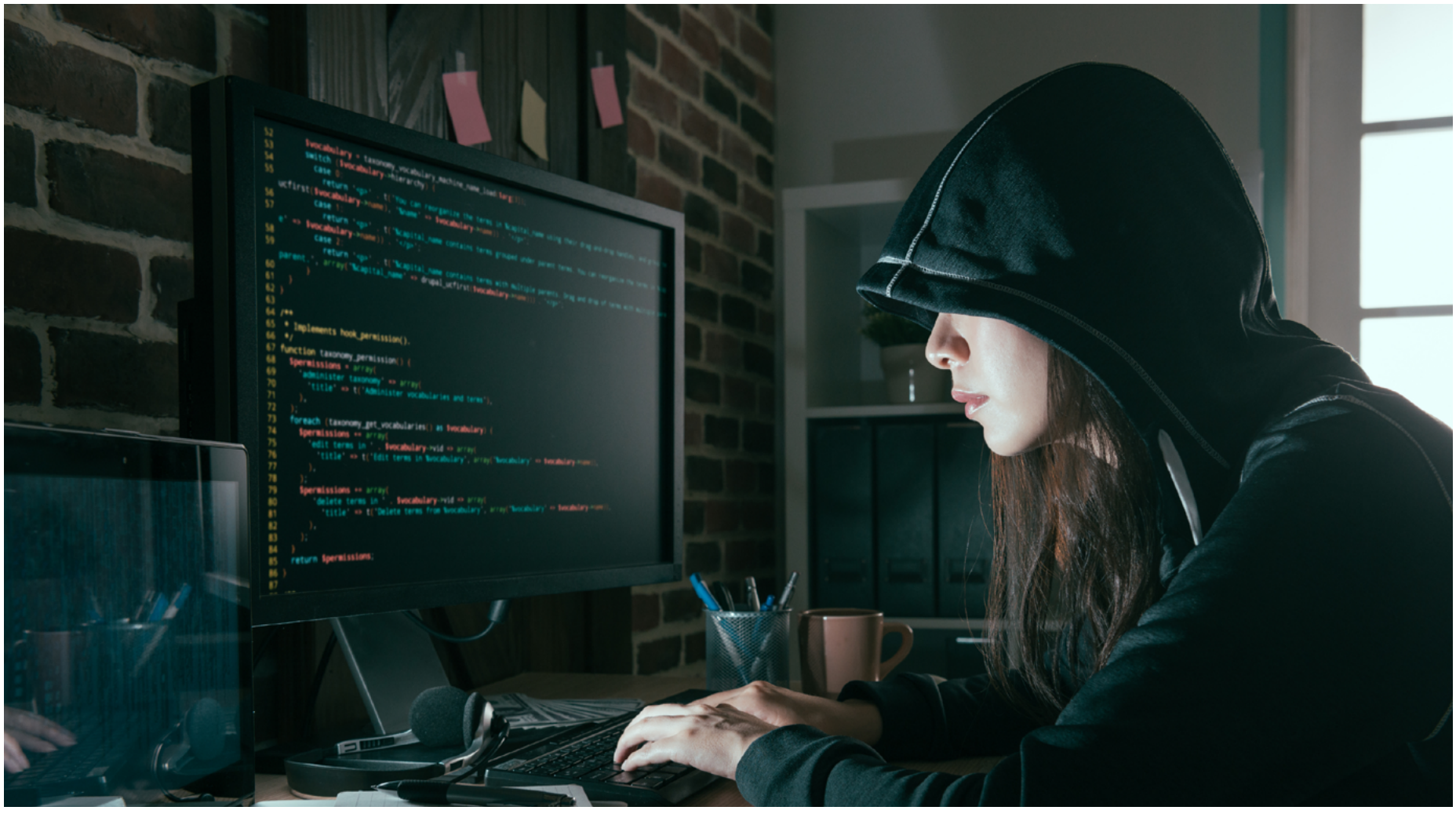
THREATSCOUT®

N.03
Febrero, 2021

Enemigo en casa: Psicología del infiltrado y su impacto en la organización.



Extracto

El infiltrado o ‘insider’ se refiere al empleado, exempleado, contratista, etc. que utiliza sus privilegios de acceso, autorizados por una organización, para comprometer, exfiltrar y/o sabotear esa misma organización. Ante el incremento de la participación interna en buena parte de los principales incidentes de fraudes cibernéticos recientes, creemos prioritario explorar las causas de este fenómeno y las aproximaciones para establecer un plan preventivo.

Introducción: ¿Cómo nos pudo pasar a nosotros?

¿Cuántas veces hemos oído a gerentes generales y directores de empresas decir que dentro de sus organizaciones reina el respeto, la armonía y el orgullo de pertenecer a ese grupo? ¿Cuántas veces no hemos oído decir a esos mismos líderes empresariales que las inversiones realizadas en seguridad física y cibernética están a la altura de estándares internacionales y en consecuencia están poco menos que blindados ante posibles ataques cibernéticos?

Pero ¿y qué pasa cuando esos ataques se organizan internamente con la participación de uno o más de esos empleados que -hasta hace minutos- vivían con respeto, armonía y orgullo por la organización?

Según un reciente estudio realizado por el Ponemon Institute y financiado por ObservelT e IBM[1], se concluye que desde el 2018 hasta mediados del 2020 ha habido un incremento del 47% de casos de ciberseguridad con participación de infiltrados o ‘insiders’.

Pero a partir de este año, 2021, gracias a la aceleración de los procesos de digitalización cortesía del COVID 19, también crecerán las estadísticas de ciberdelitos especialmente en áreas cómo: suplantación de identidad, secuestro de datos vía ransomware, exfiltración de data sensible para su comercialización en foros del darkweb y metodologías más complejas de ingeniería social para permear organizaciones con mayores niveles de protección informática.

Sin embargo, la máxima que repetimos en nuestros talleres de concientización de ciberseguridad avanzados se mantiene: “¿para qué invertir horas hombre en la evaluación de vulnerabilidades de una arquitectura de seguridad compleja, cuando puedes invertir mucho menos evaluando redes sociales de un individuo específico que te puede garantizar el acceso o, en el peor de los casos, la posibilidad de escalar privilegios para llegar al objetivo primario?”.

1 https://www.observeit.com/cost-of-insider-threats/

Pero ¿y el infiltrado dónde participa en esta dinámica? Se preguntará con ansias nuestro apreciado lector. Pues depende de las circunstancias. Existen multiplicidad de causas por las cuales un empleado puede convertirse en un infiltrado.

Tres tipos de infiltrados son los que nos deben preocupar:

TIPO	RAZÓN	IMPACTO
Infiltrado por selección o reclutamiento	Individuo captado por bandas criminales organizadas y/o actores adversariales extranjeros (APT) por sus privilegios de acceso a información sensible y/o activos críticos de una organización. Se pueden detectar por asociación y/o cambios en el estilo de vida.	Espionaje comercial, fraude continuado, generación de identidades sintéticas (perfiles falsos) para vulnerar asociaciones estratégicas, exfiltración de data sensible tanto corporativa como del personal directivo para delitos de secuestro, extorsión, etc.
Infiltrado por descontento /insatisfacción o problemas con terceros dentro de la organización.	Este tipo de individuos son impredecibles y representan un riesgo inminente dentro de sus competencias laborales. Sin embargo, son más fáciles de detectar por su comportamiento, cambios de conducta con sus compañeros entre otras señales.	Robo de propiedad intelectual, sabotajes cibernéticos (especialmente en casos de individuos con conocimientos técnicos avanzados), exfiltración de información sensible (bases de datos, etc.) para su venta o exposición pública, así como otros riesgos asociados.
Infiltrado o 'insider' no intencionales	Se refiere a aquellos individuos que filtran información sensible de manera no maliciosa, accidental y/o por desconocimiento. Si bien esta clase de individuos no representa un daño sistémico como los dos anteriores, es el caso más común dentro de las grandes organizaciones.	Revelar información confidencial -vía internet- a terceros por error, mal manejo en la destrucción física de información confidencial, pérdida de laptops, USB, teléfonos inteligentes, inadvertencia de controles específicos que procuran brechas de seguridad, etc.

Los infiltrados, en cualesquiera de sus tipos, representan un porcentaje importante de la totalidad del riesgo proyectado dentro de una organización. Si tomamos en cuenta que más del 90 % de los ataques cibernéticos requieren de la interacción humana para su éxito[2], entonces debemos factorizar la probabilidad de un infiltrado o 'insider' en alguna de las etapas de un incidente.

Se trata de reflexionar con una mentalidad enfocada a la seguridad general de una organización: ¿tenemos bases de datos que podrían ser de interés de la competencia o de algún gobierno extranjero y que podrían ser robadas, exfiltradas o manipuladas por algún empleado nuestro? ¿Un empleado considerado de confianza podría infiltrar un código malicioso en nuestra organización? ¿Acaso pudiera suceder que algún empleado, socio o contratista esté planificando robar información confidencial para negociar una posición laboral con la competencia?

Estas y otras interrogantes son las que deben evaluarse en el marco de una estrategia moderna de prevención que asuma el factor humano dentro del componente de seguridad cibernética como un elemento de planificación, facilitación, transporte y negociación de activos o información sensible...porque las respuestas a esas interrogantes anteriores, es un rotundo: Sí.

Psicología de infiltrado o 'insider': ¿Cómo es que no pudimos atar los cabos?

Encasillar a un infiltrado o 'insider' dentro de un perfil psicológico único, es una imposibilidad debido que cada caso es particular. Ciertamente en casos de espionaje, los estudios psiquiátricos más reconocidos, como los del Dr. David L. Charney[3], apuntan que los rasgos repetidos en los sujetos estudiados es la personalidad 'narcisista y antisocial', pero no son todos.

En nuestros talleres de TEKIUM sobre contrainteligencia e 'insiders' explicamos que el proceso en el cual un empleado/ejecutivo/socio/etc. se transforma en un infiltrado es un puente (de lealtad a deslealtad) que transcurre con la capacidad que tiene un individuo para lidiar con factores de estrés personales, estructurales y laborales versus la capacidad de la organización de reconocer y reaccionar (o no reconocer y en consecuencia no reaccionar) ante los indicios/signos que el empleado deja a su paso.

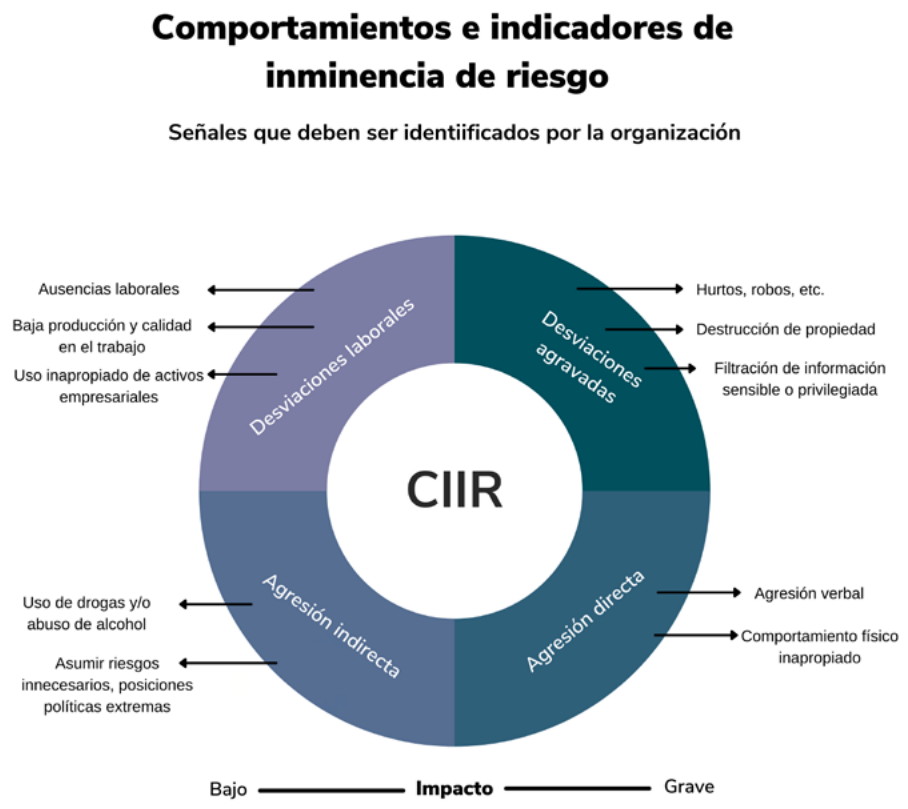
¿Qué rasgos podrían categorizar a un potencial infiltrado?

Generalmente presentan algunos, todos o una combinación de los siguientes:

- Recientes frustraciones sociales o personales.
- Flexibilidad ética.
- Lealtad reducida, condicionada o confinada a su persona y no a ideales.
- Percepción constante de sentirse con privilegios ante algo o creer la necesidad de recibir merecimientos de forma sistemática.
- Falta de empatía con compañeros de trabajo.
- Problemas con la autoridad. Incapacidad de reconocer errores frente a sus superiores y achacárselos a otros.
- Constante búsqueda de apoyo, entre colegas, para justificar una posición que generalmente es contraria a la de la superioridad.

El problema empieza a agravarse cuando la organización no reconoce estos comportamientos entre alguno de sus empleados porque ello puede reforzar la sensación de privilegiado del potencial infiltrado o 'insider', al tiempo que el individuo sienta una reducción de la responsabilidad por sus acciones.

En la figura 01 podemos observar una serie de comportamientos e indicadores de inminencia de riesgo (CIIR)[4] en los que pueden incurrir los potenciales infiltrados o 'insiders' previo a la realización de un acto de deslealtad o delito.



2 https://www.proofpoint.com/es/resources/threat-reports/human-factor

3 David L. Charney, "True Psychology of the Insider Spy," Intelligencer: Journal of U.S. Intelligence Studies (Fall/Winter 2010): 47-54. Available at https://bit.ly/2Nzo5QW

4 El CIIR proviene de una adaptación de estudio de: Paul R. Sackett, and Cynthia J. DeVore, "Counterproductive Behaviors at Work," in Handbook of Industrial, Work & Organizational Psychology, Volume 1: Personnel Psychology, edited by Neil Anderson, Deniz S. Ones, Handan Kepir Sinangil, and Chockalingam Viswesvaran (London: SAGE Publications, 2005): 145-164.

De acuerdo con las investigaciones que se han realizado en el campo de comportamiento contra-productivo laboral, y que lleva al desarrollo del modelo de inminencia de riesgo, hay tres elementos claves que se desprenden de los estudios:

Existe un patrón de ocurrencia respecto al comportamiento e indicadores de inminencia de riesgo (CIIR): los individuos que incurren en una desviación o agresión de bajo impacto suelen repetir el comportamiento.
El CIIR -generalmente- escala: El individuo que incurre en una desviación o agresión de bajo impacto tiende a escalar a comportamientos o agresiones más severas, por lo que es vital que existan mecanismos de supervisión para mitigar esta situación.
Los CIIR no ocurren de forma espontánea: factores de estrés en el hogar o en el trabajo actúan como detonantes para generar los comportamientos o agresiones que, de no ser identificadas de forma temprana, pueden traer serios problemas a una organización.

Es importante recordar que no existe un perfil psicológico o demográfico para categorizar un infiltrado o 'insider'. Las características más significativas o indicadores potenciales de riesgo para su identificación son los patrones de comportamiento: sus variaciones y/o cambios bruscos.

Todos vivimos frustraciones en nuestros trabajos, pero -en su mayoría- tenemos la resiliencia interna para superar esas experiencias. El problema es cuando hay una confluencia de factores negativos.

Por ejemplo, unas expectativas laborales insatisfechas pueden ser razón para considerar una queja, pero no para traicionar a la empresa. Sin embargo, unas expectativas laborales insatisfechas, la percepción de estancamiento potenciadas con problemas extra-laborales tales como temas maritales, enfermedades, problemas económicos y adicciones, pueden perfectamente empujar a un empleado a cometer delitos dentro de la organización.

Si no consigue mecanismos para deslastrar la presión y el apoyo necesario para evaluar de forma independiente su situación, sus problemas se convierten en obsesión y las soluciones más sencillas, aunque drásticas, son aquellas que están al alcance del individuo de una forma inmediata.

Al llegar a este punto, el individuo puede reaccionar de forma antisocial y/o planificar vengarse de la organización que `no lo ha compensado adecuadamente' infligiéndole un daño directo o buscando un beneficio personal que lo haga sentir compensado según su percepción (a veces ambas).

Es allí es cuando se inicia la fase de concepción (la idea) del delito pero que en su mente lo justifica como venganza o compensación merecida. ¿Qué sigue? La planificación para lograr la exfiltración de propiedad intelectual, información confidencial del personal o corporativos, sabotaje cibernético, etc. En otras palabras: se desencadena un potencial enemigo interno.

La mitigación de riesgo de in-filtrados o 'insiders': ¿y ahora cómo hacemos?

La firma www.statista.com, publicó en enero de este año, su último estudio referente a los incidentes más comunes relacionados con infiltrados o 'insiders' durante el 2020. Las estadísticas, basadas en un universo de 300 encuestados pertenecientes a 8 sectores diferentes, son muy llamativas y podrían proyectarse -con cautela- al ámbito mexicano dado que no hay estadísticas locales de incidentes con participación de infiltrados o 'insiders'.

Los seis renglones con valor estadístico fueron: exfiltración de información sensible con 62% del total de incidentes reportados; abuso de privilegios con 19%; snooping (intentos de obtener información privilegiada de forma furtiva) y agregación de data para formar bases de datos no autorizadas con 9.5%; sabotaje de infraestructura con 5.1%; intentos de evasión de controles de seguridad de la información con 3.8% e incidentes de cuentas empresariales compartidas con 0.6% del total de incidentes recabados.

Estas estadísticas demuestran que la exfiltración de información confidencial es el incidente más recurrente, probablemente por la demanda de la información, la falta de mecanismos de prevención orientados a delitos internos y la facilidad de ocultar o disimular su extracción (vía internet, USB, de forma física, etc.).

De acuerdo con CERT (Computer Emergency Response Team) del Software Engineering Institute de la Universidad Carnegie Mellon en los Estados Unidos, hay 16 buenas prácticas que coadyuvan a la detección y prevención de la amenaza del infiltrado o 'insider':

1. Durante las evaluaciones periódicas de riesgo corporativo, hay que factorizar el riesgo de infiltrados (empleados y/o socios comerciales) como un elemento adicional.
2. Se debe documentar de forma clara cuales son las políticas y controles internos para prevenir y/o mitigar este riesgo. Esta información debe permear transversalmente la organización de manera que todos estén informados y así evitar confusiones y/o desconocimiento de las políticas.
3. Se sugiere instaurar un programa de capacitación periódica -para todos los empleados- sobre los riesgos colectivos de esta clase de incidentes, su detección y mecanismos de reporte.
4. Es muy importante tener un mecanismo de monitoreo de comportamiento sospechoso o disruptivo que se inicie desde el proceso de selección.
5. Estructurar prácticas de 'anticipación y gerencia' de incidentes laborales contra-productivos o negativos.
6. Monitorear y asegurar los espacios físicos mediante diferentes controles.
7. Implementar controles y políticas estrictas de contraseñas y gerencia de cuentas de email corporativas.
8. Establecer separación entre tareas y privilegios. No asignar a personas con privilegios limitados a tareas que no le corresponden por acceso.
9. Considerar el riesgo de infiltrado o 'insider' en el ciclo de vida del desarrollo de software.
10. Caución con los administradores del sistema y usuarios técnicos o privilegiados.
11. Implementar alarmas o notificaciones al momento de cambios -no autorizados- dentro del sistema.
12. Registre, monitoree y audite las interacciones online de sus empleados.
13. Use defensas de separación por capas (layered) contra ataques remotos.
14. Desactive el acceso a computadoras de empleados que sean separados de sus cargos.
15. Implemente procesos de backup seguros y recuperación de data.
16. Desarrolle un plan de respuesta de incidentes para el caso de infiltrados o 'insiders'.

En Tekium, creemos que vendría bien un ejercicio de prospectiva sobre la evolución que podría presentarse -a corto plazo- de los incidentes que involucran a personal infiltrado o 'insiders' dentro de una organización.

La exfiltración de información sensible está obviamente en el tope de los incidentes. Para esta clase de delitos, generalmente existe colusión con individuos externos que tienen interés en esa información y que están dispuestos a ofrecer una contraprestación por el riesgo de extraerla. Otra opción es que el infiltrado quiera sabotear la organización y filtrar la información de forma pública a sabiendas de las consecuencias, daño reputacional y posibles retaliaciones.

Pero si tomamos como ejemplo el primer caso de colusión, también podríamos anticipar eventuales acciones de desinformación inyectados de forma maliciosa dentro de los procesos internos de la organización por parte de ese mismo empleado. Imagínese planificar la adquisición de una empresa con información errónea obtenida y presentada como fidedigna por empleados de ´confianza o socios´. Suponga que su planificación estratégica anual está basada en información incorrecta alimentada desde lo interno de la organización para favorecer a la competencia. ¿Tenemos un proceso de contrainteligencia que permita detectar este tipo de acciones o simular incidentes que vulneren la planificación interna con fines de sabotear financieramente la organización?

¿Acaso la exfiltración sistemática y progresiva de datos personales de gerentes, socios o personal considerado como 'especial' por sus privilegios no obedece a un plan bien concebido para permear una organización desde afuera?

Obvio, existe el infiltrado o 'insider' que provee la inteligencia necesaria, pero convencer a ese infiltrado de coludir con un grupo externo es mucho más fácil cuando se le explica que la data será utilizada para una operación de ingeniería social que para un secuestro o una extorsión. ¿Cierto verdad?

Acá tocamos un punto verdaderamente álgido pero recurrente. La relación entre infiltrados o 'insiders' e ingeniería social. Lo notable es que este acercamiento pareciera que va a crecer por dos razones:

A. Lo atractivo de una propuesta – que suena casi inofensiva- de obtener información personal de un objetivo por dinero con la promesa que el objetivo sólo será atacado cibernéticamente para extraerle fondos. En otras palabras, cero daños físicos, nulo contacto personal, bajas probabilidades de ser identificados y menos de ser enjuiciados.
B. El uso de infiltrados o 'insiders' por una estructura criminal en una empresa, facilita la comprensión de su funcionamiento, las medidas de seguridad y la

identificación de los individuos claves para ser atacados en una operación de ingeniería social. No necesariamente tienen que ser un ejecutivo o director, quizás el 'insider' provee información de un gerente junior quien es el administrador del sistema con manejo de claves. El punto es que develar esa operación (¿cómo se vulneró el sistema?; ¿quién proveyó la información?; ¿estaba bajo coacción o fue vulnerado por intermedio de una operación de ingeniería social?; etc.) es muy complicado y los riesgos que corre el infiltrado que proveyó la inteligencia, son marginales.

En este sentido, nosotros combinaríamos las 16 buenas prácticas sugeridas por el CERT de Carnegie Mellon contra amenazas de infiltrados o 'insiders' con 5 buenas prácticas para mitigar un ataque de ingeniería social:

1. **Aprenda a identificar un ataque de ingeniería social.** Esto se logra a través de talleres de capacitación y charlas especializadas.
2. **Mantenga su programa de concientización de ciberseguridad al personal de su organización.** Actualice los contenidos de acuerdo con los riesgos que sean detectados tanto en el entorno empresarial donde usted se desempeñe, como por las últimas técnicas identificadas por internet.
3. **Identifique y genere conciencia sobre la información de valor que podrían tratar de obtener vía ingeniería social.** ¿Qué tipo?; ¿Por qué es más probable atacar un departamento que otro?; ¿Quién es más vulnerable a sufrir un ataque y cómo podemos blindarlo?; etc.
4. **Mantenga los softwares de su compañía actualizados.** ¡Por favor! ¡Por favor!
5. **Realice auditorías de ingeniería social.** Aprenda de estos ejercicios para evaluar vulnerabilidades vistas desde el exterior.

Ya en un próximo trabajo profundizaremos en el impacto que tendría para una organización otros tipos de operaciones maliciosas que serán más comunes en el futuro tales como: operaciones de desinformación como enlaces de ingeniería social, sabotajes de bajo impacto para encubrir operaciones de mayor envergadura y el uso de identidades sintéticas con IoT.

CONCLUSIÓN: ¿alguna buena noticia?

El potencial riesgo que representa un infiltrado o 'insider' dentro de una organización es muy difícil de predecir. Basta con pensar que mientras más acelerada y profundos sean los procesos de digitalización de una empresa, mayor el riesgo de exfiltración de información sensible.

En el último reporte de la compañía de seguridad informática y una de las pioneras en detección de riesgo de infiltrados, CODE 24 (2021 Data Exposure Report)[5] se observan las siguientes tendencias:

A. Los empleados son más propensos a filtrar información confidencial ahora, que en tiempos pre COVID (28% de casos entre las empresas encuestadas previa pandemia versus 52% post pandemia).

B. Los líderes en seguridad de la información encuestados informaron que el riesgo que suponen los infiltrados y los empleados 'descuidados' representan las principales causas para la filtración de data sensible por encima de ataques externos. Pero que sólo un promedio del 20% de los presupuestos de ciberseguridad fueron invertidos en prevención de riesgo de infiltrados o 'insider'.

C. Cada 6 de 10 líderes de seguridad de la información encuestados considera que el riesgo infiltrados va a incrementar (o va a incrementar mucho) en los próximos 2 años.

D. 118 días es el promedio que se tarda en identificar una fuga de información. 55 días aproximadamente para contener los efectos/impacto de la fuga y 6 meses promedio para la investigación y remediación.

E. Menos de la mitad de las empresas encuestadas (46%) tienen un plan de prevención de riesgo de infiltrados o 'insiders'.

Si, pareciera que es un problema irreversible, difícil de detectar y aún más complicado de aceptar (no es fácil asumir que cualquier empleado, sin importar su cargo, podría convertirse en un infiltrado o 'insider'), pero es una realidad y, por ejemplo, para el sector financiero basta con navegar en el Dark Web, en un foro llamado: carding21, para entender el problema real que hay con infiltrados dentro de la banca (específicamente con ejecutivos de sucursales).
Pero este problema se puede mitigar. Teniendo programas de indicadores de riesgo que alerten sobre:

A. Individuos que trabajen a deshoras constantemente
B. Monitoreo de individuos con acceso periódico/diario/eventual a información o proyectos confidenciales,
C. Monitoreo de actividades de individuos que renuncien o sean despedidos
D. y un mecanismo de alerta temprana para identificar empleados con comportamientos extraños, agresivos y/o retraídos de manera de ofrecer apoyo psicológico y administrativo.

Estas son algunas iniciativas básicas para mitigar este riesgo, pero el problema no va a desaparecer, por el contrario, va a incrementarse por las razones anteriormente expuestas.

¿Cuánto hay que invertir para controlar este flagelo? Pues

5 http://bit.ly/3siEh7V

dependerá de la evaluación que habrá que realizar. Nuestra sugerencia: haga una evaluación de potencial riesgo de infiltrado o 'insider', evalúen sus mecanismos de contrainteligencia e implementen un programa de contención del riesgo por infiltrados o 'insiders'.

Es preferible ser proactivo. El costo de un infiltrado en la organización podría representar mucho más que pérdida de dinero, filtración de estrategias comerciales y daños reputacionales.

Tener un programa de prevención podría ser la diferencia entre la vida y la muerte porque un empleado con problemas, bajo presión y temas colaterales cómo adicciones, podría explotar en el lugar de trabajo -por cualquier razón- con consecuencias impredecibles...

Para más información:

Acerca de Nosotros

Somos un equipo de expertos en ciberseguridad, apasionados por innovar y desarrollar soluciones para contrarrestar retos y riesgos del entorno digital. Creemos en una evolución digital constante que, paralelamente, requiere de capacidades específicas para cerrar paso a quienes hacen el mal.

Nuestra manera de hacer esto, y lo que nos motiva a diario, es poder brindar a empresas la tranquilidad de dejar su ciberseguridad en nuestras manos.

TEKIUM

Avenida Patriotismo #767, piso 7. San Juan Mixcoac, C.P 03730. Ciudad de México.