Prevención proactiva: proceso de auditoría para evitar situaciones de riesgo

Abstract: los procesos de evaluación permanente y análisis de la seguridad, así como el asesoramiento y aseguramiento del sistema para limitar la superficie de exposición a la ciberamenaza, constituyen un marco de prevención proactiva al establecer una hoja de ruta de mejora continua para prevenir situaciones de riesgo ante incidentes de seguridad.

Contenido:

1. INTRODUCCIÓN 1
2. ACTUACIONES DE AUDITORÍA PARA PREVENIR SITUACIONES DE RIESGO ACTIVAS POR INCIDENTES ..1
   2.1 Evaluación de la superficie de exposición 3
   2.2 Priorización de corrección de vulnerabilidades atendiendo a la criticidad 6
3. MEDIDAS INICIALES DE SEGURIDAD A APLICAR ANTE UNA PROBLEMÁTICA DE SEGURIDAD 7
   3.1 Medidas a corto plazo 7
   3.2 Medidas complementarias 8
   3.3 Medidas de mejora continua 9

1. INTRODUCCIÓN

La evaluación permanente del estado de la seguridad de los sistemas de las Tecnologías de la Información y la Comunicación (TIC) es una actividad fundamental en cualquier organización pues, a través de evaluaciones globales del estado de la seguridad y mediante análisis de la superficie de exposición, se puede minimizar el impacto de posibles ciberamenazas sobre los activos de una entidad.

Los procesos de auditoría y análisis en el ámbito de la seguridad TIC, así como el asesoramiento general para el aseguramiento del sistema, constituyen un marco de prevención proactiva que permite prevenir situaciones de riesgo activas por incidentes de seguridad.

Dada la importancia de estos procesos, en el presente documento se establecen las actuaciones y medidas a implementar para proteger con un mejor nivel de ciberseguridad el entorno global de infraestructuras de una organización.

2. ACTUACIONES DE AUDITORÍA PARA PREVENIR SITUACIONES DE RIESGO ACTIVAS POR INCIDENTES

Al objeto de establecer un proceso de auditoría, es importante determinar de forma inicial los condicionantes previos a la ejecución de dicho proceso:

- Es esencial establecer una relación causal de la tipología de activos a auditar o el tipo de inspección a llevar a cabo, en relación con el riesgo existente. Esto es importante para:
  - Definir prioridades tanto para las propias auditorías como para los resultados de los análisis que se efectúen.
  - Establecer vinculaciones o identificaciones de problemas de seguridad que puedan ser aprovechados por un atacante.

  Así, si en una primera identificación de la problemática los activos afectados tienen que ver con determinada tecnología, se deberán definir prioridades para centrar los esfuerzos sobre esta tipología de activos.

  De esta forma, si en una primera identificación de la problemática se han podido constatar problemas con el uso de cuentas privilegiadas o movimiento entre servidores que indiquen una operativa de atacante con escalada de privilegios, deben primar las auditorías *privilegiadas*, puesto que sería esta la visión que tendría el atacante.
- Es recomendable tener una primera visión de la superficie de exposición global de la organización:
  - Servicios para accesos remotos o de teletrabajo.
  - Segmentación entre los sistemas/servicios externos y los internos.
  - Segmentación entre los servicios internos entre sí.
  - Segmentación entre la operación de usuario (puestos de trabajo, dispositivos de impresión, escritorios virtuales, etc.).
  - En el caso de las Administraciones Públicas, la relación con otros organismos:
    - Relación a través de la red SARA.
    - Relación directa con otras organizaciones:
      - Conexiones punto a punto.
      - Conexiones de un tercero a través del organismo para consumo de servicios o prestación de la interconexión a la red SARA.
  - Tipología de servicios fundamentales orientados por tipos de tecnologías:
    - Tecnologías Microsoft.
    - Tecnologías UNIX.
    - Tecnologías Linux.
    - Tecnologías IBM Z/OS.
    - Electrónica de red.

- Otras.

- Requisitos propios del negocio o de la misión propia de la organización.
  - ¿Qué servicios son fundamentales?
  - ¿Qué servicios son dependientes de elementos externos y cuáles no? Por ejemplo, si la prestación de un servicio es dependiente de conexión a la red SARA para consulta de información facilitada por otro organismo.
- Es sumamente importante interiorizar que la finalidad de la auditoría no debe consistir solamente en identificar todas las vulnerabilidades y transmitirlas como tal, sino que su objetivo último es evaluar las mismas estableciendo un proceso de priorización o triaje[1].

2.1 Evaluación de la superficie de exposición

Atendiendo a esa primera toma de contacto e información que pueda obtenerse, se articulará el siguiente proceso de auditoría que permita conocer el entorno global de infraestructuras e identificar los activos esenciales:

1. **Análisis inicial de superficie de exposición.**
   a. Llevar a cabo un análisis de los servicios expuestos, frente a los servicios internos. Se llevará a cabo una fase de identificación mediante escaneo de puertos, servicios y tecnologías.
   b. Para reducir riesgos relacionados con vectores de ataque interno o externo con afectación significativa interna (por ejemplo, acceso a servidores internos, identificación de exfiltración de datos internos, etc.), primará la necesidad de evaluación de los servicios internos frente a los servicios expuestos.

      Se llevará a cabo una identificación a través de reuniones, mapas de red que se puedan facilitar u otros mecanismos de identificación no tecnológicos de los servicios fundamentales, cómo se prestan y la segmentación existente.
   c. Para reducir riesgos relacionados con vectores de ataque exclusivamente externos (sin afectación o toma de control de sistemas internos), se llevará a cabo en una primera fase solamente la evaluación de servicios externos y en una segunda fase, aquellos servicios internos que tenga una relación directa con los servicios externos. Por ejemplo, los servidores de *back-end*, de autenticación o de Base de Datos si se ha analizado en una primera fase los frontales.

[1] Proceso de escoger, separar, entresacar. Se trata de aplicar un protocolo de evaluación de las prioridades, privilegiando la posibilidad de supervivencia, de acuerdo con las necesidades de atención y recursos disponibles a semejanza de la selección y clasificación de pacientes empleado en la enfermería y medicina de emergencias y desastres.

Se llevará a cabo una primera fase de identificación mediante escaneo de puertos, servicios y tecnologías y se obtendrá la identificación a través de reuniones, mapas de red que puedan facilitar u otros mecanismos de identificación no tecnológicos de los servicios en relación directa con los activos expuestos públicamente.

Como condición importante para llevar a cabo la auditoría en caso de que se haya producido una desconexión completa de la organización de Internet, o de las conexiones punto a punto con otros organismos, sería aplicar las ACL[2] adecuadas para poder realizar las auditorías en las condiciones similares a las que tendría un atacante en su acceso con la conexión a Internet normal.

2. **Ejecución de la Fase I de auditoría**.

   Se llevará a cabo una primera fase de auditoría sobre los activos fundamentales. En base al vector de la amenaza se identifica:

   a. Para evitar un ataque externo o ataque de vector indeterminado.
      i. Auditoría en caja negra[3] de las aplicaciones o servicios afectados.
      ii. Auditoría en caja negra de las comunicaciones.
      iii. Auditoría en caja blanca[4] de los servidores que soportan las posibles aplicaciones afectadas.
   b. Para evitar un ataque interno.
      i. Auditoría en caja blanca de los sistemas de autenticación.
      ii. Auditoría en caja blanca de los sistemas donde se alojan los datos esenciales a nivel de negocio.
      iii. Auditoría en caja blanca de los servicios fundamentales de negocio que se conocen públicamente: a usuarios externos u otras entidades.

3. **Ejecución de la Fase II de auditoría.**

   Se llevará a cabo una segunda fase. En base al vector de la amenaza se identifica:

   a. Para evitar un ataque externo.
      i. Auditoría en caja blanca de los sistemas relacionados con el acceso remoto.
      ii. Auditoría en caja blanca de los servidores de autenticación.

[2] *Access Control List*. Lista de Control de Acceso que permite controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores.

[3] Ejecución de pruebas e identificación de riesgos de seguridad sin tener información de la infraestructura ni privilegios en la misma.

[4] Ejecución de los análisis con el mayor alcance de investigación. Se requieren cuentas privilegiadas sobre los sistemas, servicios, aplicaciones o el código fuente para realizar los análisis oportunos.

iii. Auditoría en caja blanca de los servidores no expuestos.

iv. Auditoría en caja blanca de los servidores de base de datos.

b. Para evitar un ataque interno.

i. Auditoría en caja blanca de los sistemas relacionados con el acceso remoto.

ii. Auditoría en caja blanca de los servidores de aplicaciones internas.

iii. Auditoría en caja blanca de un muestreo de puestos de trabajo.

iv. Auditoría en caja blanca de los servicios de soporte a usuario.

c. Auditoría para evitar un ataque indeterminado.

i. Auditoría en caja blanca de los sistemas relacionados con el acceso remoto.

ii. Auditoría en caja blanca de los servidores no expuestos.

iii. Auditoría en caja blanca de los sistemas de autenticación.

iv. Auditoría en caja blanca de los sistemas donde se alojan los datos esenciales a nivel de negocio.

4. Ejecución de la Fase III de auditoría.

Se llevará a cabo una tercera fase. En base al vector de la amenaza se identifica:

a. Para evitar un ataque externo:

i. Auditoría en caja negra de aplicaciones o servicios internos en relación directa con las aplicaciones o servicios externos.

ii. Auditoría en caja blanca de la configuración de *firewall*.

iii. Auditoría en caja blanca de otros sistemas internos significativos y no auditados.

b. Ataque interno.

i. Auditoría en caja negra de aplicaciones o servicios publicados externamente.

ii. Auditoría en caja blanca de otros servicios internos significativos y no auditados.

iii. Auditoría de entornos de desarrollo y preproducción/integración.

c. Auditorías para prevenir en un ataque indeterminado.

i. Auditoría en caja blanca de los servidores de base de datos.

ii. Auditoría en caja blanca de un muestreo de puestos de trabajo.

iii. Auditoría en caja blanca de los servicios de soporte a usuario.

2.2 Priorización de corrección de vulnerabilidades atendiendo a la criticidad

Para un proceso de corrección de vulnerabilidades o para la implementación de aquellas que pueden ser consideradas no bloqueantes a efectos de la puesta en producción de un sistema debería primar:

- Riesgos identificables a través de auditoría que son asociables a vectores de riesgo. Por ejemplo, hallazgos de servicios o procesos asociados a la actividad de código dañino, vulnerabilidades recientemente publicadas o que hayan cambiado de estado por publicación de *exploit* o prueba de concepto.
- Vulnerabilidades o debilidades que de forma directa pueden haber sido empleadas por un atacante para la dispersión de un código dañino en la red o la escalada de privilegios. Por ejemplo, la identificación del protocolo SMBv1 en servidores o puestos de trabajo.
- Vulnerabilidades o debilidades de componentes o productos instalados que bien son innecesarios o por otro lado pueden suponer un riesgo típico en campañas de ransomware. Por ejemplo, productos ofimáticos instalados en servidores o productos ofimáticos desactualizados o fuera de soporte de puestos de trabajo tales como MS Office, Acrobat Reader o navegadores y las plantillas empleadas para las infraestructuras de acceso de usuarios remotos.
- Vulnerabilidades que, siendo de fácil explotación, pueden ser empleadas por un atacante para llevar a cabo movimientos laterales en la red o la obtención de información sensible de servidores o servicios. Ejemplo de ello son vulnerabilidades identificadas de fácil explotación como las de *Bluekeep* o *Apache Struts*.
- Otras vulnerabilidades, así como actualizaciones de Sistema Operativo o productos fuera de soporte que, sin suponer un problema para la funcionalidad de los servicios, permitan una mejora de la seguridad y la reducción de la Superficie de Exposición. Por ejemplo, retirada de servidores con sistemas operativos fuera de soporte e implementación de nuevos servidores como los correspondientes a DNS públicos.
- Resto de vulnerabilidades que son de una criticidad de nivel medio o inferior, o bien otras (que siendo complejas o imposibles de explotar) que implican para su subsanación la pérdida de funcionalidad del sistema.

  En estos casos, se aconseja la aplicación de medidas complementarias como aislamiento de los sistemas o acceso limitado a direcciones IP o puertos concretos, autenticaciones controladas/limitadas o el bloqueo de puertos y protocolos

empleados en el ataque: *RDP* (Remote Desktop Protocol) y *RPC* (Remote Procedure Call).

Siguiendo **un modelo de mejora continua, se debe primar la corrección por fases de las vulnerabilidades críticas** o de aquellas que puedan suponer una **peligrosidad potencial grave** para el sistema salvo que su aplicación suponga una pérdida de funcionalidad manifiesta de los servicios. En caso de que se identifique esa pérdida de funcionalidad, entonces deberán evaluarse **configuraciones de seguridad, medidas compensatorias o complementarias de vigilancia que hagan la superficie de exposición asumible** por parte de la entidad.

3. MEDIDAS INICIALES DE SEGURIDAD A APLICAR ANTE UNA PROBLEMÁTICA DE SEGURIDAD

Una vez evaluada la superficie de exposición y priorizada la corrección de vulnerabilidades y deficiencias de configuración, se ha de implementar una hoja de ruta de mejora continua identificando las medidas a aplicar a corto, medio y largo plazo. Dichas medidas servirán de mitigación o contingencia al tiempo que limitarán ataques o movimientos laterales en la red que pueda realizar una potencial amenaza.

Este procedimiento de implementación de medidas de subsanación atiende al modelo de mejora continua donde se ha establecido su aplicación, no exclusivamente en base a su criticidad, atendiendo entre otras cosas a:

- **Hallazgos para subsanar en el corto plazo**. Se aconseja su remediación antes de que se produzca, en su caso, la apertura de la conexión del sistema a Internet.
- **Hallazgos para subsanar de forma complementaria**. Se estima su remediación a medio plazo, mes o mes y medio, tras la identificación de la incidencia.
- **Hallazgos en mejora continua**. Requieren la aplicación de medidas adecuadas cuando no hay una fecha prevista a corto o medio plazo para su resolución.

3.1 Medidas a corto plazo

HALLAZGO	CRITICIDAD	MEDIDA DE SUBSANACIÓN A APLICAR
Aislamiento del sistema	CRÍTICA	Limitación de cualquier conexión fuera del organismo.
Usuario KRBTGT	CRÍTICA	Cambio de credenciales del usuario KRBTGT del Directorio Activo según especificaciones de Microsoft como medidas de prevención ante ataques de tipo Golden Ticket, Kerberos o similares.
Credenciales Administradores de dominio	CRÍTICA	Cambio de contraseñas de usuarios de administradores de dominio o deshabilitado de las cuentas innecesarias.
Inicio de sesión de Administradores de dominio limitado exclusivamente a DC	CRÍTICA	Generar una GPO que limite el inicio de sesión local e interactivo de los Administradores de Dominio exclusivamente en servidores con el rol de DC.
Credenciales servidores DC	CRÍTICA	Cambio de la contraseña de los servidores Controladores de Dominio.

HALLAZGO	CRITICIDAD	MEDIDA DE SUBSANACIÓN A APLICAR
Implementación del doble factor de autenticación	CRÍTICA	Implementar la funcionalidad de doble factor de autenticación en aquellos servicios de acceso externo, tales como el acceso a servicios de acceso remoto u Office 365, y que se encuentran expuestos de forma directa hacia Internet.
Afinidad geográfica de Office 365 o servicios de acceso externo	CRÍTICA	Al habilitar el mecanismo de doble factor, se ha de establecer una limitación de acceso condicional de índole geográfico a servicios de acceso remoto u Office 365, mientras no haya un control efectivo de la incidencia.
Acceso a consolas para administrar servidores críticos de negocio	CRÍTICA	Limitar, mediante ACL o Firewall local, el acceso a los equipos que se emplean para administrar servidores o servicios críticos. Se recomienda también limitar el inicio de sesión local a los usuarios que exclusivamente pueden emplear dichas consolas.
Resolución de vulnerabilidades de nivel crítico identificadas a través de las auditorías en relación con la priorización del punto 2.2	CRÍTICA	Aplicar las medidas de subsanación asociadas a las vulnerabilidades identificadas o, en su defecto, aplicar las medidas complementarias de mitigación.
Control de acceso a la red SARA y otros organismos para puertos empleados por el código dañino para su movimiento	ALTA	Limitar bidireccionalmente las conexiones por puertos empleados naturalmente por un atacante; por ejemplo, RDP y RPC entre la infraestructura del organismo y la red SARA o de otras entidades.
Credenciales usuarios del dominio	ALTA	Cambio de las credenciales de todos los usuarios de dominio.
Control de información en escritorios virtuales o escritorios remotos	ALTA	Limitar mecanismos bidireccionales de entrada y salida de datos no controladas entre el equipo remoto y el escritorio de usuario remoto (permitir USB, portapapeles, recursos compartidos, etc.).
Otras medidas que se consideren de remediación a corto plazo		

3.2 Medidas complementarias

HALLAZGO	CRITICIDAD	MEDIDA DE SUBSANACIÓN A APLICAR
Identificación y cambio de contraseñas de cuentas de servicio	CRÍTICA	Identificar las cuentas que, no siendo administradores de dominio, se encargan de administrar o levantar servicios. Dichas cuentas pueden estar en poder del atacante y podrían emplearse para iniciar acciones no autorizadas en la infraestructura.
Resolución de vulnerabilidades de nivel alto identificadas a través de las auditorías en relación con la priorización del punto 2.2	ALTA	Aplicar las medidas de subsanación asociadas a las vulnerabilidades identificadas o, en su defecto, aplicar las medidas complementarias de mitigación.

HALLAZGO	CRITICIDAD	MEDIDA DE SUBSANACIÓN A APLICAR
Firewall local de puestos de trabajo	ALTA	Con el objetivo de limitar movimientos hacia puestos de trabajo o entre ellos, se debería activar el firewall local de Windows para restringir al menos las conexiones entrantes. Se permitirían por reglas exclusivamente los accesos desde aquellas direcciones IP a puertos o servicios admitidos, tales como conexión a RDP desde equipos de microinformática, conexión para antivirus si fuera necesario, etc. En este sentido, no se ha de imponer una máxima restricción a aquellos puestos de trabajo que necesitan más puertos o servicios accesibles dado el uso que podría estar dando el organismo.
Deshabilitar o eliminar puestos de trabajo inactivos	MEDIA	Los puestos de trabajo, al igual que los usuarios, tienen credenciales que deben cambiarse periódicamente. Esto lo hacen de forma habitual los equipos activos. Sin embargo, en aquellos que están inactivos no se produce el cambio de esta y por lo tanto pueden emplearse por el atacante para autenticarse y moverse por la red.
Otras medidas que se consideren de remediación a medio plazo		

3.3 Medidas de mejora continua

HALLAZGO	CRITICIDAD	MEDIDA DE SUBSANACIÓN A APLICAR
Corrección de vulnerabilidades restantes	CRÍTICA	Tener en consideración el global de vulnerabilidades y deficiencias de configuración resultantes del proceso de auditoría efectuado y que son necesarias subsanar. La aplicación ANA del CCN-CERT está diseñada para hacer eficiente este proceso.
Firewall local de servidores	ALTA	Al objeto de limitar movimientos hacia servidores o entre ellos, se debería activar el firewall local para restringir al menos las conexiones entrantes. Se permitirían por reglas exclusivamente aquellos puertos o servicios necesarios, teniendo en consideración que determinados servicios, como el Escritorio Remoto, deberían estar limitados a un conjunto de direcciones IP autorizadas.
Gestión de administradores locales en MS Windows	ALTA	Implementar la solución LAPS que permita una gestión centralizada de cuentas de administrador local, impidiendo que una misma contraseña pueda ser empleada en múltiples activos.
Renovación de certificados de equipos	MEDIA	Sería adecuado renovar y generar nuevos certificados en servidores y servicios ya que el atacante podría haberlos vulnerado y estar bajo su control, pudiendo emplearlos para levantar servicios internos falsos.
Control de ejecución de Script de PowerShell	MEDIA	Sería recomendable configurar la política de ejecución de PowerShell (ExecutionPolicy) en modo Allsigned.
Otras medidas que se consideren de remediación a largo plazo		