RIESGOS INFORMÁTICOS

AUTOR: JAVIER CHINCHILLA MORALES

NOVIEMBRE: 2020

San Marcos

Introducción

El análisis de riesgo informático es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, a fin de determinar los controles adecuados para acetar, disminuir, transcurrir o evitar la ocurrencia del riesgo.

Tabla de contenido

Los riesgos informáticos

Las pymes se pueden ver atacadas en el ámbito de las tecnologías de información por la presencia de un virus, o software malicioso (malware) y spam, asi como por las fallas inesperadas en el funcionamiento de los dispositivos, software o hardware, para prevenirse de éstos o enfrentarse a los mismos se tiene las siguientes recomendaciones:

1. Contar con un equipo especializado en seguridad informática, lo cual facilitará que las estrategias y planes de seguridad puedan aplicarse de modo correcto y con el menor riesgo posible de humanos en el manejo y administración de cualquier tipo de eventualidad.
2. Utilizar software legal, para poder contar con el debido soporte técnico y de actualizciones del fabricante, lo cual es una ventaja de carácter indiscutible.
3. Mantenimiento de dispositivos de la empresa: esto permitirá que las vulnerabilidades se vean recucidas de manera exponencial y que su funcionamiento sea óptimo.
4. Uso de programas de antivirus y antimalware: estos son de gran utilidad para identificar y prevenir amenazas de seguridad, sin embargo, siempre es importante contar con una licencia que pueda cubrir la totalidad de los equipos.
5. Tener copias de seguridad: de toda la información, bases de datos lo cual nos garantizará que no tengamos pérdidas de recursos que pueden ser altamente sensibles para el funcionamiento de la misma.
6. Usos de contraseñas seguras: la utilización de la mismas en todos los dispositivos y aplicaciones nos ayudan a evitar riesgos innecesarios.
7. Personal capacitado: la capacitación es muy importante para que el personal sea capaz de detectar vulnerabilidades.

Definiciones

La Seguridad informática puede definirse como un conjunto de medidas de prevención y detección de riesgos, amenazas, vulnerabilidades y cualquier otro tipo de eventualidades que puedan afectar un dispositivo o conjunto de ellos.
Vulnerabilidad, es una debilidad o fallo en un Sistema de información que pone en riesgo la Seguridad de la información.
Amenaza: es toda acción que aprovecha una vulnerabilidad para atentar contra la Seguridad de un sistema de información.
La seguridad informática es la disciplina que se encarga de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Las vulnerabilidades

Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software. Que exista una vulnerabilidad no significa que se produzca un daño en el equipo de forma automática. Es decir, si un equipo informático tiene algún punto débil, no por eso va a fallar, lo único que ocurre es que es posible que alguien ataque el equipo aprovechando ese punto débil.

Las amenazas y sus impactos

Algunas de las fuentes de amenazas más comunes en el ámbito de sistemas de información son:

- Malware o código malicioso: permite realizar diferentes acciones a un atacante. Desde ataques genéricos mediante la utilización de troyanos, a ataques de precisión dirigidos, con objetivos específicos y diseñados para atacar a un dispositivos, configuración o componente específico de la red.
- Ingeniería social: Utilizan técnicas de persuasión que aprovechan la buena voluntad y falta de precaución de la víctima para obtener información sensible o confidencial. Los datos así obtenidos son utilizados posteriormente para realizar otro tipo de ataques, o para su venta.
- APT o Amenazas Persistentes Avanzadas (*Advanced Persistent Threats*): son ataques coordinados dirigidos contra una empresa u organización, que tratan de robar o filtrar información sin ser identificados. Se suelen ayudar de técnicas de ingeniería social y son difíciles de detectar.
- Botnets: conjunto de equipos infectados que ejecutan programas de manera automática y autónoma, que permite al creador del botnet controlar los equipos infectados y utilizarlos para ataques más sofisticados como ataques DDoS.
- Redes sociales: el uso no controlado de este tipo de redes puede poner en riesgo la reputación de la empresa.
- Servicios en la nube: una empresa que contrate este tipo de servicios tiene que tener en cuenta que ha de exigir los mismos criterios de seguridad que tiene en sus sistemas a su proveedor de servicios. Se ha de asegurar de contratarlos con empresas cuya seguridad este demostrada, y firmar SLA o ANS (Acuerdos de Nivel de Servicio) en los que quede definida la seguridad que necesita la empresa.

Algunos incidentes pueden implicar problemas legales que pueden suponer sanciones económicas y daños a la reputación e imagen de la empresa. Por eso, es importante conocer los riesgos, medirlos y evaluarlos para evitar en la medida de lo posible los incidentes, implantando las medidas de seguridad adecuadas.

La gestión del riesgo informático

La identificación y el establecimiento de medidas para contrarrestar las posibles amenazas y vulnerabilidades a las que se enfrenta una organización, se lleva a cabo a través de un plan de gestión de riesgos informáticos, para ello es necesario en primer lugar identificar todas las posibles vulnerabilidades de la organización a este respecto. El ámbito de la empresa, así como la naturaleza de sus actividades determinarán qué tipo de riesgos existen y el nivel crítico de cada uno de ellos. También es interesante establecer el posible impacto que tendría cada uno de ellos sobre la organización.

La finalidad de esta primera fase es la de identificar todos los posibles riesgos para, posteriormente, establecer un plan de gestión de riesgos informáticos, teniendo en cuenta todas las vulnerabilidades y peligros detectados. Uno de los aspectos en los que más se va a incidir, es en el de la seguridad de los archivos digitales de la empresa.

Tengamos en cuenta que, en dichos archivos pueden estar almacenados datos altamente sensibles, desde datos personales, hasta datos estratégicos, financieros, patentes y procesos de trabajo etc.

La estrategia a seguir en cuenta a establecer un plan de gestión de riesgos informáticos debe solventar dos posibles fuentes de riesgo básicas: la pérdida accidental de datos importantes o el robo de dichos datos.

Aún en la actualidad muchas empresas no tienen establecidas medidas efectivas para detectar y eliminar vulnerabilidades, así como para contrarrestar posibles ataques, algo que es más que recomendable.
Una vez la organización tenga clara la importancia de establecer un plan de gestión de riesgos informáticos, podrá delegar este trabajo a una empresa externa dedicada a este tipo de servicios o bien encargar tal función a miembros de la propia organización, que deberán contar con los conocimientos suficientes para identificar los riesgos y poner en marcha todas las medidas y protocolos necesarios para evitarlos.
Asimismo, es importante que todos los trabajadores de la empresa sean conocedores del plan, ya que de ellos depende en gran medida el cumplimiento de las medidas y normativas de carácter interno que se establezcan.

Conclusiones y recomendaciones

En conclusión, una vez se haya establecido un buen plan de gestión de riesgos informáticos habrá de ser debidamente comunicado y explicado a todos los trabajadores para que puedan aplicarlo de forma correcta. Habrán de impartirse formaciones o cursos en caso de que los trabajadores así lo precisen para evitar problemas en la implantación del plan de gestión de riesgos.
El entorno donde se mueve cada empresa así como las debilidades que puedan surgir son muy variables, por ello el análisis por parte de profesionales es de suma importancia. Los software de gestión de riesgos son una de las herrmientas claves para implementar un plan de gestión de riesgos y facilitar las tareas y las medidas de cara al equipo de trabajo.
.

Referencias bibliográficas

- Carpentier, J. (2016). *La seguridad informática* en la PYME. Editorial ENI.
- Cañon, L. (2015). *Ataques Informáticos Ethical Hacking y conciencia de seguridad informática en niños. (Trabajo de Fin de Grado).* Universidad Piloto, Colombia.

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica