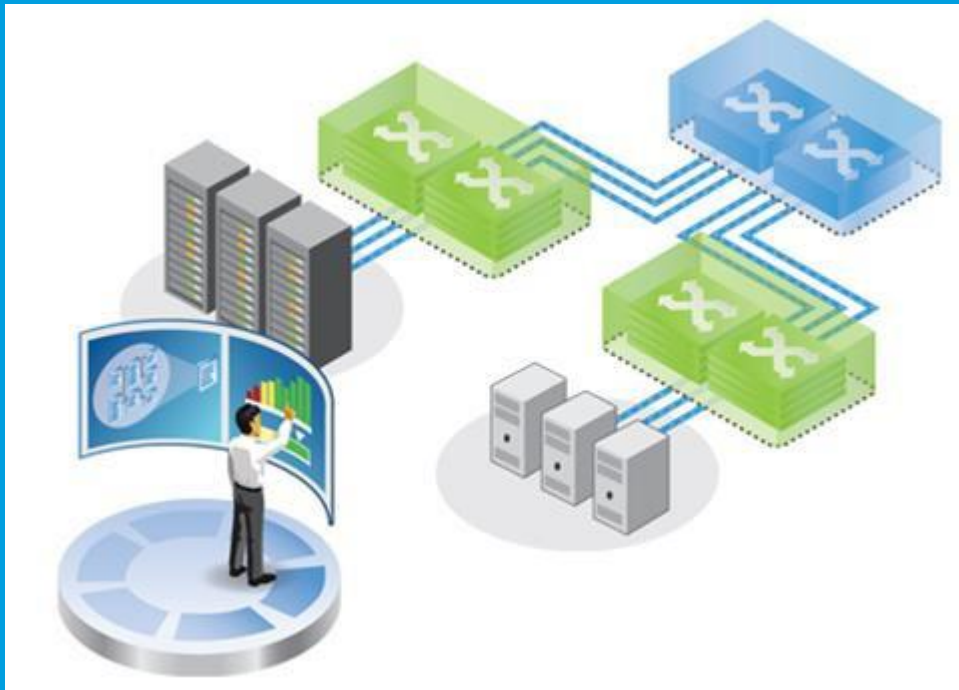
SOS CHILDREN'S VILLAGES INTERNATIONAL

Servicios de redes de TIC

Normas mundiales mínimas para la seguridad de la Información, gestión de la continuidad del negocio y gestión de redes

March 2020 - Versión 3.2 – Aprobado por el MCO

DOCUMENTO DE APOYO A LA POLÍTICA DE LA SECRETARÍA GENERAL



PUESTA EN PRÁCTICA DE POLÍTICAS Y NORMAS DE CALIDAD

USUARIOS CLAVE

Obligatorio para:	*Todas las unidades de la GSC, tolas las Asociaciones Miembro que no están en vía de la sostenibilidad, todas las Asociaciones Miembro dirigidas por la GSC*
Recomendado para:	*Asociaciones Miembro en vía de la sostenibilidad, Asociaciones de promoción y apoyo*

DOCUMENTOS, HERRAMIENTAS Y SISTEMAS RELACIONADOS

Good Management And Accountability Quality Standards	*Standard 3: Proactive protection and management of assets* 3.1 Personal information and other data must be protected 3.2. Good information and communication infrastructure
BSI Standard 200-1	*Information Security Management Systems (ISMS)* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2001_en_pdf.html
BSI Standard 200-2	*IT-Grundschutz Methodology* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.html
BSI Standard 200-3	*Risk Analysis based on IT-Grundschutz* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html
BSI-Standard 100-4	*Business Continuity Management* https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html
SecurityFocus	http://www.securityfocus.com/
Center for Internet Security	https://www.cisecurity.org
ISO/IEC 27001	http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
BCM	*The Definitive Handbook of Business Continuity Management,* http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470670142.html
SOSCV SharePoint	*Global Information Security Guidelines* https://soscv.sharepoint.com/sites/WS_000253/Wiki/Information%20Security.aspx#7
Appendix Information Security Standards V3	https://soscv.sharepoint.com/sites/WS_000254/Wiki/Network%20Services.aspx#7

RESPONSABLE DEL CONTENIDO

Función:	*Tecnología de la Información y Comunicación*
Autor:	*Oliver Vavtar, Team Leader Network Services – en estrecha colaboración con Florian Krall de la unidad ICL, DPO Dr. Kraska GSC, D-ICTs y el grupo de trabajo de Protección de Datos y Seguridad de la información de Nethope*

PROCESO DE DESARROLLO

Aprobado por:	*GSC Global ICT Network and Management Council*
Idioma original:	*Inglés*

HISTORIAL DE CAMBIOS

Versión	Fecha	Cambios
3.2	*Mar 2020*	*"Usuarios Clave" y "Proceso de Desarrollo" y capitulo 1 se alinearon con el documento de alcance del MCO y la decisión del MCO*
3.1	*Dic 2019*	*Especificación de grupos de implementación (1.3.1) y evaluación de controles, enfoque de calificación (1.3.2)*
3.0	*Jun 2019*	*Se implementó controles CIS 7.1, se revisó los controles de la GCN y SGR en términos de la operación de TIC orientada a la nube/subcontratación*
2.0	*Mar 2017*	*Se revisó servicios empresariales críticos (1.2), cloudsourcing y clasificación de servicios de ICT (2.3 Medidas organizativas), Gestión de Seguridad de la información (3), 'trae tu propio dispositivo' (BYOD) y normativa para dispositivos móviles, (3.4 Conexiones de red e Internet)*
1.1	*Ene 2015*	*Se revisó la gestión de redes (4.6 sistema de gestión de redes SGR centralizada) y estándares de hardware (2.1 Medidas técnicas)*
1.0	*Jun 2013*	*Cambios finales y acuerdo realizados por ICT Function Network*

Tabla de Contenidos

1 Introducción

1.1 Troncal digital sólida para una organización profesional y confiable

Aldeas Infantiles SOS, como organización descentralizada que utiliza aplicaciones y procesos compartidos, debe tener una troncal digital fuerte y sólida. Hoy en día, tener un entorno estable y seguro en términos de TI no es solo una necesidad comercial, es también indicación clara de ser una organización profesional y confiable. Esto tiene especial importancia para Aldeas infantiles SOS ya que cada vez se involucra más colaborando en todos los niveles con socios externos para recaudar fondos y brindar apoyo a asociaciones.
Ver también Good Management And Accountability Quality Standards

Estándar 3: Protección proactiva y gestión de activos

3.1 Información personal y otros datos que deben estar protegidos

3.2 Buena infraestructura de información y comunicación

Para satisfacer las necesidades comerciales actuales y futuras, en términos de servicios de TIC confiables, seguros y potentes, Aldeas Infantiles SOS necesitará infraestructura y sistemas completos y armonizados, que además sean más eficientes al ser operados y mucho más fáciles de manejar.

1.2 Servicios empresariales esenciales

El término “servicios empresariales esenciales” se refiere a activos y valores que son necesarios para que la organización ejecute sus negocios respectivamente, para permitir una operación comercial confiable.

Esos servicios empresariales esenciales son, por ejemplo, O365 Mail, Base de Datos de Programas PDB, D365/AmpImpact, Compass, Salesforce CRM, Digify, SOS Collaboration, SOS Controlling System, Navision Finance y otros servicios importantes on-premise y en la nube. Además, la infraestructura particular de red local e Internet como un factor de influencia subyacente y esencial, en cuanto a confiabilidad, integridad, disponibilidad y rendimiento.

1.3 Enfoque holístico

Toda medida, control, actividad o procedimiento en este documento ha sido seleccionado considerando lo que es absolutamente necesario para satisfacer las necesidades empresariales hoy en día, al contrario de aplicar medidas inapropiadas que son demasiado caras, ineficaces o incorrectas.

Sin embargo, a diferencia de reinventar la rueda, se ha implementado las mejores prácticas internacionales y las normas de facto, así como las normas de seguridad de la autoridad nacional de seguridad cibernética de Alemania, las referencias y controles ISO del Centro de Seguridad de Internet, así como las mejores prácticas de Nethope Data Protection e Information Security Workgroup, por nombrar algunos ejemplos.

1.3.1 Grupos de Implementación

El objetivo principal de este documento es llevar las medidas existentes en materia de Gestión de Seguridad de la información y Gestión de Continuidad de las Operaciones a un nivel contemporáneo y para establecer un Sistema de Gestión de Redes a fin de otorgar garantías sobre la disponibilidad de servicios de TIC y para brindar resultados predecibles en materia de TIC en términos de rendimiento de este servicio.

Aldeas Infantiles SOS ha definido tres grupos de implementación (IGs), los cuales representan un corte horizontal a través de los controles adaptados a los diferentes tipos de unidades de negocio de la organización.

Cada IG se basa en el anterior. De esta forma, IG2 incluye IG1, e IG3 incluye todos los controles de IG1 e IG2. Como ejemplo, si una unidad de negocio está compartiendo información, que está obligada a cumplir con las regulaciones de protección de datos, la unidad debe proteger dichos datos críticos y, por lo tanto, debe pasar a un IG más alto.

Grupo de Implementación 1, IG1

- Las unidades de IG1 **procesan[1] información confidencial de la organización y datos de identificación personal**, lo que también está relacionado con las regulaciones locales de protección de datos y GDPR. **La información no se publica o se hace accesible fuera** de los limites lógicos locales como los firewalls de Internet, lo cual reduce la superficie de ataque.
- Los **ataques exitosos causan un daño significante en un contexto local o regional** a las Aldeas Infantiles SOS.
- Las unidades de IG1 **tienen demandas medias en términos de disponibilidad[2] y rendimiento[3]** de sistemas y servicios IG3.

Ejemplos para una unidad IG1: AM, Unidades de Programa como Escuelas, Centros Médicos, Respuesta de Emergencias, etc.

Grupo de Implementación 2, IG2

- Las unidades de IG2 **procesan información confidencial de la organización y datos de identificación personal en gran escala[4]**, lo que también está relacionado con las regulaciones locales de protección de datos y GDPR. **La información se publica o se hace accesible desde fuera de los limites lógicos locales como los firewalls de Internet**, lo que aumenta la superficie de ataque.
- Las unidades IG2 son sujetas a **Evaluaciones de Impacto de Protección de Datos[5] (DPIAs) y revisiones para determinar si el procesamiento es "probable que resulte en un alto riesgo"**
- Los **ataques exitosos causan un daño significativo** a las Aldeas Infantiles SOS.
- Las unidades IG2 tienen **altas demandas en términos de disponibilidad y rendimiento de sistemas y servicios.**

Ejemplos para una unidad IG2: OIR, OIR/BO, Oficina Nacional, Sucursal Nacional, etc.

Grupo de Implementación 3, IG3

- Las unidades de IG3 **procesan información confidencial de la organización y datos de identificación personal en gran escala**, lo que también está relacionado con las regulaciones locales de protección de datos y GDPR. La **información se publica o se hace accesible desde fuera** de los limites lógicos locales como los firewalls de Internet, lo que aumenta la superficie de ataque.
- Las unidades IG3 son sujetas a **Evaluaciones de Impacto de Protección de Datos[6] (DPIAs) y revisiones para determinar si el procesamiento es "probable que resulte en un alto riesgo"**
- Los **ataques exitosos causan un daño significativo** a las Aldeas Infantiles SOS.
- Las unidades IG3 tienen las **mayores demandas en términos de disponibilidad y altas demandas en rendimiento de los sistemas y servicios**.

Ejemplos para una unidad IG3: Oficina Internacional, Joint Systems, 3rd parties (socios de negocios externos, ejemplo: proveedor de soluciones, proveedor de nube, empresas de consultoría, empresas externas durante el periodo de un proyecto, etc.) procesando datos confidenciales y datos de identificación personal en su rol como Sub-Procesador GDPR de Aldeas Infantiles SOS.

---

[1] Art. 4 GDPR, (2) processing, https://gdpr-info.eu/art-4-gdpr

[2] Availability demands
- Medium: >98%, allowed downtime per year max. 7d, 7h
- High: >99%, allowed downtime per year max. 3d, 15h
- Highest: >99,8%, allowed downtime per year max. 1d 2h

[3] Performance demands
- Medium: stable business service e.g. Collaboration, SalesForce, D365, etc.
- High: stable A/V real time communication e.g. Skype for Business

[4] Large scale data processing, https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf (Article 37(1)(b) and (c))

[5] Guidelines on Data Protection Impact Assessment

1.3.2 Evaluación de controles, enfoque de calificación

Todos los controles son monitoreados regularmente por medio de la herramienta ICT Performance Cockpit, en el cuál, los datos reportados también son una referencia para auditorías internas.

Al medir cada control respecto de los modelos de madurez de COBIT 5, Aldeas Infantiles SOS puede revisar las medidas ya completadas y compararlas con las medidas que necesitan ser realizadas en el futuro.

Nivel	Nombre	Descripción
0	No existente	Los procesos de gestión no se aplican en absoluto. Falta total de procesos reconocibles
1	Inicial/ad hoc	Los procesos son ad hoc y el enfoque general para la gestión es desorganizado
2	Repetible pero intuitivo	Los procesos siguen un patrón regular en el que procedimientos similares son seguidos por diferentes personas sin capacitación formal o procedimientos estándar. La responsabilidad está a cargo del individuo y los errores son altamente probables.
3	Definido	Los procesos están documentados y comunicados. Los procedimientos están estandarizados, documentados y comunicados a través de capacitaciones. Los procesos son obligatorios, sin embargo, es poco probable que se detecten desviaciones. Los procedimientos en sí mismos no son sofisticados, sino que son de formalización de las practicas existentes.
4	Gestionado y medible	La gerencia monitorea y mide el cumplimiento de los procedimientos y toma medidas cuando corresponde. Los procesos están en constante mejora y proporcionan buenas practicas. La automatización y las herramientas se utilizan de forma limitada y fragmentada.
5	Optimizado	Las buenas practicas se siguen y automatizan. Los procesos se han refinado a un nivel de buena práctica, basado en los resultados de la mejora continua y el modelado de madurez con otras empresas. IT se utiliza de forma integrada para automatizar el flujo de trabajo, proporcionando herramientas que mejoren la calidad y la eficacia, haciendo que la entidad se adapte rápidamente.

Para asegurar, que las medidas implementadas, controles, actividades y procedimientos estén perfectos, este documento y los relacionados Apéndices (2019-Global-Minimum-Standards-Appendix-INFSec-V3 ESP, 2019-Global-Minimum-Standards-Appendix-BCM-V3 ESP y 2019-Global-Minimum-Standards-Appendix-NMS-V3 ESP) serán revisados al menos una vez al año.

2 Gestión de seguridad de la información

La gestión de la seguridad de la información es un proceso continuo para proteger la información de una amplia gama de amenazas con el fin de respaldar las capacidades y valores de Aldeas Infantiles SOS, para evitar / reducir / minimizar los riesgos de seguridad que podrían resultar en pérdidas comerciales inaceptables y cumplir con los requisitos locales y/o internaciones, legales y contractuales que afectan a Aldeas Infantiles SOS.

La gestión de seguridad de la información se basa en la gestión de riesgos porque el costo de la seguridad total es prohibitivo y probablemente inalcanzable. Los riesgos se gestionan reduciendo su probabilidad y/o mitigando sus posibles consecuencias.

Enlaces y referencias

http://en.wikipedia.org/wiki/Information_security

https://www.bsigroup.com/en-GB/iso-27001-information-security/

2.1 Requisitos bajo el Reglamento general de protección de datos RGPD

Aldeas Infantiles SOS está procesando información confidencial del negocio[7] y varios tipos de información personal de donantes, beneficiarios y empleados, por lo que existe una gran demanda para mantener estos activos seguros. En relación a la información personal, la reforma a la norma de protección de datos de la UE (Reglamento General de protección de Datos, RGPD), en particular a los artículos 25, 32, 33 y 34 imponen obligaciones exigibles a las Aldeas Infantiles SOS para garantizar un nivel adecuado de seguridad de datos.

2.1.1 Art. 25 Protección de datos por diseño y por defecto

(1) Teniendo en cuenta la tecnología de punta, el costo de implementación y la naturaleza, alcance, contexto y propósitos del procesamiento, así como riesgos de diversa probabilidad y severidad de los derechos y libertades de las personas físicas que el procesamiento implica, el controlador deberá , tanto al tiempo de determinar los medios para el procesamiento como en el momento del procesamiento en sí, implementar medidas técnicas y organizativas apropiadas, como la seudonimización, que están diseñadas para implementar principios de protección de datos, como la minimización de datos, de manera efectiva y para integrar las salvaguardas necesarias en el procesamiento a fin de cumplir con los requisitos de este reglamento y proteger los derechos de los titulares de los datos.

(2) El controlador implementará medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se procesen datos personales que son necesarios para cada propósito específico del procesamiento.

Esa obligación aplica a la cantidad de datos personales recopilas, el alcance de su procesamiento, el periodo de su almacenamiento y su accesibilidad. En partículas, tales medidas garantizarán que, por defecto, los datos personales no sean accesibles, sin la intervención del individuo, a un número indefinido de personas físicas.

(3) Se puede usar un mecanismo de certificación aprobado, de conformidad con el Artículo 42, para demostrar cumplimiento de los requisitos establecidos en los párrafos 1 y 2 de este Artículo.

2.1.2 Art. 32 Seguridad del procesamiento

(1) Teniendo en cuenta la tecnología de punta, el costo de implementación y la naturaleza, alcance, contexto y los propósitos del procesamiento, así como riesgos de diversa probabilidad y severidad de los derechos y libertades de las personas físicas, el controlador y el procesador deberán implementar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad apropiado para el riesgo, incluyendo entre otros y según proceda:

(a) la seudonimización y el cifrado de datos personales;

[7] Información personal' significa toda información relacionada con una persona física identificada o identificable ('titular de los datos'); una persona física identificable es aquella que puede ser identificada, directa o indirectamente, en particular por referencia a un identificador como un nombre, un número de identificación, información de ubicación, un identificador en línea o por uno o más factores específicos a la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona física.

(b) la capacidad de garantizar confidencialidad, integridad, disponibilidad y resistencia continua de los sistemas y servicios de procesamiento;

(c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico y técnico;

(d) un proceso para probar, determinar y evaluar periódicamente la efectividad de las medidas técnicas y organizativas para garantizar la seguridad del procesamiento.

(2) Al determinar el nivel apropiado de seguridad se tendrá en cuenta, en particular, los riesgos que se presentan al procesar, especialmente de la destrucción accidental o ilegal, pérdida, alteración, divulgación no autorizada o acceso a datos personales transmitidos, almacenados o procesados de otra forma.

(3) Adhesión a un código de conducta aprobado como se menciona en el Artículo 40, o se puede usar un mecanismo de certificación aprobado como se menciona en el Artículo 42 como un elemento mediante el cual demostrar cumplimiento de los requisitos establecidos en el párrafo 1 de este Articulo.

(4) El controlador y el procesador deberán tomar medidas para garantizar que cualquier persona física que actúe bajo la autoridad del controlador o procesador, que tenga acceso a datos personales, no los procese excepto por instrucciones del controlador, a menos que se le exija hacerlo por ley de la Unión o del Estado.

2.1.3 Art. 33 Notificación de violación de información personal a la autoridad supervisora

(1) En el caso de violación de información personal el controlador deberá, sin demora injustificada y cuando sea factible, notificar la violación de información personal a la autoridad de supervisión competente de conformidad con el Artículo 55, a más tardar 72 horas después de haber tenido conocimiento del hecho, salvo que sea poco probable que la violación de datos personales resulte en un riesgo para los derechos y libertades de personas físicas. Cuando la notificación a la autoridad supervisora no se hizo dentro de las 72 horas, deberá ir acompañada de las razones para la demora.

(2) El procesador notificará al controlador, sin demora injustificada, luego de tener conocimiento de una violación de información personal.

(3) La notificación a la que se refiere el párrafo 1 deberá al menos:

(a) describir la naturaleza de la violación de información personal incluyendo, cuando sea posible, las categorías y el número aproximado de interesados involucrados, y las categorías y número aproximado de registros de datos personales involucrados;

(b) comunicar el nombre y los datos de contacto del oficial de protección de datos u otro punto de contacto donde se pueda obtener más información;

(c) describir las probables consecuencias de la violación de información personal;

(d) describir las medidas tomadas o propuestas por el controlador para tratar la violación de información personal incluyendo, cuando corresponda, medidas para mitigar sus posibles efectos adversos.

(4) Cuando, y en la medida en que no sea posible proporcionar la información al mismo tiempo, la información puede proporcionarse en fases sin demora injustificada.

(5) El controlador documentará toda violación de información personal, incluyendo los hechos relacionados con la violación de información personal, sus efectos y las medidas correctivas adoptadas. 2 Esa documentación permitirá a la autoridad supervisora verificar el cumplimiento de este Artículo.

2.1.4 Art. 34 Comunicación de una violación de información personal al titular de los datos

(1) Cuando la violación de información personal pueda resultar en un alto riesgo para los derechos y libertades de personas físicas, el controlador deberá comunicar la violación de información personal al titular de los datos sin demora injustificada.

(2) La comunicación al titular de los datos a que se refiere el párrafo 1 de este Artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de información personal y contendrá al menos la información y las medidas mencionadas en los puntos (b), (c) y (d) del Artículo 33(3).

(3) La comunicación al titular de los datos a que se refiere el párrafo 1 no será necesaria si se cumpliera alguna de las siguientes condiciones:

(a) el controlador ha implementado medidas de protección técnicas y organizativas apropiadas, y esas medidas fueron aplicadas a los datos personales afectados por la violación de información personal, en particular aquellos que hacen que los datos personales sean ininteligibles para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

(b) el controlador ha adoptado medidas posteriores que aseguran que ya no es probable que se materialice el alto riesgo para los derechos y libertades de los titulares de los datos mencionados en el párrafo 1.

(c) Implicaría un esfuerzo desproporcionado. En tal caso, se hará un comunicado público o una medida similar mediante la cual los titulares de los datos sean informados de forma igualmente efectiva.

(4) Si el controlador aún no ha comunicado la violación de información personal al titular de los datos, la autoridad de supervisión, habiendo considerado la probabilidad de que la violación de información personal resulte en un alto riesgo, puede requerir que lo haga o puede decidir que alguna de las condiciones mencionadas en el párrafo 3 se cumple.

2.2 Enfoque para la resiliencia al riesgo en curso

Para administrar varios escenarios de riesgos Aldeas Infantiles SOS Internacional se centra desde hace años en tecnología bien alineada, procedimientos organizativos bien pensados y personal bien informado que cumple con sus obligaciones de seguridad (competencias digitales, ej.: habilidades en materia de seguridad cibernética, identificación de datos personales identificables, seguridad en línea mientras se viaja, creación de una identidad en línea positiva, etc. que cubra el programa de líderes sénior, recaudación de fondos, RRHH, finanzas, TI, etc., en toda la organización).

Sin embargo, Aldeas Infantiles SOS Internacional ha reconocido que la gestión de riesgos tradicional simplemente no es ágil.

Para superar además las nuevas amenazas y riesgos, para cumplir con GDPR y otras normas y requisitos internacionales, Aldeas Infantiles SOS Internacional se centra en un enfoque holístico para la gestión moderna de la seguridad de la información, que se construye sobre una base de preparación para crear resiliencia al riesgo mediante la evaluación de vectores de riesgo desde una posición de aceptabilidad empresarial y perfiles de riesgo que cubren todos los activos, estructuras y procesos de la organización, incluida también la cobertura de toda la cadena de valores (terceros como proveedores de servicios en la nube, socios externos que procesan datos con la organización, etc.).

El objetivo es concentrar actividades en los escenarios de riesgo cibernético más probables y amenazadores, logrando un equilibrio entre resiliencia efectiva y operaciones eficientes – en continua cooperación internacional con los miembros del grupo de trabajo de Protección de Datos y Seguridad de la Información de Nethope, por ejemplo, Plan International, Save the Children, Catholic Relief Services, Trocaire, WaterAid y muchos más.

2.3 Controles CIS

Los Controles CIS ™ son un conjunto de acciones priorizadas que colectivamente forman un conjunto de mejores prácticas de defensa en profundidad que mitigan los ataques más comunes contra sistemas y redes y ayudan a las organizaciones a cumplir con la (Regulación General de Protección de Datos GDPR), en particular con:

- Articulo 25 Protección de datos por diseño y por defecto,
- Articulo 32 Seguridad del procesamiento,
- Articulo 33 Notificación de una violación de datos personales a la autoridad supervisora y
- Articulo 34 Comunicación de la violación de datos personales al titulas de los datos

Los controles CIS son desarrollados por una comunidad de expertos en TI que aplican su experiencia de primera mano cómo defensores cibernéticos para crear estas mejores prácticas de seguridad aceptadas a nivel mundial. Los expertos que desarrollan los controles CIS vienen de una amplia gama de sectores incluyendo comercio minorista, fabricación, atención médica, educación, gobierno, defensa y otros.

El Centro de Seguridad de Internet, (CIS) es una organización sin fines de lucro cuya misión es identificar, desarrollar, validar, promover y mantener las mejores prácticas en seguridad cibernética; brindar soluciones de seguridad cibernética de clase mundial para prevenir y responder rápidamente a incidentes cibernéticos; y construir y liderar comunidades para hacer posible un ambiente de confianza en el ciberespacio.

Enlaces y referencias

https://www.cisecurity.org/controls/

2.3.1 Control CIS 1: Inventario y control de activos de hardware

Administrar activamente (inventariar, dar seguimiento y corregir) todos los dispositivos de hardware en la red para que solo los dispositivos autorizados tengan acceso y que los dispositivos no autorizados y no administrados sean encontrados y se les impida el acceso.

2.3.1.1 ¿Por qué este control CIS es esencial?

Los atacantes, que pueden ubicarse en cualquier parte del mundo, continuamente escanean las direcciones de las organizaciones objetivo, esperando que sistemas nuevos y posiblemente desprotegidos se conecten a la red. Están particularmente interesados en dispositivos que entran y salen de la red de la empresa, como computadoras portátiles o en la modalidad 'traiga su propio dispositivo (BYOD)' que podrían no estar sincronizados con las actualizaciones de seguridad o ya estar comprometidos. Los ataques pueden aprovecharse de hardware nuevo instalado en la red una noche pero que no está configurado y parcheado con las actualizaciones de seguridad apropiadas sino hasta el día siguiente. Incluso los dispositivos que no son visibles desde Internet pueden ser utilizados por atacantes que ya han obtenido acceso interno y están buscando puntos pivote internos o víctimas. Los sistemas adicionales que se conectan a la red de la empresa (por ejemplo, sistemas de demostración, sistemas de prueba temporales, redes invitadas) también deben administrarse con cuidado y/o aislarse para evitar que el acceso de adversarios afecte la seguridad de las operaciones de la empresa.

Es comprensible que a empresas grandes y complejas les cueste el desafío de administrar entornos complejos y de rápido cambio. Sin embargo, los atacantes han demostrado capacidad, paciencia y voluntad de "inventar y controlar" nuestros activos a gran escala para respaldar sus oportunidades.

El control administrado de todos los dispositivos también juega un papel fundamental en la planificación y ejecución de la copia de seguridad del sistema, la respuesta a incidentes y la recuperación.

2.3.2 Control CIS 2: Inventario y control de activos de software

Administrar activamente (inventariar, dar seguimiento y corregir) todo el software en la red para que solo se instale y ejecute software autorizado, y todo el software no autorizado y no administrado sea encontrado y se impida su instalación y ejecución.

2.3.2.1 ¿Por qué este control CIS es esencial?

Los atacantes continuamente escanean las organizaciones objetivo buscando versiones vulnerables de software que puedan ser explotadas remotamente. Algunos atacantes también distribuyen páginas web hostiles, archivos de documentos, archivos multimedia, y otro contenido a través de sus propias páginas web o sitios confiables de terceros. Cuando las víctimas desprevenidas acceden a este contenido a través de un navegador vulnerable u otro programa del cliente, los atacantes comprometen sus máquinas, a menudo instalando programas de puerta trasera y bots que le dan al atacante control del sistema a largo plazo. Algunos atacantes sofisticados podrían utilizar exploits día cero, que aprovechan las vulnerabilidades desconocidas anteriormente para las cuales el vendedor de software aún no ha lanzado ningún parche. Sin el conocimiento adecuado o control del software implementado en una organización, los defensores no pueden proteger adecuadamente sus activos.

Es más probable que las máquinas mal controladas ejecuten software innecesario para fines comerciales (presentando posibles fallas de seguridad) o que ejecuten malware introducido por un atacante una vez que un sistema sea comprometido. Una vez que se ha explotado una sola máquina, los atacantes la utilizan a menudo como punto de parada para recopilar información confidencial del sistema comprometido y de otros sistemas conectados a éste. Además, las máquinas comprometidas se utilizan como punto de partida para moverse por toda la red y redes asociadas. De esta manera, los atacantes pueden rápidamente convertir una máquina comprometida en muchas. Las organizaciones que no tienen inventarios completos de software no pueden encontrar sistemas que ejecuten software vulnerable o malicioso para mitigar problemas o eliminar a los atacantes.

El control administrado de todo el software también juega un papel esencial en la planificación y ejecución de la copia de seguridad del sistema, la respuesta a incidentes y la recuperación.

2.3.3 CIS Control 3: Gestión continua de vulnerabilidades

Adquirir, evaluar y tomar medidas de forma continua sobre información nueva para identificar vulnerabilidades, remediar y minimizar la ventana de oportunidad para los atacantes.

2.3.3.1 ¿Por qué este control CIS es esencial?

Los ciberdefensores deben operar en un flujo constante de información nueva: actualizaciones de software, parches, consejos de seguridad, boletines sobre amenazas, etc. La comprensión y gestión de vulnerabilidades se ha convertido en una actividad continua, que requiere mucho tiempo, atención y recursos.

Los atacantes tienen acceso a la misma información y pueden aprovechar las brechas entre el surgimiento de conocimiento nuevo y la remediación. Por ejemplo, cuando los investigadores informan nuevas vulnerabilidades

Las organizaciones que no escanean en busca de vulnerabilidades y tratan las fallas descubiertas de forma proactiva enfrentan una significativa probabilidad de comprometer sus sistemas informáticos. Los defensores enfrentan desafíos particulares para escalar la remediación en toda una empresa y priorizar acciones con prioridades en conflicto y, a veces con efectos secundarios inciertos.

2.3.4 Control CIS 4: Uso controlado de privilegios de administración

Los procesos y herramientas utilizados para rastrear / controlar / prevenir / corregir el uso, asignación y configuración de privilegios administrativos en computadoras, redes y aplicaciones.

2.3.4.1 ¿Por qué este control CIS es esencial?

El mal uso de los privilegios administrativos es un método primario para que los atacantes se propaguen dentro de una empresa objetivo. Dos técnicas muy comunes de ataque se aprovechan de privilegios administrativos sin control. En la primera, un usuario de la estación de trabajo que se ejecuta como usuario privilegiado se deja engañar para abrir un archivo adjunto de correo electrónico malicioso, descargar y abrir un archivo de un sitio web malicioso, o simplemente navegar en un sitio web que aloja contenido del atacante que puede explotar automáticamente los navegadores. El archivo o exploit contiene códigos ejecutables que ejecutan en la máquina de la víctima de forma automática o engañando al usuario para que ejecute el contenido del atacante. Si la cuenta del usuario víctima tiene privilegios administrativos, el atacante puede dominar la máquina de la víctima por completo e instalar registradores de pulsaciones de teclas, rastreadores y software de control remoto para encontrar contraseñas administrativas y otra información confidencial. Ataques similares ocurren con el correo electrónico. Un administrador por descuido abre un correo electrónico que contiene un archivo adjunto infectado que se usa para obtener un punto pivote dentro de la red que se utiliza para atacar otros sistemas.

La segunda técnica común utilizada por los atacantes es la elevación de privilegios al adivinar o descifrar una contraseña para que un usuario administrativo obtenga acceso a una máquina objetivo. Si los privilegios administrativos se distribuyen de manera flexible y amplia, o son idénticos a las contraseñas utilizadas en sistemas menos esenciales, el atacante tiene mucha más facilidad para ganar control total de los sistemas porque hay muchas más cuentas que pueden actuar como vías para que el atacante comprometa los privilegios administrativos.

2.3.5 Control CIS 5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores

Establecer, implementar y administrar activamente (rastrear informar, corregir) la configuración de seguridad de dispositivos móviles, computadoras portátiles, servidores y estaciones de trabajo utilizando una administración y proceso de control de cambios rigurosos para evitar que los atacantes exploten servicios y configuraciones vulnerables.

2.3.5.1 ¿Por qué este control CIS es esencial?

Las configuraciones predeterminadas para los sistemas operativos y aplicaciones, tal como las ofrecen los fabricantes y vendedores, normalmente están orientadas a la facilidad de implementación y de uso, no a la seguridad. Los controles básicos, servicios y puertos abiertos, cuentas y contraseñas predeterminadas, protocolos más antiguos (vulnerables, y la preinstalación de software innecesario pueden ser explotables en su estado predeterminado.

El desarrollo de ajustes de configuración con buenas propiedades de seguridad es una tarea compleja, más allá de la capacidad de los usuarios individuales, que requiere el análisis de potencialmente cientos o miles de opciones para tomar buenas decisiones (la selección de Procedimientos y Herramientas a continuación proporciona recursos para configuraciones seguras). Incluso si se desarrolla e instala una configuración inicial sólida, ésta debe ser administrada continuamente para evitar el “decaimiento” de la seguridad a medida que el software se actualiza o parchea, llega información sobre nuevas vulnerabilidades de seguridad y las configuraciones se “retocan” para permitir la instalación de software nuevo o para ser compatible con nuevos requerimientos operativos. De lo contrario, los atacantes encontrarán oportunidades para explotar los servicios accesibles a la red y el software del cliente.

2.3.6 Control CIS 6: Mantenimiento, monitoreo y análisis de registros de auditoría

Recopilar, administrar y analizar registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.

2.3.6.1 ¿Por qué este control CIS es esencial?

Las deficiencias en el registro y análisis de seguridad permiten a los atacantes ocultar su ubicación, software malicioso y actividades en las máquinas víctima. Incluso si las víctimas saben que sus sistemas han sido comprometidos, sin archivos de registro protegidos y completos tienen total desconocimiento de los detalles del ataque y las acciones posteriores ejecutadas por los atacantes. Sin registros de auditoría sólidos, un ataque puede pasar desapercibido indefinidamente y los daños particulares causados pueden ser irreversibles.

A veces los archivos de registro son la única evidencia de un ataque exitoso. Muchas organizaciones mantienen registros de auditoría solo por cumplir, pero los atacantes confían en el hecho de que dichas organizaciones rara vez observan sus registros de auditoría, y no saben que sus sistemas han sido comprometidos. Debido a procesos de análisis de registros deficientes o inexistentes, los atacantes a veces controlan las máquinas víctima durante meses o años in que nadie de la organización objetivo lo sepa, a pesar de que la evidencia del ataque se ha registrado en archivos de registro no examinados.

2.3.7 Control CIS 7: Protección para correo electrónico y navegadores web

Minimizar la superficie del ataque y las oportunidades para que los atacantes manipulen el comportamiento a través de su interacción con navegadores web y sistemas de correo electrónico.

2.3.7.1 ¿Por qué este control CIS es esencial?

Navegadores web y clientes de correo electrónico son puntos de entrada y ataque muy comunes debido a su complejidad técnica, flexibilidad e interacción directa con los usuarios y otros sistemas y sitios web. Se puede diseñar contenido para atraer o engañar usuarios para que tomen medidas que aumenten considerablemente el riesgo y permitan la introducción de código malicioso, pérdida de datos valiosos y otros ataques. Dado que estas aplicaciones son el medio principal por el que los usuarios interactúan con entornos no confiable, estos son objetivos potenciales tanto para la explotación de código como para la ingeniería social.

2.3.8 Control CIS 8: Protección contra malware

Controlar la instalación, difusión y ejecución de código malicioso en múltiples puntos de la organización, al tiempo que optimiza el uso de la automatización para permitir la actualización rápida de la defensa, recopilación de datos y acciones correctivas.

2.3.8.1 ¿Por qué este control CIS es esencial?

El software malicioso es un aspecto integral y peligroso de las amenazas de Internet, ya que está diseñado para atacar sistemas, dispositivos y datos. Se mueve rápidamente, cambia rápidamente y entra a través de muchos puntos como dispositivos para usuario final, archivos adjuntos de correo electrónico, páginas web, servicios en la nube, acciones del usuario y medios extraíbles. El malware moderno está diseñado para evitar defensas y atacarlas o deshabilitarlas.

Las defensas de malware deben poder operar en este entorno dinámico a través de la automatización a gran escala, la actualización rápida y la integración con procesos como la respuesta a incidentes. También debe implementarse en múltiples posibles puntos de ataque para detectar, detener el movimiento o controlar la ejecución de software malicioso. Los paquetes de seguridad de punto final empresarial proporcionan características administrativas para verificar que todas las defensas estén activas y actualizadas en cada sistema administrado.

2.3.9 Control CIS 9: Limitación y control de puertos, protocolos y servicios de red

Administrar (rastrear / controlar / corregir) el uso operativo continuo de puertos, protocolos y servicios en dispositivos en red para minimizar ventanas de vulnerabilidad disponibles para los atacantes.

2.3.9.1 ¿Por qué este control CIS es esencial?

Los atacantes buscan servicios de red accesibles de forma remota que sean vulnerables a la explotación. Ejemplos comunes incluyen servidores web, servidores de correo, servicios de archivos e impresión mal configurados y servidores DNS instalados de manera predeterminada en diferentes tipos de dispositivos, a menudo sin necesidad comercial para dicho servicio. Muchos paquetes de software instalan servicios automáticamente y los activan como parte de la instalación del paquete del software principal sin informar al usuario o administrador de que los servicios han sido habilitados. Los atacantes escanean dichos servicios e intentan explotarlos, a menudo intentando explotar identificaciones de usuario y contraseñas predeterminadas o códigos de explotación ampliamente disponibles.

2.3.10 Control CIS 10: Capacidad de recuperación de datos

Los procesos y herramientas utilizados para realizar una adecuada copia de seguridad de la información esencial con una metodología probada para su recuperación oportuna.

2.3.10.1 ¿Por qué este control CIS es esencial?

Cuando los atacantes comprometen máquinas a menudo hacen cambios significativos en configuraciones y software. A veces, los atacantes también hacen sutiles alteraciones de los datos almacenados en máquinas comprometidas, lo que puede poner en peligro la eficacia de la organización con información contaminada. Cuando se descubre atacantes puede ser extremadamente difícil, para organizaciones sin capacidad confiable de recuperación de datos, eliminar todos los aspectos de la presencia del atacante en la máquina.

2.3.11 Control CIS 11: Configuración segura para dispositivos en red como cortafuegos, enrutadores y conmutadores

Establecer, implementar y administrar activamente (rastrear, informar, corregir) la configuración de seguridad de los dispositivos de infraestructura de red utilizando una gestión de configuración y proceso de control de cambios rigurosos para evitar que los atacantes exploten servicios y configuraciones vulnerables.

2.3.11.1 ¿Por qué este control CIS es esencial?

Las configuraciones predeterminadas para los sistemas operativos y aplicaciones, tal como las ofrecen los fabricantes y vendedores, normalmente están orientadas a la facilidad de implementación y de uso, no a la seguridad. Servicios y puertos abiertos, cuentas predeterminadas (incluidas las cuentas de servicio) o contraseñas, soporte para protocolos antiguos (vulnerables), preinstalación de software innecesario; todos pueden sr explotables en su estado predeterminado. La gestión de configuraciones seguras para dispositivos de red no es un evento único, sino un proceso que implica reevaluar regularmente no solo los elementos de configuración sino también los flujos de tráfico permitidos. Los atacantes se aprovechan de dispositivos de red con configuraciones que se vuelven menos seguras con el tiempo ya que los usuarios exigen excepciones por necesidades empresariales específicas. A veces, las excepciones se implementan y luego se dejan sin hacer cuando ya no son aplicables a las necesidades de la empresa. En algunos casos, el riesgo de seguridad de la excepción no se analiza ni mide adecuadamente en base a la necesidad empresarial asociada y puede cambiar con el tiempo.

Los atacantes buscan configuraciones predeterminadas vulnerables, huecos o inconsistencias en los grupos de reglas de firewall, enrutadores y conmutadores, y usan esos huecos para penetrar las defensas. Explotan fallas en estos dispositivos para obtener acceso a las redes, redirigir el tráfico de una red e interceptar información durante una transmisión. A través de tales acciones el atacante obtiene acceso a datos confidenciales, altera información importante o incluso utiliza una máquina comprometida para hacerse pasar por otros sistemas confiables en la red.

2.3.12 Control CIS 12: Protección de fronteras *(de redes)*

Detectar / evitar / corregir el flujo de información que se transfiere a través de redes de diferentes niveles de confianza con enfoque en datos que dañan la seguridad.

2.3.12.1 ¿Por qué este control CIS es esencial?

Los atacantes de centran en explotar sistemas a los que pueden llegar a través de Internet, incluidos no solo sistemas DMZ, sino también estaciones de trabajo y computadoras portátiles que extraen contenido de Internet a través de las fronteras de la red. Amenazas como grupos de crimen organizado y estados nacionales utilizan la configuración y debilidades arquitectónicas que se encuentran en los sistemas perimetrales, dispositivos de red y máquinas de clientes que acceden a Internet para obtener acceso inicial a una organización. Luego, con una base de operaciones en estas máquinas, los atacantes a menudo giran para penetrar más profundamente dentro de la frontera para robar o cambiar información o para establecer una presencia persistente para ataques posteriores contra computadoras centrales internas. Adicionalmente, se producen muchos ataques entre redes de socios comerciales, a veces denominados extranets, a medida que los atacantes saltan de la red de una organización a otra, explotando sistemas vulnerables en perímetros de extranet.

Para controlar el flujo de tráfico a través de las fronteras de la red y el contenido policial buscando ataques y evidencia de máquinas comprometidas, las defensas de las fronteras deben ser de varias capas, fiándose de firewalls, servidores proxy, redes perimetrales DMZ e IPS e IDS basados en la red. También es fundamental filtrar el tráfico entrante y saliente.

Cabe señalar que las líneas fronterizas entre redes internas y externas están decreciendo como resultado de una mayor interconectividad dentro y entre las organizaciones, así como el rápido aumento en el despliegue de tecnologías inalámbricas. Estas líneas borrosas a veces permiten a los atacantes obtener acceso dentro de las redes pasando por alto sistemas perimetrales. Sin embargo, incluso con este desenfoque de perímetros, la implantación de seguridad efectiva todavía depende de defensas perimetrales cuidadosamente configuradas que separan las redes con diferentes niveles de amenaza, grupos de usuarios, datos y niveles de control. Y a pesar de la difuminación de redes internas y externas, tener defensas efectivas con varias capas de las redes perimetrales ayuda a reducir la cantidad de ataques exitosos, permitiendo que el personal de seguridad se concentre en los atacantes que han ideado métodos para eludir las restricciones de las fronteras.

2.3.13 Control CIS 13: Protección de datos

Procesos y herramientas usados para evitar la exfiltración de datos, mitigar los efectos de datos exfiltrados y garantizar la privacidad e integridad de la información confidencial.

Tener en cuenta que, aunque las actividades relacionadas con RGPD son coordinadas por la unidad de Integridad, Cumplimiento y Legal, la responsabilidad del cumplimiento con RGPD y otras leyes y normas locales relacionadas con la protección de datos siempre recae en los Controladores (de acuerdo con las autoridades de protección de datos), que son las AM.

2.3.13.1 ¿Por qué este control CIS es esencial?

Los datos residen en muchos lugares. Se logra una mejor protección de esos datos mediante la aplicación de una combinación de cifrado, protección de integridad y técnicas de prevención de pérdida de datos. A medida que las organizaciones continúan moviéndose hacia la computación en la nube y el acceso móvil, es importante tener el cuidado adecuado para limitar e informar sobre la filtración de datos y al mismo tiempo mitigar los efectos de datos comprometidos.

Algunas organizaciones no identifican y separan cuidadosamente sus activos más delicados e importantes de la información menos delicada y de acceso público en sus redes internas. En muchos entornos, los usuarios internos tienen acceso a todos o la mayoría de los activos fundamentales. Los activos delicados también pueden incluir sistemas que proporcionan gestión y control de sistemas físicos, tales como Control Supervisor y Adquisición de Datos (SCADA). Una vez que los atacantes han penetrado dicha red pueden fácilmente encontrar y filtrar información importante, causar daño físico o interrumpir las operaciones con poca resistencia. Por ejemplo, en varias violaciones de gran repercusión mediática en los últimos años, los atacantes pudieron obtener acceso a información confidencial almacenada en los mismos servidores con el mismo nivel de acceso que datos mucho menos importantes. También hay ejemplos del uso del acceso a la red corporativa para obtener acceso y luego controlar los activos físicos y causar daño.

2.3.14 Control CIS 14: Acceso controlado basado en la necesidad de conocimiento

Los procesos y herramientas utilizados para rastrear / controlar / evitar / corregir el acceso seguro a activos esenciales (por ejemplo, información, recursos, sistemas) de acuerdo con la determinación formal de qué personas, computadoras y aplicaciones tienen la necesidad y el derecho de acceder a estos activos esenciales con base en una clasificación aprobada.

2.3.14.1 ¿Por qué este control CIS es esencial?

El cifrado de datos proporciona tal nivel de seguridad que incluso si los datos se ven comprometidos no es práctico acceder al texto plano sin recursos considerables; sin embargo y, en primer lugar, también debe establecerse controles para mitigar la amenaza de exfiltración de datos. Muchos ataques ocurrieron dentro de la red, mientras que otros involucraron el robo físico de computadoras portátiles y otros equipos que contenían información confidencial. Con todo, en muchos casos, las víctimas no se dieron cuenta que información confidencial salió de sus sistemas porque no estaban monitoreando el flujo de salida de datos.
El movimiento de datos a través de las fronteras de la red, tanto electrónica como físicamente debe ser cuidadosamente examinado para minimizar su exposición a los atacantes.

La pérdida de control sobre datos confidenciales o protegidos por parte de las organizaciones es una grave amenaza para las operaciones comerciales y una amenaza potencial para la seguridad nacional. Si bien algunos datos se filtran o pierden como resultado de robo o espionaje, la gran mayoría de estos problemas se deben a prácticas da datos poco entendidas, la falta de una arquitectura de políticas efectiva y errores de usuarios. La pérdida de información incluso puede ocurrir como resultado de actividades legítimas como e-Discovery durante un litigio, particularmente cuando las prácticas de retención de registros son ineficaces o inexistentes.

La adopción del cifrado de datos, tanto en tránsito como en reposo, proporciona mitigación contra la puesta en peligro de datos. Esto es cierto si se ha tenido el debido cuidado en los procesos y tecnologías asociados con las operaciones de cifrado. Un ejemplo de esto es la gestión de claves criptográficas utilizadas por los diversos algoritmos que protegen los datos. El proceso para la generación, uso y destrucción de claves debe basarse en procesos probados según lo definen estándares como. NIST SP 800-57.

También se debe tener cuidado para garantizar que los productos utilizados dentro de una empresa implementen algoritmos criptográficos bien conocidos y examinados, según lo identifica NIST. También se recomienda reevaluar los algoritmos y claves utilizados en la empresa de forma anual para garantizar que las organizaciones no se queden atrás en la intensidad de protección aplicada a sus datos.

Para las organizaciones que están transfiriendo datos a la nube, es importante comprender los controles de seguridad aplicados a los datos en el entorno multi inquilino de la nube y determinar el mejor curso de acción para la aplicación de los controles de cifrado y la seguridad de las claves. De ser posible, las claves deben almacenarse en contenedores seguros como los Módulos de Seguridad de Hardware (HSM).

La prevención de pérdida de datos (DLP) se refiere a un enfoque integral que abarca personas, procesos y sistemas que identifican, monitorean y protegen los datos en uso (por ejemplo, acciones de punto final), datos en movimiento (por ejemplo, acciones de red) y datos en reposo (por ejemplo, almacenamiento de datos) a través de la inspección de contenido profundo y con un marco de gestión centralizado. En los últimos años ha habido una notable transición en la atención y la inversión, de proteger la red a proteger los sistemas dentro de la red y proteger los datos en sí. Los controles DLP se basan en políticas e incluyen la clasificación de datos confidenciales, el descubrimiento de esos datos en una empresa, la aplicación de controles y la generación de informes y auditorías para garantizar el cumplimiento de las políticas.

2.3.15 Control CIS 15: Control del acceso inalámbrico

Los procesos y herramientas utilizados para rastrear / controlar / evitar / corregir el uso seguro de redes de área local inalámbricas (WLAN), puntos de acceso y sistemas de clientes inalámbricos.

2.3.15.1 ¿Por qué este control CIS es esencial?

Grandes robos de datos han sido iniciados por atacantes que han obtenido acceso inalámbrico a organizaciones desde fuera del edificio físico, eludiendo los perímetros de seguridad de las organizaciones mediante la conexión inalámbrica a puntos de acceso dentro de la organización. Los clientes inalámbricos que acompañan a los viajeros regularmente se infectan a través de la explotación remota mientras se encuentran en redes inalámbricas públicas en aeropuertos y cafeterías. Dichos sistemas explotados se utilizan como puertas traseras cuando se vuelven a conectar a la red de una organización objetivo. Otras organizaciones han reportado sobre el descubrimiento de puntos inalámbricos de acceso no autorizado en sus redes, plantados y a veces ocultos para obtener acceso sin restricciones a una red interna. Debido a que no requieren conexión física directa, los dispositivos inalámbricos son un vector conveniente para que los atacantes conserven acceso a largo plazo dentro de un entorno objetivo.

2.3.16 Control CIS 16: Monitoreo y control de cuentas

Administrar activamente el ciclo de vida de las cuentas de sistemas y aplicaciones (su creación, uso, latencia, eliminación) para minimizar las oportunidades que los atacantes puedan tener para aprovechar.

2.3.16.1 ¿Por qué este control CIS es esencial?

Los atacantes con frecuencia descubren y explotan cuentas de usuario legítimas pero inactivas para hacerse pasar por usuarios legítimos dificultando a los observadores del personal de seguridad el descubrimiento del comportamiento del atacante. A menudo se ha utilizado de esta manera incorrecta las cuentas de contratistas y empleados que han sido retirados y cuentas anteriormente configuradas para pruebas Equipo Rojo (pero que no se eliminaron después). Además, algunos infiltrados maliciosos o ex empleados han obtenido acceso a las cuentas que quedaron en un sistema mucho después de la expiración del contrato, manteniendo su acceso al sistema informático de una organización y a datos confidenciales para fines no autorizados y a veces maliciosos.

2.3.17 Control CIS 17: Implementar un programa de concientización y capacitación sobre seguridad

Para todos los roles funcionales en la organización (priorizando aquellos cuya misión es fundamental para la empresa y su seguridad), identifique las habilidades, capacidades y conocimientos específicos necesarios para apoyar la defensa de la organización; desarrolle y ejecute un plan integral para evaluar, identificar brechas y remediar a través de políticas, planificación organizativa, capacitación y programas de concientización.

2.3.17.1 ¿Por qué este control CIS es esencial?

Es tentador pensar en la defensa cibernética como un desafío técnico, principalmente, pero las acciones de las personas también juegan un papel en el éxito o fracaso de una empresa. Las personas cumplen funciones importantes en cada etapa del diseño, implementación, operación, uso y supervisión del sistema. Entre los ejemplos cabe mencionar: desarrolladores y programadores de sistemas (que pueden no comprender la oportunidad de resolver vulnerabilidades de causa raíz al principio del ciclo de vida del sistema); profesionales de operaciones de TI (que pueden no reconocer las implicaciones de seguridad de los artefactos y registros de TI); usuarios finales (que pueden ser susceptibles a conspiraciones de ingeniería social como el phishing); analistas de seguridad (que se esfuerzan por cuantificar el papel que la ciberseguridad desempeña en el riesgo general operativo/de misión, y no tienen una forma razonable de tomar decisiones de inversión relevantes).

Los atacantes son muy conscientes de estos problemas y los utilizan para planear sus explotaciones, por ejemplo: elaborando cuidadosamente mensajes de phishing que se ven como tráfico rutinario y esperado para un usuario incauto; explotando las brechas o costuras entre política y tecnología (por ejemplo, políticas que no tienen aplicación técnica); trabajando dentro de la ventana de tiempo de revisión de parches o registros; usando sistemas nominalmente no críticos para la seguridad como puntos de salto o bots.

Ningún enfoque de ciberdefensa puede tratar eficazmente el riesgo cibernético sin un medio para abordar esta vulnerabilidad fundamental. Por el contrario, empoderar a las personas con buenos hábitos de defensa cibernética puede aumentar significativamente la preparación.

2.3.18 Control CIS 18: Seguridad de software de aplicación

Administrar el ciclo de vida de seguridad de todo el software desarrollado y adquirido internamente para prevenir, detectar y corregir las debilidades de seguridad.

2.3.18.1 ¿Por qué este control CIS es esencial?

A menudo los ataques aprovechan las vulnerabilidades encontradas en el software basado en la web y otras aplicaciones. Las vulnerabilidades pueden estar presentes por muchas razones, incluyendo errores de codificación, errores lógicos, requisitos incompletos y fallas en la prueba de condiciones inusuales o inesperadas. Los ejemplos de errores específicos incluyen: falta de verificación del tamaño de las aportaciones de los usuarios; incapacidad de filtrar secuencias innecesarias de caracteres de los flujos de entrada, pero potencialmente maliciosas; incapacidad de inicializar y borrar variables; y una administración deficiente de la memoria, lo que permite que fallas en una parte del software afecten partes no relacionadas (y más fundamentales para la seguridad).

Hay una avalancha de información pública y privada sobre tales vulnerabilidades que están disponibles para atacantes y defensores por igual, así como un mercado sólido de herramientas y técnicas para permitir la “armamentización” de vulnerabilidades y convertirlas en exploits. En un ataque más de 1 millón de servidores web fueron explotados y convertidos en motores de infección para los visitantes de esos sitios mediante inyección SQL. Durante ese ataque, se utilizó sitios web confiables de gobiernos estatales y otras organizaciones comprometidas por atacantes para infectar cientos de miles de navegadores que accedieron a esos sitios web. Muchas más vulnerabilidades de aplicaciones web y no web son descubiertas regularmente.

2.3.19 Control CIS 19: Respuesta y gestión de incidentes

Proteger la información de la organización al igual que su reptación mediante el desarrollo e implementación de una infraestructura de respuesta a incidentes (por ejemplo, planes, roles definidos, capacitación, comunicaciones, supervisión administrativa) para descubrir un ataque rápidamente y luego contener el daño de manera efectiva, erradicando la presencia del atacante y restaurando la integridad de la red y los sistemas.

Tener en cuenta que a pesar de que las actividades relacionadas con el RGDP son coordinadas por la unidad Legal, de Integridad y Cumplimiento, la responsabilidad del cumplimiento del RGDP y otras leyes y normas locales relacionadas con la protección de datos siempre recae en los Controladores (de acuerdo con las autoridades de protección de datos), quienes son los AM.

2.3.19.1 ¿Por qué este control CIS es esencial?

Los incidentes cibernéticos ahora son parte de nuestra forma de vida. Incluso las empresas grandes, bien financiadas y técnicamente sofisticadas, luchan por seguirle el ritmo a la frecuencia y complejidad de los ataques. La cuestión de un ciberataque exitoso contra una empresa no es “si” sino “cuándo.”

Cuando ocurre un incidente, es demasiado tarde para desarrollar los procedimientos, informes, recopilación de datos, responsabilidad de gestión, protocolos legales y estrategias de comunicación adecuados que permitirán a la empresa comprender, gestionar y recuperarse exitosamente. Sin un

plan de respuesta a incidentes, en primer lugar, una organización puede no descubrir un ataque, o, si el ataque es detectado, la organización puede no seguir buenos procedimientos para contener el daño, erradicar la presencia del atacante y recuperarse de manera segura. Por lo tanto, el atacante puede tener un impacto mucho mayor, causando más daño, infectando más sistemas, y potencialmente extrayendo más información confidencial de lo que sería posible si hubiera un plan efectivo de respuesta a incidentes.

2.3.20 Control CIS 20: Pruebas de penetración y ejercicios equipo rojo

Poner a prueba la fortaleza general de la defensa de una organización (tecnología, procesos y personas) mediante la simulación de objetivos y acciones de un atacante.

2.3.20.1 ¿Por qué este control CIS es esencial?

Los atacantes a menudo explotan la brecha entre buenos diseños e intenciones defensivas y la implementación o mantenimiento. Algunos ejemplos incluyen: la ventana de tiempo entre el anuncio de una vulnerabilidad, la disponibilidad de un parche del proveedor y la instalación real en cada máquina. Otros ejemplos incluyen: políticas bien intencionadas que no tienen un mecanismo de aplicación (especialmente aquellas destinadas a restringir acciones humanas riesgosas); incapacidad de aplicar buenas configuraciones a las máquinas que entran y salen de la red; y la incapacidad de entender la interacción entre múltiples herramientas de defensa, o con operaciones normales del sistema que tienen implicaciones de seguridad.

Una postura defensiva exitosa requiere un programa integral de políticas y gobierno efectivas, defensas técnicas sólidas y acciones apropiadas por parte de las personas. En un entorno complejo en el que la tecnología está en constante evolución y regularmente aparecen nuevas técnicas de espionaje de los atacantes, las organizaciones deben probar periódicamente sus defensas para identificar vacíos y evaluar su nivel de preparación realizando pruebas de penetración.

Las pruebas de penetración comienzan con la identificación y evaluación de vulnerabilidades que pueden identificarse en la empresa. A continuación, las pruebas son diseñadas y ejecutadas para demostrar específicamente cómo un adversario puede subvertir los objetivos de seguridad de la organización (por ejemplo, la protección de determinada propiedad Intelectual) o alcanzar objetivos adversos específicos (por ejemplo, el establecimiento de una infraestructura secreta de Comando y Control). Los resultados proporcionan una visión más profunda, a través de la demostración, de los riesgos comerciales de varias vulnerabilidades.

Los ejercicios Equipo Rojo adoptan un enfoque integral en el espectro completo de políticas, procesos y defensas de la organización para mejorar la preparación organizativa, mejorar la capacitación de profesionales en defensa e inspeccionar los actuales niveles de desempeño. Los Equipos Rojos pueden proporcionar información valiosa y objetiva sobre la existencia de vulnerabilidades y la eficacia de las defensas y controles de mitigación ya existentes, e incluso de aquellos planificados para su futura implementación.

3 Gestión de continuidad del negocio

La Gestión de continuidad del negocio (GCN) es un proceso de gestión continuo que identifica los impactos potenciales que amenazan el servicio fundamental de negocios de una organización y proporciona un marco para el desarrollo de resiliencia y capacidad de respuesta efectiva que salvaguarde los intereses de sus partes interesadas clave, reputación, marca y valor creando actividades.

En términos de GCN, servicios de negocios fundamentales se refiere a activos y valores que deben permanecer disponibles en cualquier situación para asegurar la operación del negocio a un nivel aceptable.

Para tener éxito es necesario conocer exactamente la respectiva cadena de servicio. Esto significa estar en cada sistema particular involucrado haciendo que el servicio de negocios respectivo esté disponible.

A medida que el panorama empresarial cambia, también lo hace la naturaleza de las potenciales interrupciones. En particular, la subcontratación y las estrategias que traen cada vez más servicios locales a la nube (O365, SalesForce, D365, etc.) están también creando interdependencias nuevas y complejas en partes externas.

Un adecuado enfoque estratégico para la continuidad del negocio, para gestionar sus riesgos y amenazas tiene respuestas para:

- ¿Qué amenazas tendrían el impacto más sustancial en nuestra misión y operaciones?
- ¿Cuáles tienen más probabilidad de ocurrir?

Estos factores cambian continuamente y requieren revisión constante. Lo que sea que se haya planificado poner en marcha debe ser trabajado cuidadosamente, atentamente y a fondo.

Enlaces y referencias:

http://en.wikipedia.org/wiki/Business_continuity_management *https://www.bsigroup.com/en-GB/iso-22301-business-continuity/*

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Notfallmanagement/English_BCM_Study.pdf?__blob=publicationFile&v=3

3.1 Conceptos básicos a primera vista – mitigación de riesgos fundamentales

Los riesgos y amenazas básicas a la continuidad del negocio para las organizaciones son los desastres naturales como incendios, inundaciones, terremotos, incidentes criminales como hurto y robo o apagones. Esas cosas aún suceden y tienen que ver con la ubicación geográfica, incluso en tiempos de subcontratación y computación en la nube.

Por lo tanto, se debe planificar una estrategia bien definida y medidas adecuadas para manejar eventos así.

3.1.1 Control 1 de la GCN: Obtener y conservar un seguro

A menudo, los daños graves resultan de desastres naturales como terremotos, inundaciones, tormentas o actos deliberados como robo, vandalismo, etc. para protegerse de estas amenazas una medida posible es un seguro adecuado.

3.1.2 Control 2 de la GCN: códigos de construcción locales

Un código de construcción, o control de construcción, es un conjunto de reglas que especifican el nivel mínimo aceptable de seguridad para objetos construidos, como edificios y estructuras que no son construcciones. El objetivo principal de los códigos de construcción es proteger la salud pública, la seguridad y el bienestar general en lo que respecta a la construcción y ocupación de edificios y estructuras. Como ejemplo, el colocado inadecuado de cables podría limitar el índice de resistencia al fuego de un edificio.

Además, un cableado adecuado es clave, ejemplo, conectar cables, la conexión de circuitos, conexión de dispositivos y conexión de paneles eléctricos requiere un cableado adecuado.

3.1.3 Control 3 de la GCN: Centro de datos (CD) adecuado para dispositivos y componentes fundamentales de negocios

Un centro de datos (CD) es un lugar físico que alberga todos los componentes y dispositivos fundamentales que se ejecutan. Un CD debe situarse en un lugar seguro y bloqueado a personal no autorizado.

La siguiente consideración importante es el aire acondicionado en el CD. Un CD provisto de un sistema de aire acondicionado diseñado adecuadamente garantiza la temperatura y humedad adecuadas. Además, controlar automáticamente la temperatura y establecer un sistema de alarmas si se superan los umbrales definidos es clave.

Para detectar humo o fuego en la fase inicial es necesario instalar y mantener sistemas adecuados de detección de humo/fuego. Idealmente tener también disponible un extintor de CO2 para eliminar o controlar incendios pequeños en la etapa inicial.

Además, la entrada de agua es fundamental para la fiabilidad del sistema de TI. Medidas simples como la instalación de un drenaje de agua podrían ser buenas medidas preventivas y ayudar a superar situaciones críticas.

3.1.4 Control 4 de la GCN: sistemas UPS para componentes y dispositivos comerciales esenciales

Una fuente de alimentación ininterrumpida (UPS) es un dispositivo hardware que proporciona una fuente de alimentación de reserva en caso de un corte de energía (apagón), bajada o subida de tensión. Una UPS proporciona suficiente energía para que las máquinas se apaguen correctamente o permanezcan encendidas durante un corte de energía temporal o un apagón.

3.2 Gestión de riesgos

La gestión de riesgos es un proceso continuo de evaluación de los riesgos para el negocio como parte de un enfoque basado en el riesgo utilizado para determinar la seguridad adecuada para un sistema mediante el análisis de las amenazas y vulnerabilidades y la selección de medidas apropiadas y económicas para lograr y mantener un nivel aceptable de riesgo.

3.2.1 Control 5 de la GCN: Documentación actualizada para componentes y dispositivos empresariales esenciales

Para superar situaciones críticas de manera exitosa es importante tener documentación adecuada y actualizada de los servicios fundamentales del negocio. Esto garantiza que al terminar el día el personal que maneja crisis tendrá toda la información que necesita para lidiar con el incidente.

3.2.2 Control 6 de la GCN: Clasificación de servicios de TI y componentes y dispositivos esenciales relacionados con la empresa

La clave es considerar únicamente componentes y dispositivos esenciales para el negocio en lugar de darle mayor importancia a cualquier servicio.

Esto requiere una descripción actualizada de todos los componentes y dispositivos esenciales del negocio incluida la dependencia, tiempo total de recuperación ante desastres, ejemplo: clasificar como crítica / importante / no crítica. Especialmente en la era de la subcontratación y la computación en la nube, la infraestructura local de redes e Internet (Conectividad e Infraestructura) como factor de influencia subyacente y esencial en lo que respecta a la disponibilidad y rendimiento esenciales del negocio va ganando cada vez más importancia y debe clasificarse adecuadamente.

3.2.3 Control 7 de la GCN: Plan de emergencia para componentes y dispositivos esenciales de la empresa

Uno de los requisitos más esenciales para una Gestión de Continuidad del Negocio es garantizar planes de emergencia actualizados que cubran todas las medidas técnicas y organizativas para recuperar con éxito los servicios comerciales dañados. Esos planes deben ser probados y evaluados en términos de precisión por lo menos una vez al año.

3.2.4 Control 8 de la GCN: Proceso de copia de seguridad para recuperación ante desastres para dispositivos y componentes empresariales esenciales

Es necesario que todos los componentes y dispositivos empresariales esenciales sean capturados en una copia de seguridad adecuadamente configurada para su recuperación. También es necesario verificar a intervalos regulares que el procedimiento de copia de seguridad realmente funcione y que todos los sistemas relevantes pueden restaurarse con éxito.

La copia de seguridad debe conservarse en un lugar seguro, si es posible fuera de la empresa u oficinas. El lugar de almacenamiento debe también protegerse adecuadamente contra daño causado por los elementos, ejemplo: fuego, agua y similares.

3.2.5 Control 9 de la GCN: Pruebas de emergencia y recuperación para componentes y dispositivos empresariales esenciales

No puede considerarse confiable la planificación adecuada para situaciones de emergencia hasta que se ensaye y pruebe ser funcional. Un objetivo importante de un ensayo debe ser hacer que las personas se sientan más cómodas en sus roles y crear conciencia antes de verse sujetos al estrés por una emergencia.

3.3 Identificar y evitar un punto único de falla (SPOF)

La tecnología, incluso la de vanguardia, es vulnerable a puntos únicos de falla, en general una situación en la que la falla de un dispositivo o componente derribaría el servicio de las TIC en su conjunto. Como ejemplo, un solo enrutador de Internet que conecta la oficina a servicios en la nube como O365, SalesForce o D365.

Para protegerse de un SPOF es importante asegurarse que los componentes y dispositivos de tecnología esencial sean redundantes o puedan recuperarse dentro de un marco de tiempo aceptable.

El concepto de puntos únicos de falla también se aplica a la disponibilidad humana, en particular con la subcontratación y la dependencia de riesgos relacionados.

3.3.1 Control 10 de la GCN: Fuentes de alimentación redundantes para componentes y dispositivos empresariales esenciales

Un dispositivo con un sistema de fuente de alimentación redundante contiene en su interior dos (o más) fuentes de alimentación. Cada fuente de alimentación es capaz de alimentar todo el dispositivo y solo funciona una a la vez. Si una falla, la otra fuente de alimentación comienza a funcionar para mantener el dispositivo encendido.

3.3.2 Control 11 de la GCN: RAID para componentes y dispositivos empresariales esenciales

RAID (matriz redundante de discos independientes; originalmente matriz redundante de discos económicos) es una forma de almacenar los mismos datos en diferentes lugares en múltiples discos duros para proteger los datos en caso de una falla del disco. El uso de múltiples discos aumenta el tiempo medio entre fallas (MTBF). RAID funciona colocando datos en múltiples discos y permitiendo que las operaciones de entrada / salida (E/S) se superpongan de manera equilibrada, mejorando además el rendimiento.

3.3.3 Control 12 de la GCN: Sistemas de emergencia para componentes y dispositivos empresariales esenciales

Los sistemas de emergencia son componentes o dispositivos redundantes o duplicados/reproducidos que ayudan a evitar la no disponibilidad. Por ejemplo, un componente o dispositivo pre configurado podría mantener el tiempo de recuperación en caso de un incidente en un nivel aceptable.

3.3.4 Control 13 de la GCN: Tecnología de punta para componentes y dispositivos empresariales esenciales

La operación del servicio comercial fundamental con equipos de gran calidad y tecnología de punta garantiza una alta disponibilidad y en general un mejor soporte.

3.4 Medidas contractuales

3.4.1 Control 14 de la GCN: Cuenta de Internet empresarial

El uso de cuentas de Internet empresariales (por ejemplo, tasas de subida y bajada dedicadas, baja latencia / tiempo de respuesta dedicado, dirección IP estática, etc.) combinado con un acuerdo de nivel de servicio (ANS) adecuado, en lugar de los servicios ofrecidos por un proveedor de servicio de Internet pequeño, prepara el escenario para obtener resultados predecibles en materia de rendimiento del servicio de TIC y alta disponibilidad del servicio de Internet.

3.4.2 Control 15de la GCN: ANS y soporte profesional para sistemas empresariales esenciales

Un acuerdo de nivel de servicio (ANS) es parte de un contrato de servicio donde un servicio es formalmente definido. Un ANS también tendrá una definición técnica en términos de tiempo medio entre fallas (MTBF), tiempo medio de reparación o tiempo medio de recuperación (MTTR); varias velocidades de datos; rendimiento, fluctuación, o detalles medibles similares.

Para garantizar una alta disponibilidad del servicio es importante contar con soporte profesional para los servicios empresariales esenciales disponibles en lugar de soporte pequeño/barato de un solo técnico.

4 Gestión de redes

La gestión de redes es un factor esencial en la operación exitosa de una red. A medida que una empresa se vuelve cada vez más dependiente de los servicios en red, mantener esos servicios en funcionamiento es sinónimo de mantener el negocio en funcionamiento, en particular en tiempos de operación externa y computación en la nube.

Para proporcionar garantías sobre la capacidad de servicios de TIC esenciales para la empresa y para obtener resultados predecibles en materia de rendimiento del servicio de TIC, es necesario tener soluciones disponibles que puedan detectar y responder automáticamente a las amenazas y problemas de rendimiento en tiempo real, así como predecir posibles problemas en el futuro.

Enlaces y referencias

http://en.wikipedia.org/wiki/Network_management

http://en.wikipedia.org/wiki/Quality_of_service

4.1 Ancho de banda y gestión de servicios

4.1.1 Control 1 del SGR: Priorización de servicios empresariales esenciales

Sin control de ancho de banda una descarga iniciada por un solo cliente podría hacer que los servicios empresariales esenciales de TIC no estén disponibles para los demás clientes en la ubicación respectiva.

Sin embargo, antes de abalanzarse sobre soluciones técnicas es necesario tener una visión general de qué servicios de TIC necesitan valores preferidos (por ejemplo, Collaboration, Skype para Negocios, SalesForce, D365, etc.), qué servicios de TIC todavía funcionan bien a pesar del ancho de banda pequeño (por ejemplo, FTP subida/descarga, etc.) y qué servicios de TIC deberían retrasarse o bloquearse (por ejemplo, intercambio de archivos de punto a punto para uso privado).

4.1.1.1 Garantía del servicio

Una garantía asigna un ancho de banda mínimo a las conexiones que coinciden con una regla bastante independiente de otro tráfico que pasa por esta puerta de acceso.

4.1.1.2 Límite del servicio

Un límite especifica el ancho de banda máximo que se asigna a una conexión. Un límite define un punto más allá del cual las conexiones bajo una regla no tienen ancho de banda asignada, incluso si se dispone de ancho de banda no utilizada.

4.1.1.3 Ponderación del servicio

La asignación de ancho de banda de acuerdo con ponderaciones garantiza la plena utilización de la línea, incluso si una clase específica no está utilizando todo su ancho de banda. En tal caso, el ancho de banda restante se divide entre las clases restantes de acuerdo con sus ponderaciones relativas.

4.1.2 Control 2 del SGR: Monitoreo de Protocolo simple de administración de red (SNMP)

El monitoreo SNMP es la forma más fácil de medir la carga de tráfico en los enlaces de red, ejemplo, enrutadores y conmutadores. Permite ver la carga de tráfico en los enlaces de red a lo largo del tiempo en forma gráfica y permite configurar para la generación automática de mensajes de advertencia si, por ejemplo, se utiliza el 80% del ancho de banda durante más de 2 minutos.

Enlaces y referencias

http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol *http://www.paessler.com/*

4.1.3 Control 3 del SGR: NetFlow

NetFlow permite descubrir qué computadoras centrales, conversaciones y protocolos están consumiendo la mayor cantidad de ancho de banda y cuál es la composición del tráfico en cada enlace de red.

Los componentes y dispositivos de red que admiten NetFlow pueden recopilar estadísticas de tráfico IP en todas las interfaces donde NetFlow está habilitado y luego exportar esas estadísticas como registros de NetFlow, hacia al menos un recopilador NetFlow que hace el análisis de tráfico real.

Enlaces y referencias

http://en.wikipedia.org/wiki/NetFlow *http://www.paessler.com/* *http://www.splintered.net/sw/flow-tools/*

4.1.4 Control 3 del SGR: RT monitoreo y rastreo de paquetes

Para tener posibilidades de monitoreo en tiempo real (exploración interactiva del tráfico de datos en enlaces de red), es necesario usar un analizador de protocolos de red que permita la lectura y análisis de datos en vivo de una amplia gama de protocolos de red.

Enlaces y referencias

http://en.wikipedia.org/wiki/Packet_analyzer *http://www.wireshark.org/*

4.1.5 Control 5 del SGR: gestión y monitoreo de servicios

El propósito de la gestión de servicios / monitoreo de servicios es observar servicios basados en TCP como HTTP, SMTP o FTP, por ejemplo, para verificar automáticamente el espacio libre en disco, la carga de CPU o el uso de memoria en sistemas locales remotos, así como observar errores de TCP/IP o paquetes descartados en enlaces de red.

En caso de falla o un corte el sistema de monitoreo de red alerta automáticamente, en general por correo electrónico.

Enlaces y referencias

http://en.wikipedia.org/wiki/Network_monitoring *http://www.paessler.com/*
http://mathias-kettner.com/check_mk.html

4.1.6 Control 6 del SGR: monitoreo y redacción de informes centralizados

El monitoreo y la redacción de informes administrados de forma centralizada simplifica el redimensionamiento de la conectividad en términos de disponibilidad, gestión de capacidad y planificación.

Por supuesto, esto requiere el uso de un conjunto homogéneo de herramientas en materia de gestión del tráfico y esto, por otro lado, requiere la misma infraestructura en cada ubicación.