ANÁLISIS DE TÉCNICAS DE SEGURIDAD EN EL MANEJO DE DATOS EMPRESARIALES

Carlos Ernesto Medina Rocha[1], Cinthya Lizeth López Lizárraga[1], Hugo Alonso López Zatarain[1]

[1]Facultad de Informática Mazatlán (MEXICO)

Resumen

La presente investigación, se enfocó en la búsqueda de información para prevenir el robo de datos en las empresas, con el objetivo de llevar a cabo buenas estrategias de seguridad para lograr una mayor efectividad en el respaldo de sus datos evitando así su robo. Después de que se llevó la investigación y se acomodó la información de las diferentes técnicas que se usan hoy en día se explica como es que cada una de ellas funcionan, la manera en la que actúan ante las amenazas que se le presentan y como resultado se muestran las técnicas que actualmente usan las empresas y cuales les son más efectivas.

Palabras clave: Robo, datos, amenazas, empresas, seguridad.

1 INTRODUCCIÓN

Hace un par de décadas, la seguridad informática estaba enfocada solamente en defender los equipos y sus sistemas operativos, ya que el principal objetivo de las amenazas, era afectar su funcionamiento y evitar que los equipos dejaran de tener un buen rendimiento. Lo que antes se hacía por diversión hoy se ha convertido en algo rutinario para algunos ciber-delincuentes, que sistemáticamente organizados han llevado la infiltración a otros niveles [1].

Los tiempos van cambiando y la seguridad informática no es la excepción, con el paso de los años se han experimentado malas prácticas en contra de éstas, tales como el robo de información, usurpación de identidad e incluso infiltración en los equipos con fracturas y vulnerabilidades. Todo esto ha sido un gran problema para las empresas, ya que lo más importante para éstas, es el adecuado manejo de la información y enfocar la misma seguridad en todos sus procesos de negociación, siendo estos los más vulnerables al momento de ser atacados por estos delincuentes [2].

En el mercado actual, la competitividad e influencia de las amenazas informáticas han ido en aumento y es así en donde las diferentes organizaciones mundiales empiezan a llevar a cabo programas que ayudan a detectar ciertos delitos informáticos y las diversas acciones que existen para poder infectar las computadoras a través de archivos maliciosos [3].

Las empresas están más vulnerables al robo de información y es aquí cuando surgen las preguntas que motivaron esta investigación ¿Cuál será la mejor manera que existe para poder garantizar una óptima defensa del manejo de los datos? Se podría pensar en el típico antivirus de la empresa, pero no, ahí entran los diferentes procedimientos y métodos de defensa que se tiene para garantizar que ningún dato sea extraído ilegalmente, ese es el momento cuando se presenta una abertura de seguridad en los servidores donde se almacena información importante de las empresas, pero todo esto es parte de un proceso de protección que incluye técnicas que han sido desarrolladas para poder luchar contra los virus o archivos infecciosos, pero, ¿Cómo identificar una amenaza?, ¿Qué técnicas de seguridad se pueden implementar ante dichos ataques?, y ¿Por qué son tan importantes los respaldos de seguridad? [1].

La investigación tiene como finalidad poner a su disposición información acerca de las posibles amenazas que pueden afectar y como puede actuar ante estas, cabe recalcar que las técnicas que se requieran implementar tendrán que ser analizadas cuidadosamente, ya que de ellas dependerá el futuro éxito o fracaso de la empresa.

2 METODOLOGÍA

En los últimos años, las técnicas de seguridad como el cifrado de datos o el respaldo de la información, han incorporado nuevos protocolos y procesos con base a algoritmos, de tal manera que ha ayudado en la protección de manejo de datos empresariales, por esa razón, sin las técnicas de seguridad habría un aumento en el robo de datos, lo que provocaría un gran problema para las empresas al momento de resguardar la información que está en los servidores.

Para evitar las consecuencias de estos ataques hay que conocer los tipos de amenazas informáticas que existen, en la *Tabla 1* se muestran algunas de estas.

Tabla 1. Amenazas informáticas [4]

Amenazas	Descripción
Spam	El spam es una de las amenazas de seguridad más comunes. Mucha gente se ve afectada cada año por correo no deseado que falsifica su información engañando al usuario para que siga algunos de los enlaces que contiene.
Farming	Su objetivo es convencer al usuario de que visite un sitio web malicioso e ilegítimo redireccionando la URL legítima. Una vez dentro, el objetivo de los cibercriminales es conseguir que el usuario les dé su información personal.
Phishing	Por desgracia se trata de uno de los tipos de amenazas informáticas más fáciles de ejecutar. Consiste en enviar correos electrónicos falsos o mensajes que se parecen a los correos electrónicos enviados por compañías legítimas. Así, se hace pensar al usuario que es la compañía legítima y aumentan las probabilidades de que se comparta información personal y financiera.
Ransomware	Los hackers se cuelan en los ordenadores de sus víctimas y restringen el acceso a su sistema y archivos. Luego solicitan un pago a cambio de recuperar el control de sus datos.
Gusano informático	Esta es una amenaza de seguridad muy común. Un gusano trabaja solo, vive en el ordenador y se propaga al enviarse a otros.
Spyware / Trojan Horse	Un caballo de Troya es un programa malicioso que parece un software legítimo. Mientras está instalado en el ordenador del usuario, se ejecuta automáticamente y espía su sistema o elimina sus archivos.

Ataque distribuido de denegación de servicio	La estrategia de ataque consiste en ponerse en contacto con un sitio web o servidor específico una y otra vez. Aumenta el volumen de tráfico y colapsa el sitio web / servidor. El usuario malicioso generalmente usa una red de ordenadores zombie.
Red de equipos zombie	Esta es una forma de ejecutar varias amenazas de seguridad. El usuario malintencionado toma el control de varios ordenadores y los controla de manera remota.
Malware	Este es el nombre general dado a varias amenazas de seguridad que se infiltran y dañan un ordenador.
Virus	Un virus siempre está oculto en un software o sitio web legítimo e infecta el ordenador afectado y puede extenderse todos los que se encuentran en su lista de contactos.

En la *Tabla 2* se podrá observar cómo es que las técnicas de seguridad trabajan y cómo hacen para poder proteger la información. Se ha determinado cuáles son las técnicas más usadas en la actualidad y cómo estas funcionan.

Tabla 2. Seguridad de datos más eficaces.

Modificado de [5]

TÉCNICAS	DESCRIPCIÓN	FUNCIONAMIENTO
Encriptación de datos	Es la transformación a un código que solo las personas con el acceso a una clave especial o contraseña puede leer.	Utiliza dos claves es auto cifrado. El primer algoritmo de cifrado simétrico es el Data Encryption Standard (DES), que utiliza una clave de 56 bits y la segunda es Advanced Encryption Standard (AES) se considera más fiable porque utiliza una clave de 128 bits, 192 bits o 256 bits. Por lo tanto, nadie puede obtener esta información que no se la persona autorizada o que tenga permiso a ella [6].
Copia de seguridad (recuperación de datos)	Es un proceso de almacenamiento de copias de datos que se puede utilizar en caso de perdidas. Se puede realizar en servicios de nube u otro medio.	La intención es que, en caso de daños o perdida de archivos importantes estos se puedan recuperar completamente.

Antivirus	Es un software que permite mantener un equipo de cómputo prevenido, protegido y elimina amenazas cibernéticas.	Su función es escanear archivos con la finalidad de encontrar y eliminar virus y/o softwares maliciosos que puedan estar instalados en los equipos.
Seguros cibernéticos	Estos seguros ayudan a proteger negocios, equipos de cómputo, etc., contra pérdidas ocasionadas por un ciberataque.	Los seguros protegen la reputación de las compañías, contra la difamación o afectaciones a la privación de quien lo adquirió.
Data masking (enmascaramiento)	Existen dos tipos: dinámico y estático. Este tipo de tecnología protege la información clasificada que no debe ser leída por alguien más.	El enmascaramiento de datos estático (SDM) reemplaza permanentemente los datos sensibles al alterar los datos en reposo. El enmascaramiento dinámico de datos (DDM) tiene como objetivo reemplazar los datos confidenciales en tránsito dejando los datos originales en reposo intactos y sin cambios [7]

Actualmente, se encontró evidencia sobre los ataques a las empresas que son cada vez más hostiles y constantes, teniendo en cuenta que si se quiere limitar o acabar con ellos se tienen que implementar técnicas que sean capaz de tener una repuesta rápida y efectiva a estos ataques.

3 RESULTADOS

A continuación, se podrá observar en la *Figura 1* del impacto económico y ciberataques más comunes como consecuencia de ataques informáticos.

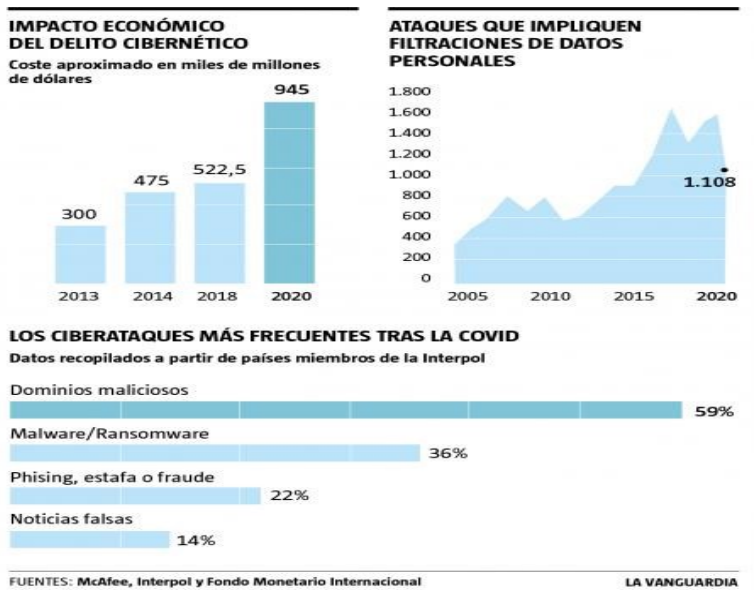

Figura 1. Ataquesinformáticos

Después de investigar y recabar información sobres las diferentes técnicas que existen se puede decir que cada una de ellas tienen su forma de actuar y proteger los datos ante los ataques que sufren las empresas en la actualidad. A continuación, se muestran los consejos [8].

- *Ataque a cuentas y permisos.*
  Se recomienda:
  - Eliminar de todos los dispositivos las cuentas innecesarias o de invitados
  - Utilizar contraseñas más seguras o largas pero fáciles de recordar con al menos 8 caracteres y cambiarlas con frecuencia.
    Por ejemplo: incluir mayúsculas, minúsculas, números y caracteres especiales (#!@]*($)

Figura 2. Contraseña Segura

- *Ataque a equipos y dispositivos de red.*
  - Mantener activos los firewalls de los ordenadores personales y de los routers que se conectan a Internet.
    Por ejemplo: en la *Fig. 3* que se podrá observar a continuación son algunos de los firewalls que existen y su función es proteger, prevenir las redes privadas de ataques o intrusos que sedean robar los datos.

Figura 3. Firewalls

- *Antimalware.*
  - Estos softwares nos ayudan a la prevención, detección y remediar programas maliciosos. Algunos ejemplos se podrán observar en la *Fig. 4.*

Figura 4. Antimalwares

- *Software.*
  - Es importante que en cuanto se lancen los parches y actualizaciones realizarlas para que estos no se encuentren vulnerables. Además, contar con copias de seguridad completas para poder recuperarla en un futuro si se llega a tener una perdida. Fig. 5, por ejemplo.

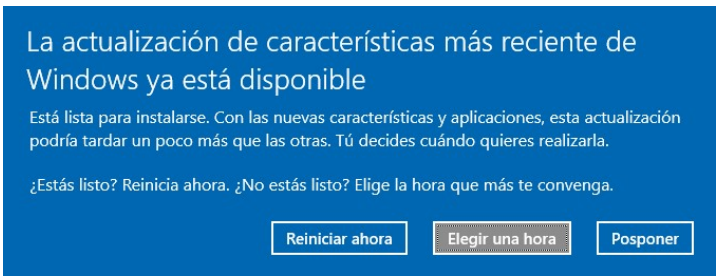

Figura 5. Actualización de software

4 CONCLUSION

Los resultados que se obtuvieron de la investigación mostraron la importancia de implementar técnicas de seguridad que ayudarán a mantener la información protegida, logrando así evitar desastrosas consecuencias como pérdidas de ingresos, pérdida de propiedad intelectual y el daño de reputación de la empresa.

En cuanto al uso de las prácticas de protección que se encuentren disponibles en la actualidad, se tiene como objetivo conservar la integridad, disponibilidad, privacidad, control y autenticidad de los datos a salvaguardar, cabe mencionar que es de vital importancia mantenerlos en estado alerta y en actualización permanente, ya que la estabilidad forma parte de las empresas, esto a su vez requiere efectivas acciones de capacitación y difusión de mejores métodos.

5 REFERENCIAS

[1] I. M. Ramírez, «La importancia de la Seguridad de la Información,» 10 Julio 2020. [En línea]. Available: https://blog.posgrados.ibero.mx/seguridad-de-la-informacion/.

[2] PowerData, «Seguridad de datos: En qué consiste y qué es importante en tu empresa,» 2021. [En línea]. Available: https://www.powerdata.es/seguridad-de-datos.

[3] «Ibero,» 2021. [En línea]. Available: https://blog.posgrados.ibero.mx/seguridad-de-la-informacion/.

[4] A. Pérez, «OBS Business School,» 26 Abril 2019. [En línea]. Available: https://www.obsbusiness.school/blog/10-amenazas-informaticas-en-el-punto-de-mira.

[5] M. Gorman, «Las 7 técnicas de seguridad de datos más efectivas,» [En línea]. Available: https://blog.bismart.com/6-tecnicas-de-seguridad-de-datos-efectivas.

[6] E. I. Ecuador, «¿Qué es el cifrado de datos y por qué es sumamente importante para las compañías?,» [En línea]. Available: https://www.inforc.lat/post/importancia-cifrado-datos.

[7] R. PowerData, «¿Qué es el data masking o enmascaramiento de datos?,» 14 Marzo 2013. [En línea]. Available: https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/bid/238741/que-es-eldata-masking-o-enmascaramiento-de-datos.

[8] INCIBE, «11+1 consejos para elevar la ciberseguridad de tu empresa,» [En línea]. Available: https://www.incibe.es/sites/default/files/contenidos/blog/Quien-este-libre-ciberriesgos-tire-primerapiedra/11consejos-elevar-ciberseguridad.png.