Controles para amenazas internas

Ya hemos hablado sobre qué son las amenazas internas, su relevancia y los riesgos que estas acarrean, ahora toca hablar de cómo prevenir, identificar y mitigar estos riesgos aplicando diversos controles. Para empezar a aplicar controles lo interesante es primero saber en qué situación se encuentra actualmente tu empresa y qué esfuerzos está poniendo en detener este tipo de amenazas. En la página de SIRIUS Edge se nos plantean una serie de preguntas que podrían resultar interesantes para identificar el desempeño de nuestra empresa frente a estas amenazas para luego poder crear un programa que ayude a mitigarlas y prevenirlas **[1]**.

- ¿Has identificado y clasificado tus datos críticos?
- ¿Has educado a tus usuarios sobre los procesos de tratamiento de los datos?
- ¿Puede definir el comportamiento normal que debería tener el usuario?
- ¿Eres capaz de identificar comportamientos anómalos?
- ¿Tienes algún control de auditoría para dejar claro las necesidades de acceso y autorización de los usuarios?
- ¿Tienes un programa efectivo de gestión de identidad y acceso (IAM)?
- ¿Prestas especial atención a los usuarios con acceso privilegiado?
- ¿Tienes alguna estrategia para auditar la adherencia a la política del usuario?
- ¿Auditas de forma rutinaria las prácticas de seguridad de terceros que influyan en tu empresa?

En el propio artículo de SIRIUS Edge podemos encontrar puntos clave para montar un programa de auditoría y CISA (Cybersecurity & Infraestructure security agency) también menciona 5 puntos clave para la creación de programas de

auditoría para amenazas internas **[2]**. Aunque estos mencionados sean interesantes he encontrado de mayor interés un artículo de LISA Instituto que da 21 puntos clave para detectar y prevenir insiders en tu organización **[3]**. En la foto podemos ver los 21 puntos que consideran claves. No voy a comentar todos los puntos ya que muchos creo que se explican por sí mismos. Me voy a centrar en el cómo desarrollar el programa formalizado de insider y en algunos puntos más que puedan resultar interesantes de hablar.

LISTA DE 21 MEDIDAS PARA PREVENIR Y DETECTAR INSIDERS

LISA Institute
Security Education

- CONOCER Y DETECTAR TUS ACTIVOS CRÍTICOS
- DOCUMENTAR Y APLICAR LAS POLÍTICAS Y CONTROLES
- ANTICIPAR Y MANEJAR LOS ASUNTOS NEGATIVOS EN EL TRABAJO
- ESTAR ATENTO A LAS REDES SOCIALES
- INCORPORAR LA CONCIENCIA DE LOS INSIDERS EN LA FORMACIÓN DE SEGURIDAD
- INSTITUIR RIGUROSOS CONTROLES DE ACCESO Y POLÍTICAS DE MONITOREO
- SUPERVISAR Y CONTROLAR EL ACCESO REMOTO
- HACER CUMPLIR LA SEPARACIÓN DE DEBERES Y EL MENOR PRIVILEGIO
- INSTITUCIONALIZAR LOS CONTROLES DE CAMBIO DEL SISTEMA
- CERRAR LAS PUERTAS A LA FILTRACIÓN DE DATOS NO AUTORIZADA
- ADOPTAR INCENTIVOS POSITIVOS
- DESARROLLAR UN PROGRAMA FORMALIZADO DE INSIDERS
- TENER CUIDADO EN EL PROCESO DE CONTRATACIÓN
- CONSIDERAR LOS INSIDERS EN LAS EVALUACIONES DE RIESGO
- ESTRUCTURAR LA GESTIÓN Y LAS TAREAS PARA MINIMIZAR EL ESTRÉS
- IMPLEMENTAR POLÍTICAS Y PRÁCTICAS DE ADMINISTRACIÓN DE CUENTAS Y CONTRASEÑAS
- DESPLEGAR SOLUCIONES PARA MONITOREAR LAS ACCIONES DE LOS EMPLEADOS
- ESTABLECER UNA LÍNEA BASE DE COMPORTAMIENTO
- DEFINIR ACUERDOS DE SEGURIDAD PARA CUALQUIER SERVICIO DE LA NUBE
- IMPLEMENTAR COPIAS DE SEGURIDAD Y PROCESOS DE RECUPERACIÓN
- DESARROLLAR UN PROCEDIMIENTO INTEGRAL PARA EL DESPIDO DE EMPLEADOS

LISA Institute
Security Education

Crear un programa de insiders puede ser clave dentro de una empresa ya que proporciona un recurso que puede ayudar a abordar el problema de los insiders. El programa al final es una medida que adopta la empresa para detectar, prevenir y actuar de forma correcta frente a estas amenazas. LISA Institute menciona los componentes comunes que tienen estos programas según el CERT:

- **Programa formalizado y definido:** Se tienen que definir la misión, las directrices a seguir, quienes son los encargados, la gobernanza y el presupuesto.
- **Participación de toda la organización:** Es importante tener la participación de todos los componentes de la empresa para obtener datos que sean útiles en el programa.
- **Supervisión del cumplimiento y la eficacia del programa:** Se crea un grupo que sirva como soporte al gerente del programa para generar nuevas ideas y cambios posibles en el programa. Para aprobar estos cambios y procedimientos que ha propuesto el equipo existe un grupo directivo. Es importante hacer evaluaciones anuales del programa, tanto desde dentro de la empresa como por parte de terceros.
- **Mecanismos y procedimientos de información confidencial:** Se tiene que permitir que cualquiera pueda reportar alguna actividad sospechosa, pero que esa persona no salga perjudicada en el proceso.
- **Plan de respuesta a incidentes de amenazas internas:** Se debe redactar un plan para gestionar las incidencias y alertas que surjan, como actuar, plazos de actuación y recursos necesarios.
- **Comunicación de eventos de amenazas internas:** Es clave comunicar de estas alertas que vayan surgiendo siempre respetando la confidencialidad y la privacidad.
- **Protección de la libertades y derechos civiles de los empleados y clientes:** Al implementar este programa se tiene que revisar cada proceso para asegurar que se

respeta la privacidad de los implicados.

- **Políticas, procedimientos y prácticas:** Redactar un documento detallando, la misión, el alcance, las directivas a seguir, las instrucciones y procedimientos estándar del programa.
- **Técnicas y prácticas de recogida y análisis de datos:** Detallar qué técnicas de monitorización se van a realizar, así como que datos se van a recoger y cuál va a ser su tratamiento con tal de asegurar la privacidad de los datos.
- **Entrenamiento y concienciación sobre las amenazas internas:** Es importante la creación de un programa de capacitación y concienciación. Creo que es un punto clave teniendo en cuenta que los empleados son los que realizan estos ataques muchas veces porque no están informados. La empresa tiene que informarles de que conductas son adecuadas y de cuáles no y concienciarse en cuanto a cómo repercute uno de estos incidentes en la empresa, en el mundo exterior e incluso en el propio empleado. En la página de CISA podemos encontrar videos, publicaciones e incluso enlaces a cursos que tratan el tema **[4]**.
- **Infraestructura de prevención, detección y respuesta:** Tener una infraestructura de defensa tanto física como en la red.
- **Prácticas de amenazas internas relacionadas con los socios comerciales de confianza:** Revisar todos los contratos firmados con terceros para poder detectar posibles amenazas emergentes.
- **Integración de Insiders con la gestión de riesgos empresariales:** En la gestión de riesgos se deben tener en cuenta las amenazas internas junto a todos los demás riesgos que puedan surgir en la empresa.

Entre los 21 puntos unos cuantos tratan el tema de la monitorización como por ejemplo el punto que habla de estar atentos a las redes sociales o las herramientas de

monitorización de empleados. Creo que son clave a la hora de saber qué es lo que el empleado hace dentro de la empresa, pero también tiene su punto negativo y es que se puede llegar a atentar contra la privacidad del propio empleado. No sería el primer caso de despido por culpa de redes sociales y hasta cierto punto no tendría que afectar al puesto de trabajo de la persona. Se tiene que encontrar un punto de monitorización en el que la empresa sea capaz de detectar amenazas, pero sin llegar a privar al empleado de su privacidad, es decir un sistema donde el empleado esté a gusto y no sienta que le están invadiendo su espacio privado. Para ello es importante informar en todo momento al empleado de cómo se le monitoriza y qué información se recopila en ese proceso.

En conclusión, si miramos a los 21 puntos veremos que existen muchos pasos a seguir para mitigar estas amenazas, pero es importante ver hasta qué punto podemos realizar tareas de monitorización de empleados sin atacar directamente a su privacidad.

Otro punto que me ha parecido clave es el mantener un control estricto de los accesos que tienen los empleados a los sistemas y la información. Sólo permitir acceso a personas que lo necesitan hace que los datos y los sistemas no estén tan expuestos como si toda la empresa tuviese acceso a ellos. Buscando documentos relevantes sobre amenazas internas en Océano me ha sorprendido como gran parte de los artículos tratan este tema. Mencionar en concreto uno de Suhair Alshehri que habla sobre la importancia de mantener controlados los accesos en el sistema sanitario para evitar amenazas internas **[5]**. Algo que en una empresa puede suponer una brecha de datos en el sistema sanitario puede poner en juego la vida de las personas, por lo que es un tema clave. Debemos tener en cuenta que a diferencia de los atacantes externos los internos ya tienen credenciales y acceso a la zona de trabajo por lo que les estamos dando facilidades de fastidiarlo todo.

P.S: Investigando sobre el tema de los controles he encontrado

un report de 2020 que contiene datos interesantes sobre las amenazas internas. Podría servir como complemento a lo ya tratado en el segundo post sobre la relevancia. **[6]**

REFERENCIAS

[1] <<5 Keys to Addressing Insider Threats>>, SIRIUS Edge, acceso el 21 de noviembre de 2020, https://edge.siriuscom.com/security/5-keys-to-addressing-insider-threats#:~:text=Two%20key%20controls%20for%20reducing,behavior%20by%20a%20single%20actor.

[2] <<ESTABLISH A COMPREHENSIVE INSIDER THREAT PROGRAM>>, CISA, acceso el 21 de noviembre de 2020, https://www.cisa.gov/establish-program

[3] <<Lista de 21 medidas para detectar y prevenir Insiders en tu organización>>, LISA Institute, acceso el 21 de noviembre de 2020, https://www.lisainstitute.com/blogs/blog/medidas-para-detectar-y-prevenir-insiders

[4] <<INSIDER THREAT – TRAINING & AWARENESS>>, CISA, acceso el 21 de noviembre de 2020, https://www.cisa.gov/training-awareness

[5] Suhair, Alshehri. 2016. << Using Access Control to Mitigate Insider Threats to Healthcare Systems>>. Paper. IEEE International Conference on Healthcare Informatics. Océano.

[6] <<Insider Threat Report>>, Cybersecurity Insiders, acceso el 22 de noviembre de 2020, https://www.cybersecurity-insiders.com/wp-content/uploads/2019/11/2020-Insider-Threat-Report-Gurucul.pdf