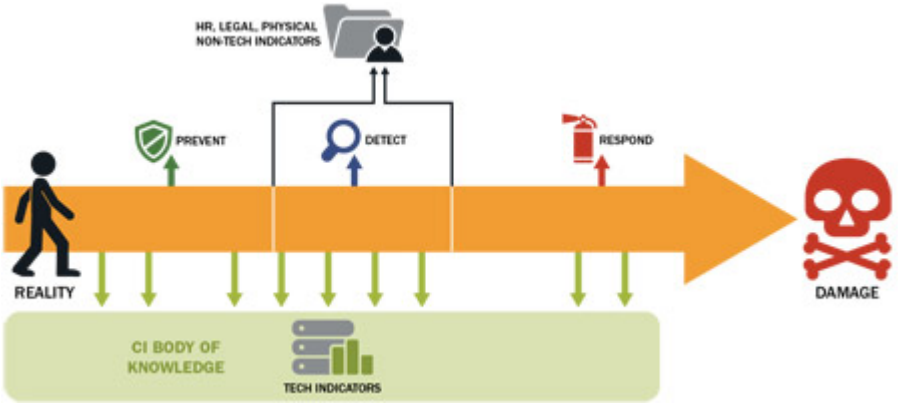
Insider threats: Audit controls

Para este cuarto post me centraré en explicar un **framework metodológico** elaborado por la consultora **EY** para crear un **plan exitoso para la gestión y control de las amenazas** internas en las organizaciones. [1]



https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/disgruntled-employees/

Como ya hemos podido ver en los posts anteriores, **las empresas se están concienciando** del peligro que corren frente a este tipo de amenaza, que riesgos asociados conlleva y cuáles son las tendencias actuales en este campo.

Debido a esta importancia que ha alcanzado situándose como una de las primeras preocupaciones de las organizaciones, es normal que hayan surgido diversos frameworks para elaborar una plan o estrategia con el que hacerle frente a esta amenaza. Como he dicho, me centraré en el desarrollado por EY, pero he de mencionar algunos otros que me parecen también muy acertados.

El primero de ellos está elaborado por **Forcepoint** y consiste en **9 pasos para construir un buen programa de insider threats**. Básicamente está centrado en elaborar un plan de moitorización de los usuarios en todo momento para evaluar los riesgos potenciales de cada perfil y transacción. [2]

El segundo no es tanto un framework sino que es una presentación que realizó el **CERT National Insider Threat Center de la Carnegie Mellon's Software Engineering Institute**. En esta presentación se aborda el tema de cómo **crear los controles necesarios en relación a las insider threats**. [3]

El tercero trata sobre el mundo de las amenazas internas en general, pero en su segunda parte se centra más en los **controles**, sobretodo de **mitigación**, para estas amenazas y proviene de **ISACA**. [4]

Por otro lado tenemos algunos documentos muy interesantes que tratan

este asunto tanto del **Deparment of Defense** estadounidense como la guía de **GTAG** para la auditoría de insider threats. [5][6]

Por último, he querido traer también un par de artículos que listan una serie de **buenas prácticas para poder reducir el riesgo de ser afectados por un insider threat**. [7][8]

Una vez explicado la multitud de opciones que existen al buscar un framework de este tipo (estás solo son una breve muestra), empezaré a atratar la que he elegido para la publicación de hoy.

Al tratarse de un framework metodológico está basado en pasos, en este caso consta de 8. Si se realizan todos de forma satisfactoria, EY asegura que conseguiremos tener un plan de insider threats exitoso. Los pasos en cuestión son los siguientes:

1. Conseguir dentro de la organización el **patrocinio de algún directivo senior** y elaborar **políticas** que animen al resto de stakeholders a unirse. Por otro lado, es de suma importancia no perder la **cultura empresarial** en esas políticas. Este paso es fundamental ya que, para poder elaborar el plan, es necesario que sea aprobada por la junta o comité correspondiente su desarrollo.
2. Desarrollar procesos repetitivos que pueden **registrar**, **monitorizar** y **mitigar** las **amenazas internas**. Siendo importante conocer en qué grado se están evitando o mitigando estas amenazas.
3. Aprovechar los **planes de seguridad de la información y seguridad corporativa**, así como, la **gobernanza de la información**, para identificar y comprender que **activos son críticos** para nuestra organización.
4. Utilizar **analítica de datos para potenciar** y mejorar nuestro sistema de detección, clasificación y mitigación de amenazas internas. Es necesario resaltar que por sí sola la analítica no puede constituir un programa de detección de insider threats.
5. Coordinación con el **departamento legal** u otro órgano de consejo legal para tener en cuenta desde el inicio los principios de **privacidad**, **portección de datos** y de **transferencias de datos**. Este paso está muy relacionado con la **RGPD** que comenté en el anterior post (Si la organización opera o tiene relación con **Europa**).
6. Realizar **controles de forma regular** a personal y proveedores, especialmente a los que tengan acceso a activos críticos o tengan un puesto de alto riesgo.
7. Implementar un **sistema de gestión de consecuencias claro** con el objetivo de que los incidentes del mismo tipo se traten de la misma forma **estándar** e involucrar siempre a las partes correctas en cada caso.
8. Crear un **plan de formación continuo** para que todos los involucrados estén al día en cuanto a las medidas para amenazas internas y de esta forma sean menos vulnerables a sufrirlos y si se diera el caso sepan como gestionarlos.

Con esta metodología podemos observar que la parte fundamental para que un plan de este tipo tenga éxito son las **personas**. Lo más complicado y con mayor criticidad siempre es que las personas estén **interesadas e involucradas** en ello. Si esto no fuera así, evidentemente el plan será más débil y se podrían

encontrar brechas de seguridad de forma más sencilla. Por ello, es importante que la directiva siempre **tenga en cuenta a todos los agentes que intervienen en sus procesos de negocio** y que los involucre en este tipo de iniciativas lo máximo posible.

Referencias:

[1] “Managing insider threat” – EY

https://www.ey.com/Publication/vwLUAssets/EY-managing-inside-threat/$FILE/EY-managing-inside-threat.pdf

[Consultado el 22/11/18]

[2]“Build an Insider threat program” – Forcepoint

https://www.infosecurityeurope.com/__novadocuments/364341?v=636322524334430000

[Consultado el 22/11/18]

[3] “Create insider threat controls” – CERT National Insider Threat Center de la Carnegie Mellon’s Software Engineering Institute

https://published-prd.lanyonevents.com/published/rsaus18/sessionsFiles/8016/HUM-R02-A-Framework-to-Effectively-Develop-Insider-Threat-Controls.pdf

[Consultado el 22/11/18]

[4] “Mitigation control on insider threat” – ISACA

http://m.isaca.org/chapters11/Indonesia/Documents/7%20December%202016%20-%20Mitigation%20Control%20on%20Insider%20Threat.pdf

[Consultado el 22/11/18]

[5]»Insider threat evaluation and audit»- Department of Defense

https://www.nsi.org/pdf/reports/Insider%20Risk%20Evaluation.pdf

[Consultado el 22/11/18]

[6]»Auditing insider threat programs»- GTAG

https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Auditing-Insider-Threat-Programs.aspx

[Consultado el 22/11/18]

[7] “5 layers of defense to prevent insider threats” – ISACA

https://www.isaca.org/CYBER/CYBER-SECURITY-ARTICLES/Pages/5-layers-of-defense

-that-prevent-insider-threats.aspx

[8] “Best practices for insider threat prevention” – Netwrix

https://www.netwrix.com/Insider_Threat_Prevention_Best_Practices.html