Diseño de planes de securización (Bastionado de redes y sistemas)

Análisis de riesgos

Estudio de los bienes, sus vulnerabilidades y las probabilidades de materialización de amenazas, con el propósito de determinar la exposición anual al riesgo de cada bien ante cada amenaza.

Puede ser cuantitativo, cuando esta exposición se expresa en unidades monetarias, o cualitativo, cuando se expresa en una escala relativa de gravedad, por ejemplo del 1 al 10. Dada la dificultad que entraña el cálculo preciso de las probabilidades citadas, se suele elegir esta último.

Fases del análisis de riesgos:

1. Identificación y valoración de activos
2. Identificación y valoración de las amenazas
3. Identificación de las medidas de seguridad existentes
4. Identificación y valoración de vulnerabilidades
5. Identificación de restricciones y objetivos de seguridad
6. Determinar medidas del riesgo
7. Determinar el impacto
8. Identificación y seleccionar las medidas de protección

Principios de la Economía Circular en la Industria 4.0

Los 10 principios de la Economía Circular:

1. El residuo se convierte en recurso. Todo el material

biodegradable vuelve a la naturaleza y el no biodegradable se reutiliza.
2. Reintroducir en el circuito económico aquellos productos que ya no corresponden a las necesidades iniciales de los consumidores.
3. Reutilizar ciertos residuos o partes de ellos que todavía pueden funcionar para elaborar nuevos productos.
4. Reparar y encontrar una segunda vida para los productos estropeados o defectuosos.
5. Reciclar los materiales que se encuentran en los residuos.
6. Aprovechar energéticamente los residuos que no se pueden reciclar.
7. Eliminar la venta de ciertos productos para implantar un sistema de alquiler de bienes. Cuando el producto cumple su función principal, vuelve a la empresa y esta lo desmonta para reutilizar las piezas que pueden ser utilizadas nuevamente.
8. Eliminar los combustibles fósiles para producir el producto, reutilizar y reciclar.
9. Considerar los impactos medioambientales a lo largo del ciclo de vida de un producto y los integra desde su concepción.
10. Establecer un método de organización industrial en un mismo territorio caracterizado por una gestión optimizada de los stocks y de los flujos de materiales, energía y servicios.

Por la naturaleza de los sistemas industriales, un fallo de seguridad en ellos puede poner en peligro el proceso de calidad del producto, la continuidad de negocio o la seguridad de los trabajadores, por tanto, es esencial disponer de las herramientas necesarias para garantizar el control de los entornos operacionales. Es necesaria una estrategia de ciberseguridad Industria 4.0.

Con la llegada de la Industria 4.0. y la conectividad del

mundo IoT, los sistemas de control industrial ya no sólo se verán afectados por típicas averías o errores de operación en la gestión industrial, sino que, además se sumará el factor de la ciberseguridad que hasta ahora, era un desconocido en el mundo Industrial.

Algunas de las tecnologías de la Industria 4.0 al servicio de la economía circular son:

- El Internet de las cosas y el análisis de los datos: los productos que se conectan a Internet permiten a los fabricantes controlar y analizar su rendimiento a distancia y recabar la información de uso, lo que permite implantar diferentes modelos de negocios circulares.
- Robótica: Los avances en la robótica permite a los fabricantes emplear robots en una cantidad de aplicaciones cada vez mayor, incrementando el rendimiento y reduciendo los desechos, así como también prolongando la vida útil de los productos.
- Impresión 3D: El uso de la impresión 3D para la producción bajo demanda de repuestos mejora la rentabilidad y prolonga el ciclo de vida de los productos y equipos.

Plan de medidas técnicas de seguridad

Algunos planes de medidas:

- Teletrabajo seguro.
- Borrado seguro y gestión de soportes.
- Uso de dispositivos móviles.
- Antimalware.
- Auditoría de sistemas.
- Comercio electrónico.
- Control de acceso.

- Copias de seguridad.
- Gestión de logs.
- Protección de las páginas web.
- Respuesta a incidentes.
- Uso de criptografía.
- Actualización de software.

Políticas de securización más habituales

Las políticas de securización tratan los aspectos y elementos esenciales donde debemos aplicar seguridad y que deben estar bajo control. Cada política tiene una lista de chequeo de las acciones que debe tomar el empresario, su equipo técnico y sus empleados.

Guías de buenas prácticas para la securización de sistemas y redes

En primer lugar hay que analizar su estado de seguridad y definir a dónde quiere llegar. Esto se plasmará en una serie de políticas y normativas que van a dirigir la forma de abordar la seguridad en el día a día (textos sacados de INCIBE).

Como resultado de lo anterior, pondrán en marcha, si aún no lo han hecho, o mejorarán su sistema de control de accesos lógicos, pues al igual que controlamos quién entra en nuestras instalaciones, debemos controlar quién entra en nuestros sistemas.

Cualquier reflexión que se haga sobre seguridad llevará a la conclusión de las copias de seguridad son la forma de recuperarse de casi cualquier incidente. No deben faltar en cualquier pyme que quiera sobrevivir a un incidente.

Básico y esencial es también la protección antimalware pues los virus mutan para hacerse cada vez más dañinos y peligrosos. Ninguna pyme está exenta de este riesgo.

Y no habrá protección eficaz si utilizamos sistemas o aplicaciones obsoletas y desactualizadas pues son más vulnerables. Por ello actualizar todo el software es fundamental.

Nuestra red ha de estar protegida para evitar todo tipo de intrusiones en nuestros sistemas. Y como el acceso desde el exterior de clientes y colaboradores se hace imprescindible en un medio comercial electrónico no descuidaremos la seguridad de la información cuando es comunicada hacia y desde el exterior.

No menos importante es proteger la información almacenada en todo momento pues los soportes pueden extraviarse o deteriorarse. Controlar los soportes de la información durante toda su vida útil es también una medida de seguridad elemental.

Vigilar nunca está de más y para ello pondremos los medios para llevar un registro de actividad dónde podamos observar cómo interaccionan los usuarios con los sistemas y detectar anomalías en su comportamiento.

Por último pero no menos importante es dar los pasos necesarios para garantizar la Continuidad de negocio pues es todos, incluso las pymes, podemos sufrir un incidente de seguridad.

Más información

- https://www.jesusninoc.com/03/18/clears-resource-records-cache-dns-server/

Estándares de securización de sistemas y redes

Los estándares de seguridad son técnicas generalmente establecidas en materiales publicados que intentan proteger el entorno cibernético de un usuario u organización. Este entorno incluye a los propios usuarios, redes, dispositivos, todo el software, procesos, información en almacenamiento o tránsito, aplicaciones, servicios y sistemas que pueden conectarse directa o indirectamente a las redes.

El objetivo principal es para reducir los riesgos, incluyendo prevención o atenuación de cyber-ataques. Estos materiales publicados consisten en colecciones de herramientas, políticas seguridad, conceptos de seguridad, salvaguardas de seguridad, guías, enfoques de gestión de riesgos, acciones, capacitación, mejores, prácticas, aseguramiento y tecnologías.

Estándares:

- ISO/IEC 27001 y 27002
- NERC
- NIST
- ISO 15408

Caracterización de procedimientos, instrucciones y recomendaciones

Hay que crear protocolos de actuación y dar instrucciones desde el punto de vista de la seguridad, además de aportar recomendaciones a los protocolos de actuación.

Niveles, escalados y protocolos de atención a incidencias

Es frecuente que existan múltiples incidencias a la vez, por lo que es necesario determinar un nivel de prioridad para la resolución de las mismas. Dependiendo de la prioridad, se asignarán los recursos necesarios para la resolución de la incidencia.

Si no se puede resolver en primera instancia un incidente y para ello se tiene que recurrir a un especialista o a algún superior que pueda tomar decisiones que se escapan de su responsabilidad. Este proceso se denomina escalado.

Hay dos tipos de escalado:

- Escalado funcional: Se requiere el apoyo de un especialista para resolver la incidencia.
- Escalado jerárquico: Se acude a un responsable de mayor autoridad para tomar decisiones que se escapan de las atribuciones asignadas a ese nivel, como, por ejemplo, asignar más recursos para la resolución de un incidente específico.