Controles de seguridad

José Galaviz

1 Inventario de dispositivos autorizados y no autorizados

- Mantener un inventario permanente de dispositivos conectados y que pueden operar dentro de la organización.
- Servidores, estaciones de trabajo, laptops, tablets, etc.
- También los que se pueden conectar remotamente.

Inventario de software autorizado y no autorizado

- Identificar software vulnerable para la organización y desautorizar su uso.
- Hacer un catálogo de software de sistema y de aplicación que puede utilizarse.
- Dar alternativas seguras a las necesidades.

Configuraciones seguras de hardware y software

- Establecer configuraciones estándar seguras en el software de sistema.
- Imágenes de SO seguras.
- Mantenimiento de parches de seguridad y versiones estables.

Evaluación contínua de vulnerabilidades y mitigación

- Estar permanentemente informado de exploits, vulnerabilidades en el hardware y software que se utiliza.
- Hacer los cambios o actualizaciones pertinentes.

Defensa contra malware

- Usar software especializado en detección y eliminación de software malicioso.
- Que se actualice automáticamente.
- Establecer políticas de prevención que impidan que el malware ingrese a los sistemas.

Seguridad de software de aplicación

- Probar el software de terceros y el elaborado internamente para verificar su seguridad.
- Establecer políticas seguras de diseño y desarrollo de software.
- Capacitar al personal de desarrollo.
- Establecer controles de seguridad en el acceso a las aplicaciones de manera remota: inspeccionar el tráfico, establecer alertas.

Control de dispositivos inalámbricos

- Sólo los dispositivos que cumplen con los requisitos de configuración se pueden conectar a la red interna.
- Asegurarse de que todos los puntos de acceso inalámbricos son accesibles y configurables remotamente.
- Escanear frecuentemente para detectar puntos de acceso no autorizados.

Capacidad de recuperación

- Implementar un plan de recuperación de información tras un ataque.
- Implementar un esquema de recuperación segura de evidencia del incidente.
- Establecer políticas de respaldo que permitan continuar con la operación crítica lo más pronto posible minimizando la pérdida.
- Determinar y pronosticar las capacidades de almacenamiento requeridas.
- Determinar la redundancia requerida.

Evaluación frecuente de la capacitación en seguridad

- Evaluar las capacidades y conocimientos de seguridad del personal. Desde las áreas técnicas especializadas hasta el no directamente involucrado con el manejo de información sensible.
- Establecer un plan de capacitación permanente para todos:
  - Desde security awareness, hasta…
  - Entrenamiento certificado (CISSP, p. ej.)
- Establecer el perfil adecuado para cada tipo de personal.

Configuraciones seguras para equipo de seguridad perimetral

- Enrutadores, cortafuegos, switches, puntos de acceso; todos deben tener configuraciones adecuadas y seguras para proteger las diferentes áreas de la organización.
- Establecer áreas de seguridad diferenciada si es necesario.

Limitar puertos,protocolos y servicios disponibles

- Aplicar políticas de filtrado de paquetes basándose en el host y en el puerto de acceso.
- Verificar el tráfico y tener capacidad de bloquear el tráfico no autorizado.
- Limitar acceso externo en lo posible.
- Remover software y servicios no necesarios.

Control estricto de privilegios de administración

- Usar passwords robustos.
- Cada quien tiene acceso sólo a lo que requiere para hacer su trabajo.
- Tiene acceso mientras tenga ese trabajo.
- Autenticar y validar cada cuenta.
- Establecer tiempos límite.
- Autorizar en función de una jerarquía de acceso.

Mantener y verificar las bitácoras de seguridad

- Establecer un sistema de alertas automático sobre los logs de seguridad del sistema.
- Verificarlos, renovarlos, y respaldarlos

Prevenir pérdida de datos

- Establecer políticas de qué sale y qué no de la organización y por qué medios.
- Minimizar la exposición de información sensible.

Pruebas de penetración, respuesta a incidentes

- De ser posible contratar empresa especializada en seguridad para hacer pruebas de penetración y hacking de sombrero blanco.
- Tener un equipo capacitado en respuesta a incidentes.