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

www.lisainstitute.com

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

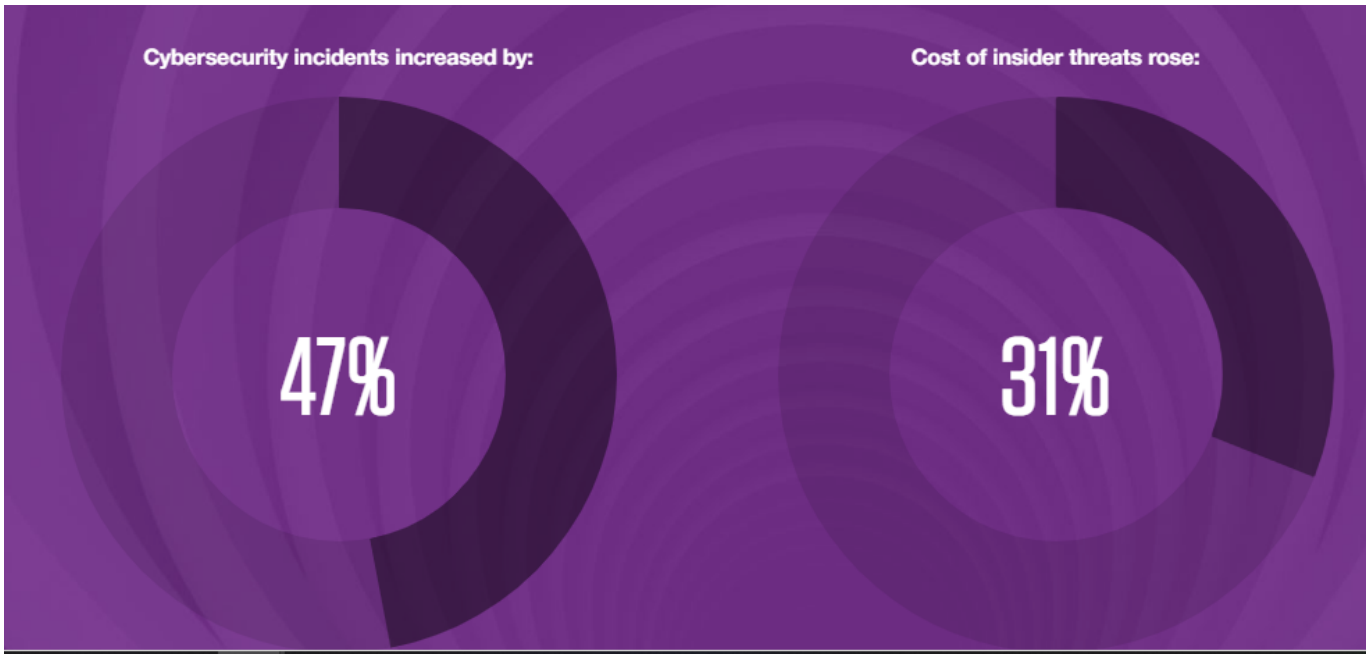
---

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]

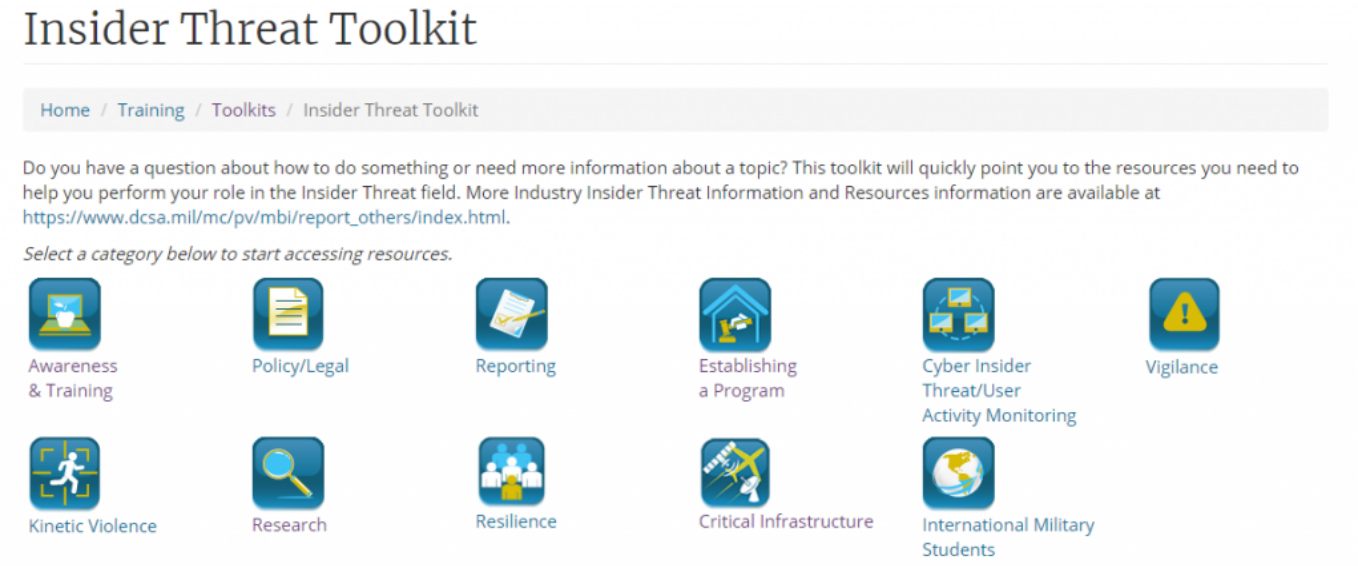


Viendo un caso de ejemplo es la mejor manera de entender el impacto que puede tener sobre la empresa. En mi caso, he elegido un hecho acontecido a la empresa Canadiense Shopify Inc. Con sede en Ottawa, Ontario. Es una empresa que se centra en el comercio electrónico y ofrece un portal web donde las tiendas 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

---

Insider Threats: Derechos del empleado y del empleador

https://www.universidades.com.pa/blog/privacidad-en-el-trabajo-donde-esta-el-limite

En las entradas anteriores, he tratado de acercar al lector una visión general de las amenazas internas. También hemos podido observar cuál es la situación actual en las organizaciones con respecto a este tema, donde comprobamos que genera preocupación pero todavía no alcanzan la suficiente concienciación en algunos ámbitos. En la tercera entrada tratamos cuáles eran los principales riesgos asociados a las amenazas internas, es un tema muy extenso ya que existen multitud de riesgos que se pueden derivar de una amenaza interna, ya sea intencional o de forma involuntaria. Por último, en el anterior post quise traer diferentes frameworks metodológicos que permiten crear un plan contra las amenazas internas que permite crear políticas y controles para prevenirlas o bien para mitigarlas.

En la última entrada, traté de explicar que las personas eran la pieza fundamental para el éxito de este tipo de planes, aunque de forma constante hice alusión a las personas de forma genérica y a todos los individuos involucrados. Con estos términos no hay que confundir cuál es el foco principal de las amenazas internas, **los empleados**. Por lo tanto, al describir en el framework la necesidad de monitorizar las actividades de los empleados y darles una formación adecuada para que sufran el menor número de despistes que podrían dar pie a una brecha de seguridad, se suscitan unas cuestiones de

gran relevancia, ¿Qué **derechos de privacidad** deben disfrutar los empleados? ¿Hasta qué grado puede o debe llegar la **monitorización** por parte de la organización? ¿Quién tendrá acceso a los datos producidos por esta monitorización? ¿Estarán estos **datos ligados a un algoritmo automático o de perfilado**? y podríamos continuar con una infinidad de cuestiones más, pero al final el tema será siempre la privacidad y la no discriminación a la vez que la seguridad de la organización.

Por lo tanto, a mi entender, todo debería estar sujeto a la **RGPD** y dentro de poco a la renovada **LOPD**. El problema reside en que esta privacidad choca con el derecho de las organizaciones de monitorizar sus sistemas informáticos por seguridad. [1]

Respecto a este dilema, hemos podido observar que las últimas sentencias del **TEDH** (tribunal europeo de derechos humanos) dan mayor relevancia a la privacidad como derecho humano que al poder de las empresas de vigilar sus sistemas informáticos. Es decir, están dando a entender que el fin no siempre justifica los medios y que no todo vale para la seguridad, es necesario llegar a un equilibrio entre seguridad y privacidad. [2][3][4]

Queda patente que las legislaciones aún no están a la altura en este aspecto, recordemos que en España el 98,7% de las empresas de más de 10 empleados posee acceso a internet y 3 de cada 5 empleados usa ordenadores con fines empresariales según la encuesta sobre tecnologías de la información y las comunicaciones del Instituto Nacional de Estadística. Con ello podemos imaginar que todas estas personas son susceptibles de verse afectadas por el dilema de la seguridad contra la privacidad en el entorno laboral.

Algunos casos que han tenido gran repercusión pueden ser:

- **El caso de las cajeras:** Un supermercado fue condenado por el tribunal de Estrasburgo al no respetar la privacidad de dos de sus empleadas. Lo que sucedió en esta ocasión fue que el supermercado tenía fundadas sospechas de que las dos empleadas robaban, por lo que decidió instalar cámaras ocultas sin el conocimiento de estas empleadas para atraparlas “in fraganti”. Estas prácticas de vigilancia de empleados no están permitidas, por lo que prevaleció el derecho a la privacidad de las empleadas.
- El segundo caso es el de un trabajador rumano llamado **Barbulescu**, en esta ocasión, el empleador de este hombre espió los mensajes privados de Barbulescu que se habían realizado desde su cuenta de correo electrónico personal. En esta ocasión también prevaleció el derecho a la privacidad del trabajador.

Podemos ver en ambas situaciones que el derecho a la privacidad de los empleados se vio comprometida, lo que también tienen en común es que los empleados **no estaban informados** de los datos que el empleador tendría disponibles y además en ninguno de los casos se expresó **consentimiento explícito** por parte de los empleados.

De todo ello, podemos deducir que no es el fin de la monitorización de los empleados por parte de las organizaciones, sino que es una transición hacia

una monitorización mucho más informada y, sobre todo, lo más importante, consentida por el empleado.

La mayoría de estas técnicas se pueden realizar informando al empleado y si este las consiente de forma explícita, aun así, algunas de ellas no son aplicables si transgreden alguna otra norma o ley vigente. Por lo que podemos decir, que se tiene en cuenta tanto la privacidad de los empleados como la seguridad de las organizaciones, pero con un correcto **equilibrio entre ambas.**

Como parte de esta regla de información hacia los empleados, podemos ver también que se está produciendo un aumento de formación para los empleados a cerca del uso permitido y autorizado de los sistemas informáticos de las organizaciones. Gracias a estas medidas, se podrán minimizar las situaciones que causan controversia como el uso de los correos electrónicos profesionales para realizar actividades privadas. Ya que, muchas de estas actividades pueden no estar permitidas por la organización o ser limitadas.

Una de estas medidas de autorización de uso puede ser las políticas de uso, podemos encontrar un ejemplo de plantilla para utilizar como política de uso del email profesional propuesta en **Knowledge leader** , también ofrecen otras políticas relativas a los derechos de empleado y empleador. [5][6]

A su vez, en esta fuente, podemos encontrar un cuestionario de conformidad relativo a los derechos de ambas partes. [7]

Probablemente, en el futuro cercano, veamos nuevas regulaciones respecto a estos aspectos con medidas y legislaciones similares a la RGPD, pero mucho más enfocadas a los empleados. También aparecerá nueva regulación hacia la privacidad del empleado fuera del entorno laboral, es decir desconexión del trabajo fuera de horario laboral. [8][9]

Referencias:

[1] «Protección de datos y relaciones»- Expansión

http://www.expansion.com/blogs/sagardoy/2018/05/28/proteccion-de-datos-y-relaciones.html

[Consultado el 28/11/18]

[2] «Privacidad del trabajador»- El economista

https://www.eleconomista.es/empresas-finanzas/noticias/9013232/03/18/La-privacidad-del-trabajador-por-encima-de-la-proteccion-de-la-propiedad.html

[Consultado el 28/11/18]

[3] «Privacidad del trabajador»- 20minutos

https://www.20minutos.es/noticia/3291741/0/privacidad-trabajador-encima-proteccion-propiedad/

[Consultado el 28/11/18]

[4] «Derecho a la intimidad del trabajador»- Sanahuja miranda

https://www.sanahuja-miranda.com/es/blog/tiene-trabajador-derecho-intimidad-ambito-laboral

[Consultado el 28/11/18]

[5] «Plantilla política de email»- Knowledge Leader

https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/policiesproceduresemailpolicy

[Consultado el 28/11/18]

[6] «Plantilla políticas de los derechos del empleador y empleado»- Knowledge Leader

https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/policyemployerandemployeerights
[Consultado el 28/11/18]

[7] «Cuestionario de los derechos del empleador y empleado»- Knowledge Leader

https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/questionnairecomplianceoverviewemployeeemployerrights

[Consultado el 28/11/18]

[8] «Desconexión del trabajador»- El boletín

https://www.elboletin.com/noticia/167931/nacional/proteccion-de-datos-incorpora-el-derecho-a-la-desconexion-digital-fuera-del-trabajo.html

[Consultado el 28/11/18]

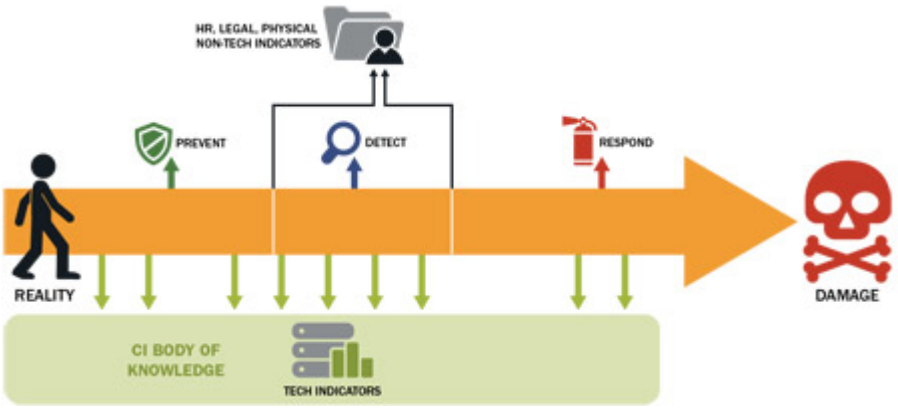
[9] «Desconexión del trabajador»- Informática jurídica

http://www.informatica-juridica.com/trabajos/derecho-desconectarse-la-proteccion-la-privacidad-del-empleado-frente-al-patrono-del-entorno-laboral/

[Consultado el 28/11/18]

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

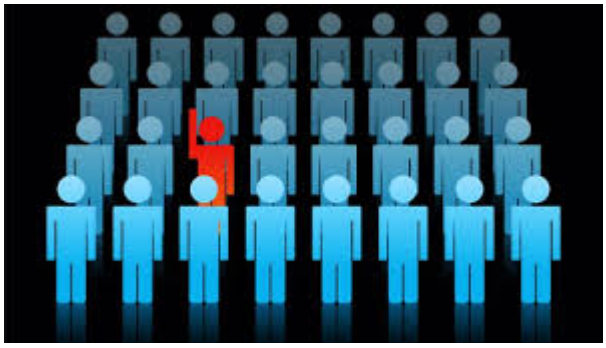
https://www.isaca.org/CYBER/CYBER-SECURITY-ARTICLES/Pages/5-layers-of-defense-that-prevent-insider-threats.aspx

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

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

Insider threat: Risks

Una vez que ya conocemos en que consisten las **amenazas internas** y su situación actual en las organizaciones, destinaré este tercer post a hablar acerca de los **riesgos** que llevan asociadas estas amenazas internas.



http://blog.ss8.com/controlling-insider-threats-through-visibility-analytics-and-intelligence/

Primero, me parece importante destacar como el riesgo de las amenazas internas es un concepto muy **difícil de precisar**, debido principalmente al impacto que tienen los distintos factores (los privilegios, autorizaciones o puesto de la persona). Es necesario, por lo tanto, **catalogar** este tipo de amenazas, tanto las conscientes como las accidentales. Es decir, si el insider threat de forma pasiva proviene del CEO de la compañía, podríamos encontrar un sinfín de riesgos asociados ya que tiene acceso prácticamente a toda la empresa y a información muy crítica.

En cambio, si la amenaza interna es por ejemplo algún miembro del servicio de mensajería, mantenimiento o limpieza, es posible que tengan mucho menos privilegios y por ende un menor acceso a los datos. Esto no quita a que también hay que tenerles muy en cuenta ya que debido a su perfil pasan más desapercibidos permitiéndoles entrar prácticamente sin que nadie sea consciente de ello.

Realizada está pequeña explicación, ahora me centraré en las **“High impact breaches”** o, dicho de otro modo, las grandes brechas de seguridad a las que estamos expuestos debido a las amenazas internas. [1]

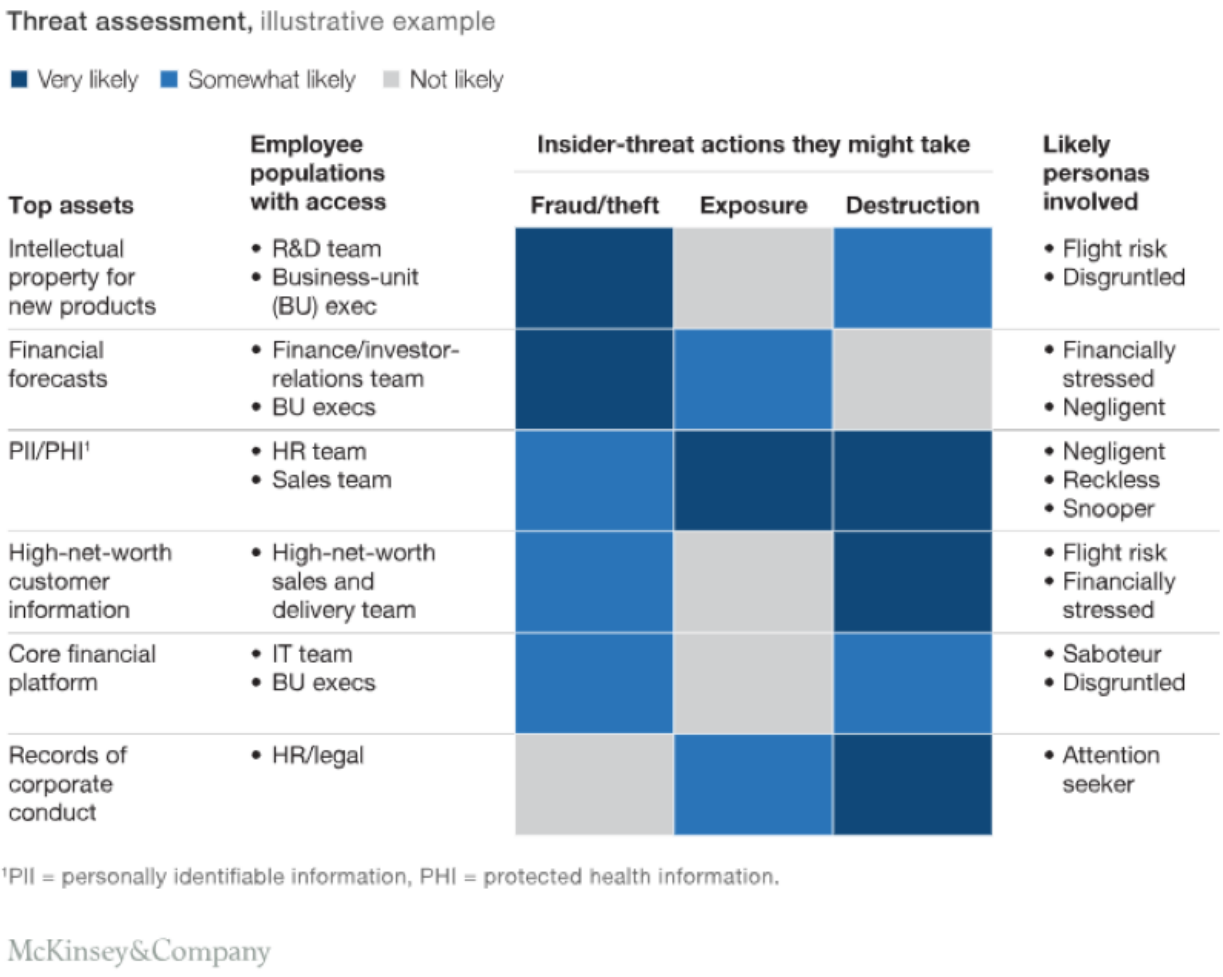
El primero puede ser el más evidente o esperado y es el **robo de información personal** que pueda identificar a una persona. Este afectaría en mayor medida a los insider threat que no son conscientes de que lo son. Si a estas personas se les roba esta información para suplantar su identidad, podría tener una gran repercusión para la organización y también para su reputación. Quiero comentar también que en este punto hay que tener mucho cuidado ya que según el **RGPD** estos datos deben seguir unas estrictas directrices de privacidad y conservación. Imaginemos que en vez de a un empleado de la empresa se la roban los datos personales a clientes de la empresa. En ese

caso podríamos estar sujetos a una gran **sanción** y a la correspondiente **mala reputación** que llevan asociados estos incidentes.

A su vez, es muy relevante mencionar que ahora las organizaciones deben **comunicar estas brechas** de seguridad en un **plazo máximo de 72h**. Esta legislación un claro ejercicio de transparencia pero que puede tener graves consecuencias para la imagen de las organizaciones.

El siguiente riesgo del que voy a hablar es el **sabotaje industrial**. Este en concreto posee una gran criticidad ya que podría causar estragos en la organización incluso a no poder recuperarse de ello.

El tercero que comentaré puede estar relacionado con el primero, en este caso será el **robo de información confidencial y propiedad industrial**. Para según qué tipos de organizaciones como puede ser las dedicas a sacar patentes, el robo de alguna de estas antes de ser aprobada podría suponer una gran pérdida para la empresa. También podrían darse casos de que se haga pública información confidencial. Este último escenario encajaría más en gobiernos y podría tener gran impacto en la geopolítica. Recordemos que en la actualidad los datos son considerados el activo más importante en las organizaciones como se puede apreciar en el siguiente gráfico elaborado por a consultoría McKinsey&co además de los distintos tipos de riesgos que corre cada activo fundamental.[2]



https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk#0

El cuarto es la **denegación de servicios**. En la actualidad gran parte de sus negocios tienen un volumen considerable negocio sustentado en internet, pero esto es un mal menor si comparamos lo que podría ocurrir si se realiza este ataque contra infraestructuras críticas como puede ser una central nuclear, una presa o a los satélites de un país. En definitiva, un riesgo muy a tener en cuenta.

El quinto que quiero mencionar es la **infección de software malicioso de forma extendida**. Como bien sabemos, hoy en día la mayoría de grandes y medianas empresas están informatizadas casi por completo y un malware que afecte a todos estos sistemas puede suponer un parón en el negocio con sus respectivas pérdidas y consecuencias. Pero esto es solo un escenario de la infinidad que se podrían dar. Por ejemplo, podríamos tener siempre a alguien dentro de los sistemas que pueda ver todo sin nosotros conocer que está ahí. O en un caso más extremo, ¿Qué pasaría si una persona consigue instalar y ejecutar correctamente un malware dentro de uno de los mayores bancos del mundo teniendo acceso a las cuentas de sus clientes?

El último de los riesgos que voy a comentar consiste en que los **sistemas de registros financieros se vean comprometidos**. Esto es particularmente crítico para grandes empresas que tengan que auditar de forma frecuente sus cuentas ya que si estos sistemas se ven comprometidos o inutilizados podrían causar que la auditoría no se lleve a cabo o que se haga de una forma incorrecta. Las consecuencias de que esto sucediese pueden ser grandísimas y tener un gran impacto en el mercado. Dentro de este riesgo, podemos destacar el papel fundamental que juegan los auditores TI asegurando la integridad de los sistemas y datos para la posterior auditoría financiera.

Como hemos podido observar, estos riesgos asociados tienen un gran impacto para las organizaciones de ahí el concepto que he mencionado al principio “high impact breaches”. Por lo tanto, podemos ver porque **las organizaciones están tan preocupadas** por tener un correcto plan de gestión de las amenazas internas y cada vez están más concienciadas de ello.

En el próximo post trataré de explicar y analizar las principales medidas que toman actualmente las empresas para conseguir prevenir o mitigar este tipo de riesgos. [3]

Referencias:

[1] “Types of insider threats” – Security intelligence

https://securityintelligence.com/these-5-types-of-insider-threats-could-lead-to-costly-data-breaches/

[Consultado el 22/11/18]

[2] “Human element of cyberrisk”- Mckinsey&Co

https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk#0

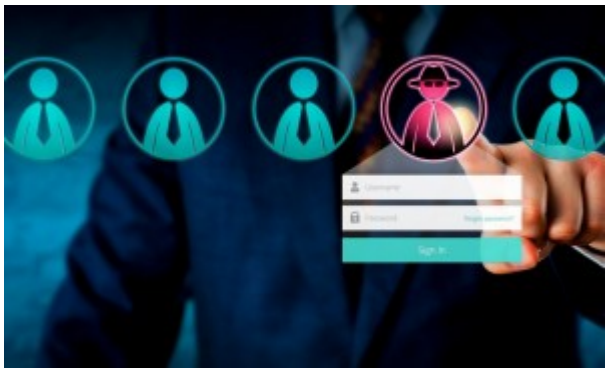
[Consultado el 22/11/18]

[3] “Managing insider threats” – EY

https://www.ey.com/Publication/vwLUAssets/EY-managing-insider-threat-a-holistic-approach-to-dealing-with-risk-from-within/$FILE/EY-managing-insider-threat.pdf

[Consultado el 22/11/18]

Últimas tendencias en los insider threats



https://130e178e8f8ba617604b-8aedd782b7d22cfe0d1146da69a52436.ssl.cf1.rackcdn.com/mitigating-insider-threat-lessons-from-indian-fraud-case-showcase_image-4-a-10674.jpg

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]

Insider Threats, el principal riesgo para las empresas

https://www.information-age.com/manage-mitigate-insider-threats-123469477/

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]