

Definición de necesidades en términos de seguridad informática

Etapa de definición

La etapa de definición de las necesidades de seguridad es el primer paso hacia la implementación de una política de seguridad.

El objetivo es determinar las necesidades de organización mediante la redacción de un inventario del sistema de información y luego estudiar los diferentes riesgos y las distintas amenazas que representan para implementar una política de seguridad apropiada.

La etapa de definición se compone entonces de tres etapas:

- Identificación de las necesidades
- Análisis de los riesgos
- Definición de la política de seguridad

Identificación de las necesidades

La etapa de identificación de las necesidades consiste en realizar en primer lugar un inventario del sistema de información, en particular de la siguiente información:

- Personas y funciones
- Materiales, servidores y los servicios que éstos brindan
- Esquematización de la red (esquema de direcciones, topologías físicas y lógicas, etc.)
- Lista de los nombres de dominio de la empresa.
- Infraestructura de la comunicación (routers, conmutadores, etc.)
- Información delicada

Análisis de los riesgos

La etapa de análisis de riesgos consiste en relevar los diferentes riesgos que se advierten, estimar sus probabilidades y, por último, estudiar su impacto.

La mejor forma de analizar el impacto de una amenaza consiste en calcular el costo de los daños que causaría (por ejemplo, un ataque a un servidor o un daño de los datos de vital importancia de la compañía).

Partiendo de esta base, sería interesante confeccionar una tabla de riesgos y de sus potencialidades (es decir, la probabilidad de que existan) dándoles niveles escalonados de acuerdo con una escala que debe definirse. Por ejemplo:

- Infundado (o improbable): la amenaza es insostenible
- Débil: la amenaza tiene pocas probabilidades de existir
- Moderada: la amenaza es real
- Alta: la amenaza tiene muchas probabilidades de existir

Cómo definir la política de seguridad

La política de seguridad es el documento de referencia que define los objetivos de seguridad y las medidas que deben implementarse para tener la certeza de alcanzar estos objetivos.

La política de seguridad define un número de reglas, procedimientos y prácticas óptimas que aseguren un nivel de seguridad que esté a la altura de las necesidades de la organización.

Este documento se debe presentar como un proyecto que incluya a todos, desde los usuarios hasta el rango más alto de la jerarquía, para ser aceptado por todos. Una vez redactada la política de seguridad, se deben enviar a los empleados las cláusulas que los impliquen para que la política de seguridad tenga el mayor impacto posible.

Métodos

Existen muchos métodos para desarrollar una política de seguridad. A continuación, se mostrará una lista no exhaustiva de los métodos principales:

- **MARION** (*Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux* [metodología del análisis de riesgos informáticos por niveles]), desarrollado por CLUSIF. <https://www.clusif.asso.fr/fr/production/mehari/>
- **MEHARI** (*MEthode Harmonisée d'Analyse de Risques* [método armonizado de análisis de riesgos]) <https://www.clusif.asso.fr/fr/production/mehari/>
- **EBIOS** (*Expression des Besoins et Identification des Objectifs de Sécurité* [expresión de las necesidades e identificación de los objetivos de seguridad], desarrollado por la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) <http://www.ssi.gouv.fr/fr/confiance/ebios.html>
- **MAGERIT**: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas <http://www.coit.es/publicac/publbit/bit128/bitcd1/legisla/pg5m21.htm>
- **Estándar ISO 17799**: Denominada también como ISO 27002, es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la International Organization for Standardization y por la Comisión Electrotécnica Internacional en el año 2000, con el título de *Information technology - Security techniques - Code of practice for information security management*. El estándar ISO/IEC 17799 tiene su origen en el British Standard BS 7799-1 que fue publicado por primera vez en 1995. http://es.wikipedia.org/wiki/ISO/IEC_17799

Cómo implementar medidas de seguridad

Etapas de implementación

La etapa de implementación consiste en establecer los métodos y mecanismos diseñados para que el sistema de información sea seguro, y aplicar las reglas definidas en la política de seguridad.

Los principales mecanismos que se usan para asegurar una red contra intrusiones son los sistemas firewall. Sin embargo, este tipo de mecanismos no protege la confidencialidad de los datos que circulan en la red.

Por lo tanto, en la mayoría de los casos, es necesario usar algoritmos criptográficos, los cuales garantizan la confidencialidad del intercambio.

La configuración de una red virtual privada (VPN, por sus siglas en inglés) puede proporcionar seguridad adicional, ya que toda la información se halla codificada.

Auditorías de seguridad

El concepto de auditoría

Una auditoría de seguridad consiste en apoyarse en un tercero de confianza (generalmente una compañía que se especializa en la seguridad informática) para validar las medidas de protección que se llevan a cabo, sobre la base de la política de seguridad.

El objetivo de la auditoría es verificar que cada regla de la política de seguridad se aplique correctamente y que todas las medidas tomadas conformen un todo coherente.

Una auditoría de seguridad garantiza que el conjunto de disposiciones tomadas por la empresa se consideren seguras.

Prueba de intrusión

Las pruebas de intrusión (abreviado como pen tests [penetration tests, pruebas de penetración]) consisten en probar los métodos de protección del sistema de información sometiendo el sistema a una situación real.

Generalmente, se utilizan dos métodos:

- El **método de la caja negra**, el cual consiste en intentar penetrar en la red sin tener conocimientos del sistema para generar una situación realista
- El **método de la caja blanca** que consiste en intentar penetrar en el sistema conociéndolo por completo para poner a prueba al máximo los límites de seguridad de la red

Es necesario el consentimiento (preferentemente por escrito) del nivel más alto de la jerarquía antes de realizar estas pruebas, debido a que pueden causar daños y a que los métodos utilizados se consideran ilegales sin la autorización expresa del propietario del sistema.

Una prueba de intrusión representa una buena forma de aumentar la conciencia de las personas involucradas en el proyecto cuando éste muestra una falencia. Por otro lado, no garantiza la seguridad del sistema, ya que quienes realizan las pruebas pueden obviar vulnerabilidades. Las auditorías de seguridad constituyen un método más eficaz para garantizar un nivel de seguridad superior en el sistema, ya que en éstas se tiene en cuenta elementos organizacionales y humanos, y se analiza la seguridad en forma interna.

Cómo detectar incidentes de seguridad

Etapas de detección de incidentes

Para ser completamente fiable, un sistema de información seguro debe aplicar medidas que permitan detectar incidentes.

Por consiguiente, existen sistemas de detección de intrusiones (o IDS, por sus siglas en inglés) que controlan la red y pueden activar una alarma cuando una solicitud resulta sospechosa o no cumple con la política de seguridad.

El uso de estas sondas investigativas y los parámetros relativos a éstas deben estudiarse cuidadosamente, ya que este tipo de mecanismo puede generar muchas falsas alarmas.

Reacción ante incidentes de seguridad

Es fundamental identificar las necesidades de seguridad de una organización para establecer las medidas que permitirán a dicha organización evitar una situación catastrófica, como una intrusión, una falla en los equipos o incluso un daño por filtración de agua. No obstante, es imposible evitar por completo todo tipo de riesgos, por lo que todas las empresas deben estar preparadas para experimentar algún día una situación catastrófica.

En estas circunstancias, resulta fundamental una reacción rápida, ya que una máquina afectada hace peligrar el sistema de información de la compañía en su totalidad. Además, cuando el compromiso provoca el mal funcionamiento del servicio, una interrupción prolongada puede aparejar pérdidas económicas. Por último, en los casos en los que se ha alterado un sitio web (modificación de páginas) la reputación de la compañía está en juego.

Etapas de reacción

Generalmente, la etapa de reacción es la que menos se toma en cuenta en los proyectos de seguridad informática. Esta etapa consiste en prever eventos y planificar las medidas que deben tomarse si surge un problema.

En el caso de una intrusión, por ejemplo, el administrador de sistemas puede reaccionar de una de las siguientes maneras:

- Obtener la dirección del hacker y contraatacar
- Cortar el suministro eléctrico de la máquina
- Desconectar la máquina de la red
- Reinstalar el sistema

El problema es que cada una de estas acciones puede resultar más perjudicial (particularmente en términos de costos) que la intrusión en sí misma. En efecto, si el funcionamiento de la máquina comprometida es fundamental para el funcionamiento del sistema de información o si se trata de un sitio web de ventas online, una interrupción prolongada del servicio podría ser catastrófica.

A su vez, en este tipo de situaciones es importante establecer pruebas en caso de que se realice una investigación judicial. De lo contrario, si la máquina comprometida se ha usado para realizar otro ataque, la compañía corre el riesgo de ser considerada responsable.

La implementación de un plan de recuperación de desastres permite a la organización evitar que el desastre empeore y tener la certeza de que todas las medidas tomadas para establecer pruebas se aplicarán correctamente.

Asimismo, un plan contra desastres desarrollado correctamente define las responsabilidades de cada individuo y evita que se emitan órdenes y contraórdenes, que impliquen una pérdida de tiempo.

Restauración

En el plan de recuperación, se debe especificar en detalle cómo hacer que el sistema comprometido vuelva a funcionar correctamente. Es necesario tomar en cuenta los siguientes elementos:

- **Anotar la fecha de intrusión:** conocer la fecha aproximada en la que se ha comprometido la máquina permite a la organización evaluar el nivel de riesgo de intrusión para el resto de la red y el grado de compromiso de la máquina.
- **Restringir el compromiso:** tomar las medidas necesarias para que el compromiso no se expanda
- **Estrategia de seguridad:** si la compañía tiene una estrategia de seguridad, se recomienda comparar los cambios que se realizaron a los datos del sistema comprometido con los datos supuestamente fiables. Si los datos están infectados con un virus o un troyano, la restauración de éstos puede expandir aún más el daño.
- **Establecer pruebas:** por razones legales, es necesario guardar los archivos de registro diario del sistema corrompido para poder restituirlos en caso de una investigación judicial

Cómo configurar un sitio de reemplazo: en lugar de reinstalar el sistema comprometido, es preferible desarrollar y activar a tiempo un sitio de reemplazo que permita que el servicio continúe activo cuando sea necesario.

Práctica del plan contra desastres

De la misma forma en que los simulacros de incendio son fundamentales para repasar un plan de escape en caso de incendio, la práctica del plan contra desastres permite a una organización confirmar que el plan funciona y garantizar que todas las personas involucradas sepan qué hacer.