Últimas tendencias en los insider threats

Author : paucabla

Date : 10 noviembre, 2018

En el último post, expliqué de forma general en qué consistían los insider threats y además traté de aportar algunos datos a cerca de un estudio que llevó acabo CA technologies sobre la concienciación de las organizaciones frente a estos riesgos. [1] Hoy quiero hacer hincapié en la relevancia que deberían de tener este tipo de riesgos para las organizaciones actualmente, así como la relevancia o prioridad real que le otorgan. Para ello, he elegido el ejemplo de un estudio llevado a cabo en Canadá. En este país se elaboró un informe en 2012 [2] acerca de las insider threats en el que participaron diferentes organizaciones del país. Asimismo, este mismo año se ha publicado el mismo informe con datos actualizados del año 2017. Un nuevo estudio ha sido publicado hace menos de una semana actualizando el informe con los datos de 2018. [3].

En estos informes se trata la prevención, mitigación y gestión de este tipo de riesgos. Y como he mencionado anteriormente, al realizar la comparación entre los dos estudios se puede ver cuales han sido los cambios más sustanciales en las tendencias, hubo unas 267 respuestas en la encuesta para la elaboración del informe.

Por ejemplo, en 2012 menos del 14% de los encuestados confirmaron la existencia en la organización de una definición operativa de lo que es un insider threat, mientras que en 2017 el 18% de los que respondieron lo hicieron de forma afirmativa. Por lo que se puede ver que ha sido un avance, aunque no excesivo.

Uno de los puntos que han destacado otros medios sobre el informe es la pérdida de confianza a la hora de responder a las insider threats que han tenido las organizaciones en los últimos 5 años. Esto puede ser debido al aumento en tamaño y complejidad de los sistemas de tecnologías de la información o incluso al hecho de que todos los empleados ahora llevan al trabajo los aparatos Smart (Smartphone, smartwatch, tablets, etc..), siguiendo tendencias tan

populares como el BYOD (Bring your own device).[4] Esto representa nuevos y numerosos riesgos para las organizaciones, en especial del segundo tipo que comentaba en el post anterior, insider threats involuntarios o accidentales. Todos estos dispositivos se podrían utilizar como vectores de entrada a los sistemas de la organización.

Sigamos con datos extraídos del informe que a mi parecer pueden ser preocupantes. Por ejemplo, en la encuesta de 2012 se preguntó si en sus organizaciones estaban claramente definidos los roles y responsabilidades para la gestión de insider threats. En aquel entonces el 73,5 por ciento de los encuestados respondió que sí lo estaban, mientras que en la última encuesta realizada en 2017 tan solo el 46,4 por ciento lo hizo. Esto supone un retroceso en la concienciación acerca de este imponente riesgo. Además, el 40% en 2017 dijo que no habían recibido ninguna formación relacionada con los insider threats.

De acuerdo con estos datos, en mi opinión, podemos ver como en el post anterior las organizaciones comenzaban a darse cuenta del riesgo y la amenaza que suponen las insider threats. Aunque es posible que como en el caso de Canadá, no estén enfocando correctamente las formas de mitigarlo o evitarlo. Existe una clara diferencia entre la jerarquía superior de la empresa (la ejecutiva), que si que es conocedora de las medidas a tomar y el estrato inferior (la operativa), que muchas veces por falta de formación, se expone a riesgos de manera involuntaria. Si que es preciso matizar el siguiente punto, la formación y conocimiento de estos riesgos y amenazas es muy útil, pero pueden existir algunas medidas que no todos los empleados deberían conocer ya que podrían causar una brecha de seguridad

Pero como he insistido en numerosas ocasiones, más de la mitad de los casos de insider threats se producen de forma involuntaria, y es por ello por lo que se debería dar una formación adecuada a todos los miembros de la organización y ofrecer consejos o recomendaciones a los agentes externos que están relacionados con la empresa. (los stakeholders)

De esta forma, se podría reducir drásticamente el número de casos. Este tema es el que se tratará en alguno de los próximos post junto con la identificación de los riesgos asociados o producidos por las insider threats.

En definitiva, puedo decir que se está avanzando en el campo de la concienciación pero que aún queda mucho camino por recorrer.

[1] “Insider threat 2018 report”

– https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

[consultado el 10/11/18]

[2]”Preventing, mitigating and Managing Insider Threats”

- https://www.conferenceboard.ca/e-library/abstract.aspx?did=5451

[consultado el 10/11/18]

[3]”Updating our knowledge of the insider threat”

- https://www.conferenceboard.ca/e-library/abstract.aspx?did=9956

[consultado el 10/11/18]

[4] “Bring your own device” (Océano)

BYOD. (2016). Smart Business Columbus, 24(6), 40. Retrieved from https://search-proquest-com.proxy-oceano.deusto.es/docview/1779441059?accountid=14529

[consultado el 10/11/18]

[5] “Insider threats still nuclear”

- https://www.newswire.ca/news-releases/the-insider-threat-majority-of-canadian-organizations-still-unclear-on-what-it-means-698885751.html

[consultado el 10/11/18]