de cracker/hacker estará determinado por el nivel de comprensión de los riesgos involucrados.

3.2.1 Intentos de sondeo en un sistema NPSN

Los incidentes de este tipo incluirían: intentos repetidos de inicio de sesión, comandos repetidos de ftp, telnet o rsh e intentos repetidos de devolución de marca.

3.2.1.1 Identificar el problema

Identifique la fuente de los ataques observando los archivos de registro del sistema y las conexiones de red activas. Haga copias de toda la información de seguimiento de auditoría, como los archivos de registro del sistema, el archivo de historial raíz, los archivos utmp y wtmp, y guárdelos en un lugar seguro. Capture la información del estado del proceso en un archivo y luego almacene el archivo en un lugar seguro. **Registre todas las acciones.**

3.2.1.2 Notificar a UTREEE CSA

Notifique a UTREEE CSA dentro de los 30 minutos. Si no se puede contactar con el CSA de UTREEE, notifique al CSO de UTREEE o a la persona de respaldo de UTREEE CSA. El CSA de UTREEE o su persona de respaldo será responsable de notificar a otros niveles de administración.

3.2.1.3 Identificar a Hacker/Cracker

Si se puede identificar la fuente de los ataques, entonces el CSA de UTREEE (o una persona designada) se comunicará con el administrador del sistema o el analista de seguridad de ese sitio e intentará obtener la identificación del pirata informático / cracker. La NIC puede ser una fuente para obtener el nombre y el número de teléfono del administrador del sitio remoto. Si se puede identificar al hacker/cracker, la información debe proporcionarse a la CSO o ISO de UTREEE. El CSO o ISO de UTREEE proporcionará instrucciones sobre cómo proceder, si es necesario. **Registre todas las acciones.**

3.2.1.4 Notificar al CERT

Si no se puede identificar la fuente de los ataques, UTREEE CSA se comunicará con los equipos de Internet CERT y CIAC y les proporcionará información sobre el ataque. ***NOTA - La divulgación de información debe ser aprobada por UTREEE ISO o alguien que él designe. **Registre todas las acciones.**

3.2.1.5 Seguimiento

Después de la investigación, el CSA o CSO de UTREEE debe escribir un breve informe que describa el incidente y las acciones que se tomaron y distribuirlo a las personas apropiadas. Realice el análisis de seguimiento como se describe en la sección 2.4.

3.2.2 Actividad activa de piratas informáticos / crackers

Los incidentes de este tipo incluirían cualquier sesión activa o comando de una persona no autorizada. Algunos ejemplos incluirían una sesión activa de rlogin o telnet, una sesión ftp activa o un intento de devolución de acceso telefónico exitoso. En el caso de una actividad activa de piratas informáticos / crackers, se debe tomar una decisión sobre si permitir que la actividad continúe mientras recopila pruebas o sacar al pirata informático / cracker del sistema y luego bloquear a la persona. Dado que un pirata informático puede hacer daño y estar fuera del sistema en cuestión de minutos, el tiempo es crítico al responder a los ataques activos de los piratas informáticos. Esta decisión debe ser tomada por la ISO de UTREEE o alguien que él designe (es decir, el CSO de UTREEE). La decisión se basará en la disponibilidad de personal calificado para monitorear y observar al hacker / cracker y el nivel de riesgo involucrado.

3.2.2.1 Notificar a las personas adecuadas

Notifique a UTREEE CSA lo antes posible. Si no puede comunicarse con él / ella dentro de los 5 minutos, comuníquese con la persona de respaldo. El CSA de UTREEE será responsable de notificar a otro personal apropiado. El CSA de UTREEE, con la posible ayuda del LSA involucrado, será responsable de tratar de evaluar lo que busca el hacker / cracker y los riesgos involucrados en permitir que el hacker / cracker continúe su actividad.

El CSA de UTREEE notificará al CSO de UTREEE lo antes posible. Si no puede comunicarse con él dentro de los diez minutos, se debe contactar a su persona de respaldo. El CSO de UTREEE puede tomar la decisión de permitir que el pirata informático continúe o bloquearlo del sistema. Según la decisión, siga los procedimientos de 2.1 o 2.2 a continuación.

El CSA o CSO de UTREEE notificará a la ISO de UTREEE dentro de los 30 minutos. La ISO de UTREEE escalará a un nivel superior de gestión si es necesario.

3.2.3 Eliminación de Hacker/Cracker del sistema

3.2.3.1 Instantánea del sistema

Haga copias de toda la información de seguimiento de auditoría, como los archivos de registros del sistema, los archivos de historial raíz, los archivos utmp y wtmp, y guárdelos en un lugar seguro. Capture la información del estado del proceso en un archivo y luego almacene el archivo en un lugar seguro. Cualquier archivo sospechoso debe moverse a un lugar seguro o archivarse en cinta y luego eliminarse del sistema. Además, obtenga una lista de todas las conexiones de red activas. Un analista de la sala de control puede brindar asistencia para obtener información instantánea sobre el sistema. **Registre todas las acciones.**

3.2.3.2 Bloquear al hacker

Elimine todos los procesos activos del pirata informático / cracker y elimine cualquier archivo o programa que pueda haber dejado en el sistema. Cambie las contraseñas de cualquier cuenta a la que haya accedido el hacker/cracker. En esta etapa, el hacker/cracker debe ser bloqueado del sistema. **Registre todas las acciones.**

3.2.3.3 Restaurar el sistema

Restaure el sistema a un estado normal. Restaure cualquier dato o archivo que el pirata informático / cracker pueda haber modificado. Instale parches o correcciones para cerrar cualquier vulnerabilidad de seguridad que el hacker / cracker pueda haber explotado. Informar a las personas adecuadas. Todas las acciones realizadas para restaurar el sistema a un estado normal deben documentarse en el libro de registro de este incidente. **Registre todas las acciones.**

3.2.3.4 Notificar a otras agencias

Informe el incidente al CNSRT de Ames, al CERT de Internet y al CIAC. ***NOTA: la divulgación de información debe ser aprobada por la ISO de UTREEE o alguien que él designe. **Registre todas las acciones**.

3.2.3.5 Seguimiento

Después de la investigación, el CSA o CSO de UTREEE debe escribir un breve informe que describa el incidente y las acciones que se tomaron y distribuirlo a las personas apropiadas. Realice el análisis de seguimiento como se describe en la sección 2.4.

3.2.4 Monitoreo de la actividad de piratas informáticos / crackers

No existen procedimientos establecidos para monitorear la actividad de un pirata informático. Cada incidente se tratará caso por caso. La ISO de UTREEE o la persona que autoriza la actividad de monitoreo debe proporcionar orientación a quienes realizan el monitoreo. Una vez que se ha tomado la decisión de dejar de monitorear las actividades del pirata informático y eliminarlo del sistema, se deben seguir los pasos descritos en la sección 3.2.3 anterior.

3.2.5 Evidencia de incidentes pasados

En el caso de que se descubra un incidente después del hecho, no siempre hay mucha evidencia disponible para identificar quién era la persona o cómo obtuvo acceso al sistema. Si descubre que alguien ha irrumpido con éxito en un sistema UTREEE, notifique a UTREEE CSA dentro de un día hábil. El CSA de UTREEE será responsable de notificar a las personas apropiadas e investigar el incidente.