DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

20 Controles Críticos (CIS Controls 7.1)

Fundamentos de ciberseguridad

Profesor

Juan Ignacio Iturbe A., Mg.

Introducción

- Los controles CIS (*Center for Internet Security*) son un conjunto de acciones priorizadas y altamente focalizadas.
- Colectivamente forman un conjunto de mejores prácticas de defensa.
- Mitigan los ataques más comunes contra sistemas y redes.
- La información disponible para los profesionales de seguridad sobre lo que deberían hacer para proteger su infraestructura no es escasa.

Introducción

- Como defensores, tenemos acceso a una extraordinaria variedad de información y tecnología:
  - herramientas de seguridad
  - hardware
  - estándares de seguridad
  - entrenamientos y clases
  - certificaciones
  - bases de datos de vulnerabilidad
  - orientación, mejores prácticas
  - catálogos de controles de seguridad
  - innumerables listas de verificación de seguridad
  - puntos de referencia
  - recomendaciones

Introducción

- Para la comprensión de las amenazas:
  - *feeds* de información de amenazas
  - informes
  - herramientas
  - servicios de alerta
  - estándares
  - *frameworks* de intercambio de amenazas

Introducción

- Para colmo, estamos rodeados de:
  - requisitos de seguridad
  - marcos de gestión de riesgos
  - regímenes de cumplimiento
  - mandatos regulatorios
  - Etc

¿Cuáles son las áreas más críticas que debemos abordar y cómo debe una empresa dar el primer paso para madurar su programa de gestión de riesgos?

¿Dónde y cómo empiezo?

¿cómo podemos encaminarnos con una hoja de ruta de fundamentos y una guía para medir y mejorar?

¿Qué pasos defensivos tienen el mayor valor?

Los controles CIS

- Estos son los tipos de problemas que provocaron y ahora conducen los controles CIS.
- Los controles de CIS han sido madurados por una comunidad internacional de personas e instituciones que:
  - comparten información sobre ataques y atacantes, herramientas, ayudas de trabajo y traducciones.
  - identifican problemas comunes.
  - mapean los Controles de CIS a los marcos regulatorios y de cumplimiento.
  - documentan historias de adopción y compartir herramientas para resolver problemas.

Principios

1. *La ofensiva informa a la defensa:* aprender continuamente y usar aquello demostrado.
2. *Priorización:* invierta en los controles que proporcionen mayor reducción del riesgo.
3. *Mediciones y métricas:* establezca un lenguaje común.
4. *Diagnóstico y mitigación continuos:* mediciones continuas para validar la efectividad de los controles y para dirigir la prioridad de los siguientes pasos.
5. *Automatización:* automatice las defensas.

Controles CIS: ¿Qué es lo que deberíamos estar todos haciendo?

Básicos

1. Inventario y control de activos de hardware
2. Inventario y control de activos de software
3. Gestión continua de vulnerabilidades
4. Uso controlado de privilegios administrativos
5. Configuración segura de hardware y software
6. Mantenimiento, monitoreo y análisis de logs de auditoría

Controles de "Higiene cibernética"

Fundamentales

7. Protecciones para correo electrónico y navegador web
8. Defensas contra malware
9. Limitación control de puertos de red, protocolos y servicios
10. Capacidad para recuperar datos
11. Configuración segura para dispositivos de red
12. Defensa perimetral
13. Protección de datos
14. Control de acceso basado en la necesidad de conocer
15. Control de acceso inalámbrico
16. Control y monitoreo de cuentas

Organizacionales

17. Implementar un Programa de concientización y entrenamiento
18. Seguridad en las aplicaciones de software
19. Respuesta ante incidentes y gestión
20. Pruebas de penetración y ejercicios "Red Team"

Estructura del documento de los Controles CIS

- La presentación de cada control del documento CIS incluye los siguientes elementos:
  - Descripción de la importancia de cada control (¿Por qué es importante este control?) en cuanto al bloqueo o identificación de un ataque y una explicación de cómo un atacante explota activamente la ausencia de dicho control.
  - Una tabla de acciones específicas ("sub-controles") que una organización debe tomar para implementar el control.
  - Procedimientos y herramientas que permiten la implementación y automatización del control.
  - Ejemplo de diagramas de relaciones de entidades que muestran los componentes de la implementación.

Grupos de implementación

- La versión 7.1 de los CIS Controles introduce los grupos de implementación (IG).
- Históricamente, los Controles CIS utilizaron su orden para enfocar las actividades de ciberseguridad.
- Muchas de las prácticas dentro de los controles de higiene cibernética CIS pueden ser difíciles de implementar para organizaciones con recursos limitados.
- Por lo que CIS actualizó su guía para priorizar la utilización del Control CIS.

Grupos de implementación

- Cada IG identifica un subconjunto de los Controles CIS para una organización con un perfil de riesgo y recursos similares.
- Cada IG se basa en el anterior.
- Las organizaciones deben implementar sub-controles en IG1, seguidos por IG2 y luego IG3.

IG 1	IG 2	IG 3
Negocio familiar Aprox. 10 empleados Experiencia y recursos limitados en TI y ciberseguridad Preocupación: “Mantener el negocio operando” Sus datos sensibles son la información financiera y la de sus empleados	Organización regional Emplea a individuos responsables de administrar y proteger la infraestructura de TI Diferentes perfiles de riesgo según la función y la misión del trabajo. Pueden tener cargas de cumplimiento normativo. Preocupación importante es la pérdida de la confianza del público si se produce un ataque exitoso. A menudo almacenan y procesan información confidencial de clientes o empresas y pueden soportar interrupciones breves del servicio	Organización con miles de empleados Emplea expertos en seguridad que se especializan en las diferentes facetas de la ciberseguridad (por ejemplo, gestión de riesgos, pruebas de penetración, seguridad de aplicaciones) Sus sistemas y datos contienen información confidencial o funciones que están sujetas a supervisión regulatoria y de cumplimiento. Debe abordar la disponibilidad de servicios y la confidencialidad y Integridad de los datos sensibles. Los ataques exitosos pueden causar un daño significativo al bienestar público.

Ejemplo de control

CIS CONTROL 13: PROTECCIÓN DE DATOS

CIS Control 13: Protección de datos

Los procesos y herramientas utilizadas para prevenir la exfiltración de datos, mitigar el efecto de la exfiltración de datos y asegurar la privacidad e integridad de la información sensible.

¿Por qué es importante este control?

Los datos residen en muchos lugares. La mejor manera de lograr la protección de esos datos es mediante la aplicación de una combinación de encriptación, protección de integridad y técnicas de prevención de pérdida de datos. A medida que las organizaciones continúan su avance hacia la computación en la nube y el acceso móvil, es importante que se tome la precaución adecuada para limitar e informar sobre la filtración de datos al tiempo que se mitigan los efectos del compromiso de los datos.

Algunas organizaciones no identifican ni separan cuidadosamente sus activos más sensibles y críticos de información menos sensible y de acceso público en sus redes internas. En muchos entornos, los usuarios internos tienen acceso a todos o la mayoría de los activos críticos. Los activos sensibles también pueden incluir sistemas que proporcionan administración y control de sistemas físicos (por ejemplo, SCADA). Una vez que los atacantes han penetrado en dicha red, pueden encontrar y extraer fácilmente información importante, causar daño físico o interrumpir operaciones con poca resistencia. Por ejemplo, en varias filtraciones de alto perfil en los últimos dos años, los atacantes pudieron obtener acceso a datos confidenciales almacenados en los mismos servidores con el mismo nivel de acceso que los datos menos importantes. También hay ejemplos de cómo usar el acceso a la red corporativa para obtener acceso para controlar los activos físicos y causar daños.

Sub control	Tipo de activo	Función de Seguridad	Control	Descripción	Grupos de implementación		
					1	2	3
13.1	Datos	Identificar	Mantener un inventario de información sensible	Mantenga un inventario de toda la información sensible almacenada, procesada o transmitida por los sistemas de tecnología de la organización, incluidos los ubicados en la organización o en un proveedor de servicios remoto.	●	●	●
13.2	Datos	Proteger	Remover datos o sistemas sensibles que no son accedidos regularmente por la Organización	Elimine datos o sistemas sensibles a los que la organización no accede regularmente desde la red. Estos sistemas solo se utilizarán como sistemas autónomos (desconectados de la red) por parte de la unidad de negocio que necesite utilizar el sistema de vez en cuando o completamente virtualizados y apagados hasta que sea necesario.	●	●	●
13.3	Datos	Detectar	Monitorear y bloquear el tráfico de red no autorizado	Implemente una herramienta automatizada en el perímetro de la red que monitoree la transferencia no autorizada de información sensible y bloquee dichas transferencias mientras alerta a los profesionales de seguridad de la información.			●
13.4	Datos	Proteger	Permitir solamente el acceso a proveedores de servicios de nube o correo autorizados	Permita solo el acceso a proveedores de servicio de almacenamiento en la nube o correo electrónico autorizados.		●	●

Sub control	Tipo de activo	Función de Seguridad	Control	Descripción	Grupos de implementación		
					1	2	3
13.5	Datos	Detectar	Monitorear y detectar cualquier uso no autorizado de cifrado	Monitoree todo el tráfico que sale de la organización y detecte cualquier uso no autorizado de cifrado.			●
13.6	Datos	Proteger	Cifrar el disco duro de todos los dispositivos móviles	Utilice software de cifrado de disco completo aprobado para cifrar el disco duro de todos los dispositivos móviles.	●	●	●
13.7	Datos	Proteger	Gestionar dispositivos USB	Si se requieren dispositivos de almacenamiento USB, se debe usar software corporativo que pueda configurar sistemas para permitir el uso de dispositivos específicos. Se debe mantener un inventario de tales dispositivos.		●	●
13.8	Datos	Proteger	Gestionar las configuraciones de lectura/escritura de sistemas para medios removibles externos	Configure los sistemas para que no escriban datos en medios extraíbles externos, si no existe una necesidad de negocio para admitir dichos dispositivos.			●
13.9	Datos	Proteger	Cifrar los datos en dispositivos de almacenamiento USB	Si se requieren dispositivos de almacenamiento USB, todos los datos almacenados en dichos dispositivos se deben cifrar en reposo.			●

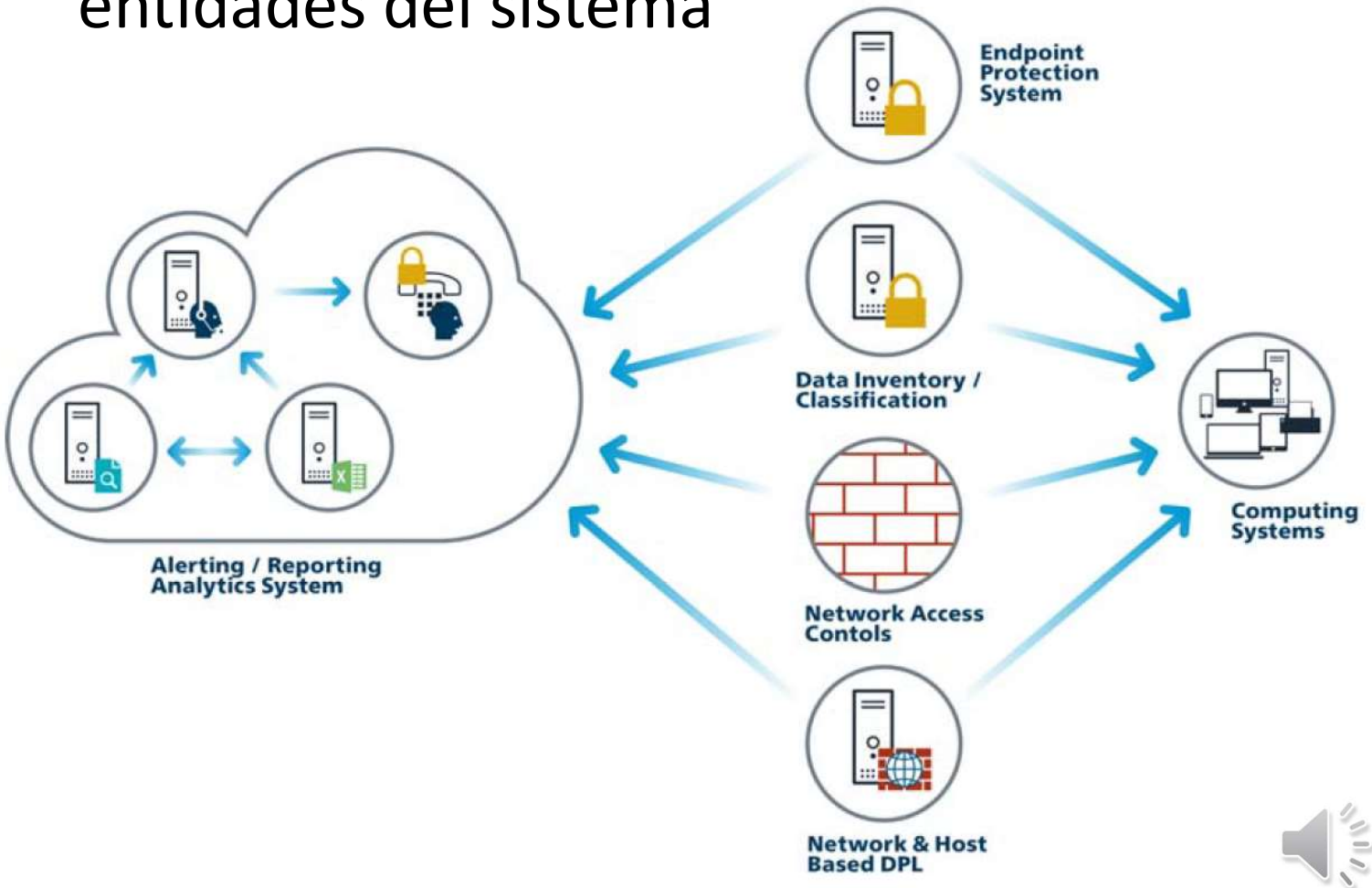
CIS Control 13: Procedimientos y herramientas

Es importante que una organización comprenda cuál es su información sensible, dónde reside y quién necesita acceder a ella. Para derivar niveles de sensibilidad, las organizaciones necesitan armar una lista de los tipos clave de datos y la importancia general para la organización. Este análisis se usaría para crear un esquema general de clasificación de datos para la organización. Las organizaciones deben definir etiquetas, tales como por ejemplo "Sensible", "Confidencial para el negocio" y "Pública", y clasificar sus datos según esas etiquetas. Una vez que se ha identificado la información privada, se puede subdividir en función del impacto que tendría para la organización si se viera comprometida.

Una vez que se ha identificado la sensibilidad de los datos, cree un inventario o mapeo de datos que identifique las aplicaciones de negocio y los servidores que albergan esas aplicaciones. Luego, la red debe segmentarse para que los sistemas del mismo nivel de sensibilidad estén en la misma red y segmentados de los sistemas con diferentes niveles de confianza. Si es posible, los firewalls deben controlar el acceso a cada segmento.

El acceso a los datos debe basarse en los requisitos del trabajo y en la necesidad de saberlo. Se deben crear requisitos de trabajo para cada grupo de usuarios para determinar a qué información necesita acceder el grupo para realizar sus trabajos. En función de los requisitos, el acceso solo se debe otorgar a los segmentos o servidores de datos que se necesitan para cada función de trabajo. El registro detallado debe activarse para los servidores con el fin de rastrear el acceso y permitir que el personal de seguridad examine los incidentes en los que se accedió incorrectamente a los datos.

Diagrama de relaciones de entidades del sistema



Bibliografía

- https://www.cisecurity.org/
- https://learn.cisecurity.org/cis-ram