

Certified Information Systems Security Professional

Buenos Aires Bootcamp

Donald R. Glass CISSP, CISA, CCNA, MCSE, MCSE+I, CNE

Agenda

Operations Security.

- Conceptos Generales.
- Controles Operacionales.
- Trusted Facility Management.
- Administración de Configuraciones.
- Amenazas/ Ataques.

Operations Security

Conceptos Generales

Seguridad Operacional

Seguridad Operacional refiere al acto de comprender las vulnerabilidades y amenazas de las operaciones de los centros de cómputo/ computadoras con el objetivo de dar soporte a dichas actividades que son las que permiten que los sistemas funcionen adecuadamente.

Este dominio se concentra en aquellos controles que permiten proteger el *hardware*, *software* y los *medios de almacenamiento de datos*.

Principios Generales de Seguridad

Responsabilidad (Accountability).

Mínimo Privilegio (Least privilege).

Separación de Tareas.

Reducción de Riesgos.

Defensa en Capas (Layered defense).

Redundancia.

Responsabilidad (Accountability)

Revisiones de Personal - Background checks.

Administración de Passwords.

Monitoreo (Logging) de toda actividad.

- Log protegido/ duplicado.

Reporte de Problemas y Procedimientos de Cambios.

- Reporta, localiza y resuelve problemas que afecten al servicio prestado.
 - Reduce fallas.
 - Previene recurrencias.
 - Reduce el impacto.
- Tipos - Performance/disponibilidad.

Responsabilidad (Accountability)

Reporte de Problemas y Procedimientos de Cambios.

- Análisis de Violaciones.
 - Repetición de errores.
 - Autoridad Excesiva.
 - Acceso Irrestricto.
 - Patrones - hackers, empleados descontentos.
 - Clipping level – nivel base de cantidad de violaciones que establecesn condiciones normales.

Mínimo Privilegio (Least privilege)

Control granular de acceso sobre los comandos/ utilidades del sistema.

Permisos de acceso individuales.

Existencia de componentes y procedimientos de Hardware/Software que permitan el acceso autorizado e inhabiliten aquel que no lo sea.

Revisión periódica de accesos otorgados/ necesarios.

Separación de Tareas

Todo cambio/ modificación requiere de aprobación.

El staff del área de Operaciones no debe

- codificar ni aprobar cambios a aplicaciones/ sistemas.
- realizar tareas de seguridad informática.
- realizar funciones de data entry.

Las responsabilidades en el área de Operaciones deben ser divididas.

Operations Security

Controles Operacionales

Controles de Operaciones

Protección de Recursos.

Controles de Hardware.

Controles de Software.

Controles de Entidades-Privilegiadas.

Controles de Medios.

Controles de Acceso Físico.

Protección de Recursos

Hardware.

- Comunicaciones.
- Medios de almacenamiento.
- Sistemas de Procesamiento.
- Computadoras stand-alone.
- Otros dispositivos (impresoras, faxes, etc).

Protección de Recursos

Software.

- Librerías de Programas y código fuente.
- Software propietario o de proveedores.
- Sistemas Operativos y Utilidades de los sistemas.

Protección de Recursos

Datos.

- Backups.
- Archivos de usuario.
- Archivos de contraseñas.
- Directorios del sistema operativo.
- Logs del sistema y rastros de auditoría.

Controles de Hardware

Mantenimiento de Hardware.

Cuentas de usuario de mantenimiento.

Control de puertos de diagnóstico.

Control físico del hardware.

- Terminales y estaciones de operación.
- Gabinetes o armarios en dónde se almacenen datos.
- Data centers de Servidores y Comunicaciones.
- Pools de modems y cuartos de cableado de telecomunicaciones.

Controles de Software

Administración del sistema anti-virus.

Prueba de software (software testing).

Utilidades del sistema (system utilities).

Almacenamiento seguro de software/ datos.

Controles de Backup.

Controles de Entidades Privilegiadas

El acceso a entidades privilegiadas, también conocido como *funciones de operación privilegiadas* se define como el acceso especial o extendido a recursos informáticos que se le otorga a operadores y administradores de los sistemas.

Clases de entidades privilegiadas:

- Comandos del sistema.
- Parametros del sistema.
- Programa de control del sistema (Control Program Management).

Controles de Medios de Almacenamiento

Controles de Seguridad de Medios de Almacenamiento.

- Registro de uso de medios (logging).
- Control de accesos a los medios.
- Eliminación/ borrado. Destrucción apropiada de medios de almacenamiento (*data remanence*).

Controles de viabilidad de medios de almacenamiento.

- Etiquetado.
- Trato (uso, transporte de los medios de almacenamiento).
- Almacenamiento.

Controles de Acceso Físico

Hardware.

- Control del equipamiento computacional y de comunicaciones.
- Control de los medios de almacenamiento.
- Control de reportes y logs impresos.

Software.

- Control de los archivos de backup.
- Control de las aplicaciones de producción.
- Control de datos/ información sensitiva/ crítica.

Controles de Acceso Físico

Personal.

- Personal del departamento de IT.
- Personal de limpieza.
- Personal de mantenimiento del sistema de A/C.
- Personal de empresas de servicios contratado.
- Consultores, proveedores y personal temporario.

Monitoreo y Auditoría

Monitoreo.

- Detección de Intrusos.
- Penetration Testing.
- Análisis de Violaciones de seguridad.

Auditoría.

- Auditorías de Seguridad/ IT.
 - Interna.
 - Externa.
- Registros de Auditoría (Logs).

Operations Security

Trusted Facility Management

Definiciones

Aceptación (Acceptance).

- Verificación que los requerimientos de seguridad y performance hayan sido alcanzados

Acreditación (Accreditation).

- Aceptar formalmente que el nivel de seguridad es adecuado, la autorización para operar es adecuada y el nivel de riesgo existente es aceptable.

Certificación (Certification).

- Pruebas formales de los controles de seguridad.

Definiciones

Operational assurance.

- Verificación de que el sistema opere en concordancia con sus requerimientos de seguridad.

Assurance.

- Grado de confianza de que las medidas de seguridad implantadas funcionan como se espera.

Trusted System Operations

Trusted computer base – Todo el HW/FW/SW se encuentra protegido por mecanismos adecuados de seguridad a un nivel apropiado de sensibilidad/ seguridad de forma tal de asegurar el cumplimiento de una política de seguridad dada.

Trusted facility management – soporta roles separados de operación y administración (B2).

Claramente se identifican las funciones de administración de seguridad.

Trusted recovery procedures

La seguridad del sistema no resulta comprometida ante una caída del sistema y su posterior recuperación.

Requiere de backups.

Reboot (Crash or pérdida de electricidad).

Recuperación de file systems (recursos perdidos).

Recupero de archivos y bases de datos (datos/ base de datos inconsistentes).

Revisión de archivos/ controles de seguridad (sistema comprometido).

Operations Security

Administración de Configuraciones

Administración de Configuraciones

Controlar modificaciones al sistema:

- Hardware.
- Firmware.
- Software.
- Documentación relacionada.

Asegurar la integridad y limitar cambios no autorizados.

Administración de Configuraciones

Controles base.

- Políticas, standards y procedimientos.
- Responsabilidades.
- Requerimientos.
- Evaluaciones de impacto.
- Nivel de mantenimiento del software (software level maintenance).

Operations Security

Amenazas/ Ataques

Amenazas a la seguridad Operacional

Pérdida Accidental.

- Errores u omisiones en inputs de operadores.
- Errores de procesamiento de transacciones.

Actividades Inapropiadas.

- Contenido Inapropiado.
- Desperdicio/ Uso indebido de recursos corporativos.
- Sexual/ Racial Harassment.
- Abuso de privilegios o derechos.

Amenazas a la seguridad Operacional

Operaciones ilegales y Ataques intencionales.

- Monitoreo (eavesdropping).
- Fraude.
- Robo.
- Sabotaje.
- Ataques externos.

Operations Security

Preguntas?

This document was created with Win2PDF available at <http://www.daneprairie.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.