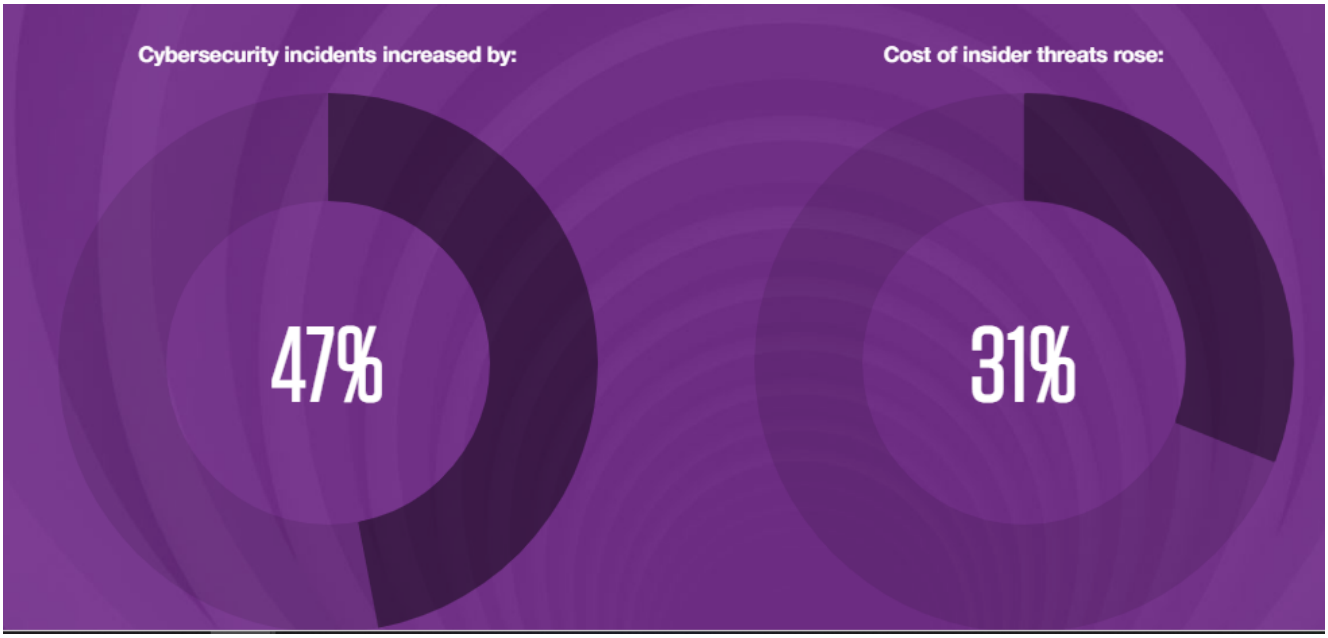
La importancia de las amenazas internas

En el anterior post hable sobre que eran las amenazas internas y trate el tema de forma general dando pequeñas pinceladas sobre el tema. Durante el texto se habló sobre la importancia de minimizar estas amenazas y la importancia que este tenía. En este post ahondare en esto haciendo uso de ejemplos prácticos y datos relevantes que muestren la gran importancia que tiene mantener a raya las amenazas internas en las organizaciones. Al hablar de algún caso, ahondar en datos globales, ver qué organismos están interesados en el tema y que toolkits existen os daréis cuenta de cómo es de vital importancia mantener a raya las posibles amenazas internas que puedan surgir, ya sean intencionadas o no.

Para empezar a ver la importancia de estas amenazas voy a empezar con un enfoque más global haciendo uso de diversos datos recogidos recientemente. En concreto me voy a centrar en el informe del Instituto Ponemon "Coste 2020 de las amenazas internas: Global". Se trata de un informe que abarca 12 meses sacado a principios de año por lo que gran parte de los datos serán del 2019. En este se detecta que en dos años la frecuencia de estos incidentes ha aumentado un 47% contabilizando en este informe un total de 4.716 incidentes. En el anterior post ya comenté un poco que esto podía deberse a la velocidad en la que la tecnología avanza lo cual hace que surjan más amenazas y más posibilidades. Las empresas se han dado cuenta de la importancia de contener las amenazas por lo que se ha visto un crecimiento del 86% en la dedicación de investigar porque surgen y cómo pararlas. El coste de una de estas amenazas, según indica el informe, es diferente dependiendo del tiempo que haga falta emplear para neutralizarla. Una compañía hace un desembolso de más o menos €12.57 millones al año cuando una amenazada dura más de 90

días, siendo 77 el promedio de días que se tarda en contener estas amenazas. En el informe y en la noticia enlazada en las referencias, de donde salen estos datos, se muestra mucha más información, pero para resaltar un apunte final decir que el desembolso de una compañía grande es de unos €16.42 millones al año en este tipo de amenaza y €7.04 millones el de una pequeña. Son cifras que deberían llamar nuestra atención y la de las empresas para empezar a poner el foco en este tipo de amenazas.[1][2]

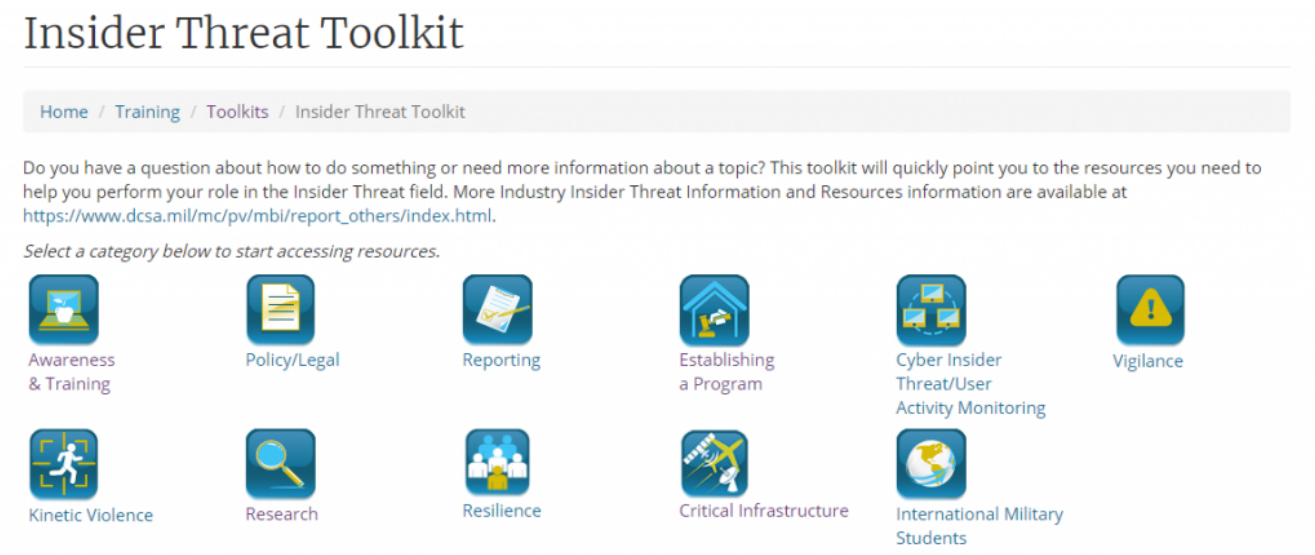


Viendo un caso de ejemplo es la mejor manera de entender el impacto que puede tener sobre la empresa. En mi caso, he elegido un hecho acontecido a la empresa Canadiense Shopify Inc. Con sede en Ottawa, Ontario. Es una empresa que se centra en el comercio electrónico y ofrece un portal web donde las tiendas pueden vender sus productos [3]. La noticia a comentar data del 23 de septiembre de este mismo año y es que ese mismo mes Shopify se vio envuelta en una brecha de datos por culpa de unos empleados del grupo de soporte que robaron datos de unos 200 comerciantes. La propia compañía asegura que no ha sido un tema de vulnerabilidad de datos si no que un ataque por parte de los dos empleados. Han conseguido datos de las compañías que utilizan el servicio y de ahí también se ha podido acceder a listas de clientes. La buena noticia es que por lo que se sabe no se ha filtrado ningún tipo de tarjeta de

crédito ni datos de pago, pero imagina por un momento que alguien consigue datos bancarios de miles de personas. Si se diera el caso, podría ser un gran golpe para las empresas, para Shopify y para toda la gente que ha dejado su información bancaria dentro del servicio, podría suponer que alguien ajeno a la empresa pierda tanto sus datos como verse afectado monetariamente. Aunque es cierto los datos que han obtenido aún no ser de gran riesgo pueden ser usados para enviar spam y correos maliciosos a los afectados. En el artículo destaca que Shopify fue rápida a la hora detectar la brecha, desautorizar a los atacantes, despedirlos y seguir investigando el asunto ahora a manos del FBI. Por lo que parece no se deben de haber utilizado los datos obtenidos, pero nunca se sabe lo que podría llegar a pasar. La compañía resalta que estas amenazas son de las peores ya que dan muy mala imagen a la compañía y que son un tipo de amenaza en la que siempre que depositas tu confianza en un empleado te estás arriesgando. Además, ahora en época de Covid les ha resultado más difícil controlar el comportamiento de tus empleados para saber si pueden ser una amenaza. El propio artículo menciona otro caso en el que un atacante ofreció $1 millón a un empleado de Tesla por poner un ransomware de forma intencionada. [4]

Sería raro dudar de la importancia cuando septiembre se considera el “National Insider Threat Awareness Month”. Se trata de un esfuerzo colaborativo entre distintas organizaciones para enfatizar y dar la importancia que merece a la documentación, detección y mitigación de estas amenazas. Este año se han centrado en la elasticidad a la hora de recuperarse de este tipo de amenazas [5]. En un artículo de

itgovernance hablan sobre la importancia de la ISO27001 para controlar o evitar estas amenazas. La ISO27001 es un estándar de mejores prácticas para gestionar la seguridad de la información. Este estándar va más allá de nuestro tema, pero como se comenta en el artículo es importante aplicarla ya que tener la información interna segura y controlada puede evitar que un atacante interno acceda a ella y pueda utilizarla en contra de la empresa [6]. También existen varios toolkits a usar, como por ejemplo el que ofrece CDSE (Center for Development of Security Excellence). Este toolkit está abierto y disponible para ver sin ninguna restricción. En él podremos acceder a varios topics donde tendremos pdfs con las best practices e información importante para que podamos establecer nuestro propio programa de contención. Es interesante ver todos los puntos que trata el toolkit para entender a la perfección cómo funcionan estas amenazas y cómo tocan muchos temas críticos dentro de la empresa. [7]



En conclusión, podríamos decir que la importancia de intentar contener y evitar estas amenazas es alta. Es cierto que hacerlo puede ser costoso pero una incidencia de este tipo puede suponer un gran golpe para la empresa y costarle bastante dinero. Además, las mejoras en seguridad que se apliquen para este tipo de amenazas también pueden ser de utilidad frente a amenazas externas.

REFERENCIAS

[1]<< Amenazas internas: cuando el peligro está en tu propia empresa>>, Interbel, acceso el 19 de octubre de 2020, https://www.interbel.es/amenazas-internas/#:~:text=Las%20organizaciones%20más%20grandes%20(más,de%20euros%20en%20amenazas%20internas

[2]<< 2020 Cost of Insider Threats Global Report>>, Observeit, acceso el 19 de octubre de 2020, https://www.observeit.com/cost-of-insider-threats/

[3]<<Shopify>>, Wikipedia, acceso del 19 de octubre de 2020, https://en.wikipedia.org/wiki/Shopify

[4]<<Shopify Insiders Attempted to Steal Customer Transactional Records>>, Infosecurity https://www.infosecurity-magazine.com/news/shopify-insiders-records/

[5]<<Insider Threat Awareness Month: Expect the Unexpected>>, Homeland Security Today, acceso el 19 de octubre de 2020https://www.hstoday.us/subject-matter-areas/airport-aviation-security/insider-threat-awareness-month-expect-the-unexpected/

[6]<<Use ISO27001 to combat the insider threat, experts say>>, itgovernance, acceso el 19 de octubre de 2020, https://www.itgovernance.co.uk/media/press-releases/use-iso27001-to-combat-the-internal-threat-expert

[7]<< Insider Threat Toolkit>>, CDSE, acceso el 19 de octubre de 2020, https://www.cdse.edu/toolkits/insider/index.php