Evolución de la Seguridad Informática

La Seguridad Informática ha experimentado un profundo cambio en los últimos años. Inversiones aisladas llevadas a cabo con el objetivo de fortalecer la seguridad en puntos muy concretos han dado paso a inversiones para asegurar el bien más valioso de la empresa, la información, enfocando la seguridad hacia los procesos de negocio de la empresa.

Durante los años 80 y principios de los 90 la Seguridad Informática se centraba en proteger los equipos de los usuarios, es decir, proporcionar seguridad a los ordenadores y su sistema operativo. Esta seguridad lógica, entendida como la seguridad de los equipos informáticos para evitar que dejasen de funcionar correctamente, se centraba en la protección contra virus informáticos.

Con la aparición de Internet y su uso globalizado a nivel empresarial la Seguridad Informática comenzó a enfocarse hacia la conectividad de redes o networking, protegiendo los equipos servidores de aplicaciones informáticas, y los equipos servidores accesibles públicamente a través de Internet, y controlando la seguridad a nivel periférico a través de dispositivos como Firewalls. Es decir, la posibilidad tecnológica de "estar conectados" llevaba implícita la aparición de nuevas vulnerabilidades que podían ser explotadas, la exposición de información crucial para el negocio que podía ser accesible precisamente gracias a esa conectividad.

El perfil de atacante de un sistema informático ha cambiado radicalmente. Si bien antes los objetivos de un atacante o hacker podían ser más simples (acceder a un sitio donde nadie antes había conseguido llegar, o infectar un sistema mediante algún tipo de virus, pero sin

ningún tipo de ánimo de lucro), en la actualidad los atacantes se han percatado de lo importante que es la información y sobre todo de lo valiosa que puede ser. Se trata de grupos organizados que aprovechan las vulnerabilidades de los sistemas informáticos y las redes de telecomunicaciones para acceder a la información crítica y sensible de la empresa, bien a través de personal especializado en este tipo de ataques, o bien comprando en el mercado negro kits de explotación de vulnerabilidades para obtener información muy específica.

Ante esta nueva situación, las empresas se protegen con nuevas tecnologías:

- Sistemas IDS (*Intrusion Detection System)*. Sistemas de monitorización y detección de accesos no permitidos en una red.
- Sistemas IPS (*Intrusion Prevention System)*. Sistemas de prevención de intrusión. No solo monitoriza el tráfico para detectar vectores de ataque en una red, sino que el sistema es capaz de bloquearlos.
- Honey pot. Instalación de equipos aparentemente vulnerables que en realidad no contienen ninguna información sensible de la empresa sino que están diseñados para atraer y detectar a los atacantes, protegiendo los sistemas realmente críticos.
- SIEM (*Security Information en Event Management)*. Sistemas de correlación de eventos y generación de alertas, capaces de integrar diferentes dispositivos, lanzar acciones en función de las alertas, y almacenar los registros para un posterior análisis de los mismos.

Los nuevos vectores de ataque, el cambio en los perfiles de los atacantes, y sobre todo la importancia crucial de la información clave y crítica para el negocio de una empresa, hacen que el concepto de Seguridad Informática haya evolucionado hacia el concepto de Seguridad

de la Información, cuyo objetivo principal consiste en alinear las inversiones en seguridad con los objetivos generales de la empresa y sus estrategias de negocio. La Seguridad de la Información se basa en el diseño de Políticas de Seguridad integrada en los planes estratégicos de la empresa. Para la definición de dichas Políticas es necesario tener en cuenta diversos factores, tales como la localización de la empresa, tamaño y número de sedes, condicionantes geográficos, cumplimientos legales y normativas vigentes, normas ISO de la empresa, etc.

Es necesario para le empresa conocer en todo momento cuánto vale su activo más crítico y valioso, la información del negocio, y cuáles son las brechas de seguridad que podrían propiciar el acceso a la misma. Es necesario conocer el estado de la seguridad en todo momento a través de análisis de riesgos dinámicos que permitan identificar las principales amenazas y cuantificar los riesgos asociados a la materialización de las mismas, teniendo en cuenta varios factores clave: el valor de la información, la probabilidad de que una amenaza pudiera presentarse, y el impacto que tendría sobre el negocio la materialización de la misma.

Más que hablar de evolución de la seguridad, quizás se debería hablar de integración de la Seguridad Informática (medidas técnicas) en la Seguridad de la Información (medidas organizativas). La Seguridad de la Información es un concepto más global que persigue definir e integrar Políticas de Seguridad en los planes estratégicos. Se cuantifican los riesgos, se identifican aquellos más críticos para el negocio de forma continua, se plantean escenarios de crisis y se diseñan planes de continuidad de negocio y recuperación ante desastres. Toda esta información, junto con un buen diseño del organigrama de seguridad, una profunda integración de la seguridad en los planes estratégicos de la empresa, y una permanente

implicación de la gerencia y del personal directivo de la empresa, permitirán conocer dónde y cómo utilizar las medidas técnicas de Seguridad Informática (línea operativa) en el marco de la Seguridad de la Información y sus medidas organizativas (línea estratégica).

AUTOR: DAVID LÓPEZ

LINK

https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica

Lectura característica de la seguridad informática

Seguridad Informática. Es un estado de cualquier tipo de información (informático o no) que indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo.

Características

Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

Integridad: los activos o la información solo pueden ser modificados por las personas autorizadas y de la forma autorizada.
Confidencialidad: la información o los activos informáticos son accedidos solo por las personas autorizadas para hacerlo.
Disponibilidad: los activos informáticos son accedidos por las personas autorizadas en el momento requerido.

Irrefutabilidad (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Dependiendo de las fuentes de amenaza, la seguridad puede dividirse en tres partes: Seguridad física, Seguridad ambiental y Seguridad lógica.
En estos momentos la seguridad informática es un tema de dominio obligado por cualquier usuario de Internet, para no permitir que su información sea comprometida.

Términos relacionados con la seguridad informática

Activo: recurso del sistema de información o relacionado con este, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.
Amenaza: es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
Ataque: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
Control: es una acción, dispositivo o procedimiento que elimina o reduce una vulnerabilidad.
Impacto: medir la consecuencia al materializarse una amenaza.
Riesgo: Es la probabilidad de que suceda la amenaza o evento no deseado
Vulnerabilidad: Son aspectos que influyen negativamente en un activo y que posibilita la materialización de una amenaza.
Desastre o Contingencia: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.
Aunque a simple vista se puede entender que un Riesgo y una Vulnerabilidad se podrían englobar un mismo concepto, una definición más informal denota la diferencia entre riesgo y vulnerabilidad, de modo que la Vulnerabilidad está ligada a una Amenaza y el Riesgo a un

Impacto.

Se puede describir la relación entre vulnerabilidad, amenaza y control de la siguiente manera:

una amenaza puede ser bloqueada aplicando un control a una vulnerabilidad.