Insider Threats, el principal riesgo para las empresas

Author : paucabla

Date : 16 octubre, 2018

Quiero aprovechar este post para dar a conocer el tema del que tratará este blog durante los próximos dos meses. El tema en cuestión serán las “insider threats” lo que al español podríamos traducir como amenazas o riesgos internos.

En primer lugar, me gustaría presentar una definición a cerca de este tema.

Una “insider threat” es una amenaza contra la seguridad, datos o procesos de una organización. Esta amenaza proviene de alguien cercano o conocedor de la empresa, como pueden ser empleados, exempleados, proveedores, clientes. En definitiva, cualquier stakeholder que tenga acceso a información confidencial, sistemas o redes de la empresa y haga un mal uso de las mismas. [1]

Hace algunos años, las empresas ponían mucho énfasis en proteger sus datos, procesos y redes desde un carácter estructural. Por una parte, esto está bien ya que añade protección. Pero la mayoría de ellas no se dieron cuenta que el eslabón más débil de toda esta seguridad siempre serían sus empleados, clientes o proveedores. Es decir, puedes tener un sistema extremadamente seguro, pero si alguien con acceso a él vende esa información de acceso o directamente hace un uso no autorizado de la misma, ese sistema pasaría de extremadamente seguro a totalmente vulnerable.

En la actualidad, estas empresas ya se han dado cuenta del riesgo que suponen los riesgos asociados a las personas para sus empresas y que este probablemente sea mayor y más difícil de proteger que aquellas provenientes de las infraestructuras. Por ello, han empezado a tomar cartas en el asunto.

Dentro de los “insider threats” podemos encontrarnos con dos categorías principales, la

primera haría referencia a las amenazas realizadas con un fin malicioso como puede ser la intención de robar o perjudicar a la compañía. Y por otro lugar, tenemos a todas las amenazas que se producen de manera accidentalsegún un estudio de ca technologies. [2] En la actualidad, se dan los dos tipos de amenazas a partes iguales.

De este estudio podemos extraer algunos datos que pueden resultar de interés, por ejemplo:

- El 90% de las compañías se siente vulnerable frente a los “insider attacks”.
- Un 53% de las empresas que forman parte del estudio confirman haber sufrido un ataque de este tipo en los últimos 12 meses.
- Las empresas casi en su mayoría (superior al 90%) están optando por sistemas de monitorización de sus empleados y aplicaciones. Lo que aparte de descubrir ataques, ayuda después a acelerar las tareas forenses.
- Las tecnologías más populares para la detección de “insider attacks” son: Data Loss Prevention (DLP), encriptación, gestión de acceso, sistemas de logs y sistemas de detección y prevención de intrusiones.
- El 86% de las empresas tienen o están desarrollando un programa para las “insider threats”. El 36% tiene ya el programa en uso y el 50% está trabajando en ello.

Para terminar con este primer post, quería dar mi opinión personal acerca del tema. En primer lugar, he de decir que este es el tipo de riesgo o amenaza para las empresas que más grave me parece y el más difícil de controlar e incluso de detectar. Por ejemplo, un ex empleado descontento podría haber estado fotografiando información confidencial desde su usuario autorizado durante mucho tiempo y ofrecérsela a la competencia sin que nadie supiera que poseía esta información. En los próximos posts trataré de traer casos reales en los que se hayan demostrado este tipo de actitudes.

Pero lo que me parece más preocupante es la otra categoría de “insiders”, los accidentales. Creo fundamental que las empresas realicen programas de formación en este aspecto para todos los empleados para poder atajar este asunto que les puede suponer una gran lacra en el futuro. En cuanto al estudio, me parece muy llamativo las cifras que se manejan ya que prácticamente todas las empresas se sienten muy vulnerables frente a estas amenazas. No obstante, la mayoría estas empresas, no poseen en la actualidad un programa para hacerlas frente, aunque bien es cierto que la mitad de ellas están en progreso. Esto demuestra la importancia que está cobrando en este sector.

En el próximo post, trataré de traer al blog algunas noticias actuales de casos en los que ha habido problemas en las empresas debido a estos “insider threats” e insider attacks”.

Referencias:

[1] “What is an insider threat?” – https://www.observeit.com/insider-threat/ [consultado el8/10/18]

[2] “Insider threat 2018 report” – https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf [consultado

el 8/10/18]