LA FUNCIÓN DEL DEPARTAMENTO DE RECURSOS HUMANOS EN LA PREVENCIÓN DE AMENAZAS DE AGENTES INTERNOS

DESCRIPCIÓN GENERAL

Las amenazas de agentes internos constituyen un reto dinámico y en constante evolución para las organizaciones. Los profesionales de Recursos Humanos (HR, por sus siglas en inglés), junto con sus homólogos de seguridad, desempeñan un papel integral en el desarrollo y la contribución a los equipos de gestión de amenazas multidisciplinarios para detectar, disuadir y mitigar eficazmente las amenazas de agentes internos.[1] Como repositorio central de información del personal, es probable que los profesionales de HR identifiquen patrones, comportamientos y tendencias que ayudarán a mitigar los posibles daños a una organización y sus empleados. Dependiendo del tipo y tamaño de la organización, las pérdidas financieras y de reputación asociadas con las amenazas de agentes internos podrían costar millones al año.

Una amenaza de agentes internos se puede tratar de un empleado actual o anterior, un socio comercial o un contratista que intencionada o involuntariamente causa daño a una organización y su personal utilizando métodos físicos o cibernéticos:

Violencia: Terrorismo y violencia en el lugar de trabajo.

Espionaje: Robo de la propiedad intelectual de una empresa asociada a la seguridad nacional.

Amenaza cibernética: Intrusiones intencionadas o no intencionadas que violan o exponen la infraestructura de tecnología de la información de una organización.

Sabotaje: Actos físicos o cibernéticos que repercuten en la capacidad de una organización para funcionar mediante subversión, obstrucción, interrupción o destrucción.

Robo: Robo de propiedad física, propiedad intelectual y/o información financiera de una organización.

POSIBLES INDICADORES

Las amenazas de agentes internos, ya sean por causas negligentes o maliciosas, plantean graves riesgos de seguridad para una organización. La capacidad de evaluar, identificar y mitigar de forma proactiva los problemas del personal es crucial para garantizar un lugar de trabajo seguro. Conocer y reconocer las señales de advertencia que plantean los agentes internos malintencionados es fundamental para la prevención y la mitigación. Estas posibles señales o indicadores de advertencia pueden incluir, entre otros:

- Conflictos con compañeros de trabajo o supervisores; infracción empedernida de las políticas organizacionales.
- Incumplimiento de las tareas obligatorias de capacitación en seguridad.
- Medias disciplinarias: suspensiones, amonestaciones, destituciones o reducciones de título o sueldo.
- Uso de las redes sociales para amenazar a la organización o a su personal.
- Factores estresantes observables o verbalizados, que pueden incluir expectativas personales, profesionales, financieras o insatisfechas que podrían aumentar el riesgo de que un agente interno emprenda acciones hostiles o malintencionadas.

DATOS Y ACONTECIMIENTOS

- Entre 2019 y 2022, mientras trabajaba como gerente de rehabilitación en un hospital local, un gerente del hospital utilizó una tarjeta de crédito corporativa para realizar compras no autorizadas de tarjetas de crédito prepagas y de regalo. A continuación, transfería fondos de las tarjetas obtenidas fraudulentamente a sus cuentas personales para ocultar la estafa, realizar compras personales y retirar grandes cantidades de efectivo para jugar en casinos. En ese periodo se robaron y blanquearon más de $607,000 dólares.

- Desde junio de 2021 hasta mayo de 2023, un empleado de un departamento del orden público de la ciudad robó cheques, incluidos cheques pagaderos a la división de compensación laboral del departamento de asuntos legales. A continuación, pasó esos cheques a otras personas, quienes depositaron o intentaron depositar versiones falsificadas, alteradas y endosadas de forma fraudulenta de esos cheques en cuentas bancarias de terceros. Aproximadamente 40 cheques, por un total de aproximadamente $600,000, se robaron y depositaron como parte de la estafa.

- En abril de 2021, ocho personas murieron en un tiroteo masivo perpetrado por un antiguo empleado en unas instalaciones de transporte de Indianapolis (Indiana). Un año antes, la madre del antiguo empleado contactó a la policía para informar que, según el FBI, podría intentar “suicidarse a través de la policía”.

1 Un equipo de gestión de amenazas es un órgano de gobierno multidisciplinario que incluye representantes de HR, tecnología de la información, seguridad de la información, seguridad física, departamentos de asuntos legales y otras entidades que se centran en identificar, evaluar y mitigar posibles amenazas de agentes internos.

ESTRATEGIAS DE MITIGACIÓN Y MEDIDAS DE PROTECCIÓN DEL DEPARTAMENTO DE RECURSOS HUMANOS

Los profesionales de HR deben establecer un marco de evaluación que incluya indicadores de amenazas y señales de comportamiento. Los departamentos de HR desempeñan un papel fundamental, ya que intervienen en todas las fases del ciclo de vida laboral de un empleado: antes de la contratación, durante la contratación y después de esta.

ACCESO, PLANIFICACIÓN Y PERSONAL

Precontratación (selección y contratación)

- Investigar las señales de alerta durante el proceso de entrevista, pero tenga cuidado de no infringir las leyes de privacidad relevantes o las leyes sobre antecedentes penales “ban the box” (protecciones estatales para los posibles empleados condenados por un delito contra la descalificación automática).
- Verificar la exactitud del currículum vitae y las referencias de contacto de un posible empleado.
- Detectar posibles indicadores negativos, entre ellos:
  - Actividad delictiva pasada y relevante (por ejemplo, realizar verificaciones de antecedentes penales)
  - Denuncias de violencia en el pasado
  - Historial de infracción de políticas

Empleo (incluidos ascensos y reasignaciones)

- Realizar capacitaciones rutinarias y obligatorias sobre concientización sobre seguridad física y ciberseguridad contra amenazas de agentes internos.
- Comunicar políticas organizacionales claras y seguir los procedimientos establecidos.
- Crear mecanismos para que empleados y gerentes aporten comentarios de forma recíproca y compartan sus inquietudes.
- Establecer una línea base de comportamiento normal tanto para los empleados como para las redes de TI para ayudar a identificar cambios significativos, incluida la supervisión de la actividad de la red para detectar actividades peligrosas o inapropiadas.
- Crear una cultura de responsabilidad compartida, conexión y respeto asegurándose de que las denuncias de los testigos se valoren y se traten con discreción, al tiempo que hace hincapié en que el objetivo es ayudar a sus compañeros de trabajo.
- Abordar posibles quejas.
- Identificar e informar sobre cambios de comportamiento al Equipo de gestión de amenazas y a los departamentos correspondientes.

Cese/ despido

- Entregar las notificaciones de despido con respeto y de manera que se reduzcan al mínimo la intromisión y la vergüenza.
- Realizar una entrevista al dejar el puesto de trabajo para evaluar la perspectiva del empleado que se desvincula.
- Tener un plan para recuperar las pertenencias de los empleados y poner fin a su acceso físico y digital.
- Establecer un procedimiento para informar a los demás empleados cuando se produce el despido.
- Revisar los acuerdos de propiedad intelectual/no revelación de información con el empleado desvinculado.
- Tratar al empleado que se desvincula con dignidad y profesionalismo

RECURSOS ADICIONALES PARA PROPIETARIOS Y OPERADORES

Para obtener asistencia regional directa, visite www.cisa.gov/about/regions.

Para obtener recursos adicionales sobre amenazas de agentes internos y otros productos e información sobre seguridad de infraestructura, visite cisa.gov/insider-threat-mitigation.