proofpoint.

LIBRO ELECTRÓNICO

Los parámetros que importan:

Guía del CISO para evaluar, priorizar y justificar presupuestos de ciberseguridad adaptados a la empresa

proofpoint.com/es

SECCIÓN 1

De chivo expiatorio a estratega

Para comprender en qué medida ha evolucionado la función del CISO en los últimos años, basta leer el testimonio de un ejecutivo en una reciente mesa ronda de Proofpoint.

"Cuando empecé en el sector, la función del CISO se parecía a la de un chivo expiatorio", recuerda. La dirección necesitaba a alguien a quien culpar si las cosas iban mal. Pero la mayoría de las veces, daban prioridad a las pólizas de seguros genéricos frente a las inversiones en equipos y soluciones de seguridad. En otras palabras, los CISO eran expertos en tecnología que disponían de recursos limitados.

Pero las cosas están cambiando. Las amenazas son cada vez más complejas y pueden afectar a mucho más que a un pequeño número de sistemas de una empresa. Y cuando los ciberataques se convierten en fugas de datos masivas, pueden dañar o destruir una marca.

Esto ha cambiado la forma en la que la dirección considera las inversiones en ciberseguridad, y el papel del CISO. Ahora los consejos de administración prestan mucha más atención a lo que hacen los CISO. Y como indica el término "Jefe" (Chief) de su título, los CISO está estrechamente involucrados en la estrategia global de la empresa. Cada vez con mayor frecuencia, contribuyen a diseñar la transformación digital de una forma que afronte los riesgos, optimice los procesos empresariales y reduzca pérdidas evitables.

"Cuando empecé en el sector, la función del CISO se parecía a la de un chivo expiatorio".

Nuevos desafíos entrañan nuevos costes

Esta evolución viene acompañada de nuevas necesidades presupuestarias. Según un estudio reciente de Forrester, el 60 % de los responsables de la toma de decisiones de seguridad de la empresa aumentaron sus presupuestos de seguridad en 2020[1].

Y los que no gastan más intentan estirar al máximo los fondos de los que disponen. Los presupuestos de ciberseguridad actuales hacer frente a varios desafíos:

- Evolución de las normativas y requisitos
- Migración progresiva a la nube
- Adopción repentina de modelos de trabajo remoto e híbrido
- Evolución del panorama de amenazas

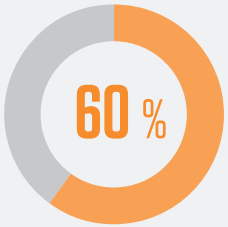
Preparación para el futuro

A medida que los CISO se adaptan a estos cambios, muchos esperan que los presupuestos sigan aumentando (un 11 % de media) para poder hacer frente a los desafíos futuros. Casi dos tercios (65 %) piensa que estarán mejor situados para resistir ciberataques y recuperarse para 2023[2].

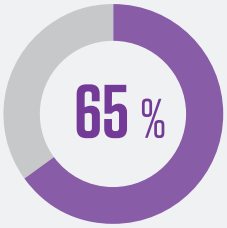
Sin embargo, el nivel de preparación sigue siendo una preocupación importante. Aunque los responsables se muestran optimistas sobre su capacidad para resistir los ataques y recuperarse en el futuro, tienen menos confianza en su capacidad actual. En nuestro informe Voice of the CISO 2021, el 66 % de los CISO consideraban que su organización no estaba preparada para hacer frente a un ciberataque[3].

Las personas, y no las tecnologías de red, constituyen el nuevo perímetro. Y la adopción de nuevos modelos de trabajo (híbrido o teletrabajo a tiempo completo) no hace sino complicar y dificultar todavía más la seguridad.

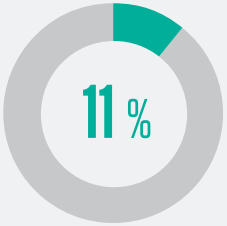
Como responsable de la seguridad, puede orientar su presupuesto para gestionar mejor estos cambios. Este libro electrónico describe las mejores prácticas para evaluar los riesgos, determinar la tolerancia a riesgos de su empresa, evaluar su solución actual y priorizar gastos y justificar su presupuesto frente al consejo de administración.



de los responsables de la toma de decisiones de seguridad de la empresa aumentaron sus presupuestos de seguridad en 2020.



de los CISO piensa que estarán mejor situados para resistir ciberataques y recuperarse para 2023



esperaban aumentar los presupuestos para hacer frente a los desafíos futuros

1 Forrester. "Global Security Budgets in 2021" (Presupuestos de seguridad globales en 2021), agosto de 2021
2 Proofpoint. "Voice of the CISO", mayo de 2021.
3 Proofpoint. "Voice of the CISO", mayo de 2021.

SECCIÓN 2

Evaluación de la tolerancia a riesgos

En primer lugar, evalúe su exposición a amenazas y establezca su tolerancia a riesgos mediante un marco adaptado a su empresa. Existe un gran número de marcos disponibles. Durante el debate de estos temas con la dirección y los miembros de consejo de administración, asegúrese de comunicar el marco que está utilizando y sus razones para hacerlo.

El poder de las cifras

La cuantificación de riesgos no es una ciencia exacta, y puede resultar compleja. Sin embargo, dedicar tiempo a cuantificar los riesgos y la tolerancia a riesgos de su empresa le ayudará a justificar su presupuesto posteriormente. También puede analizar el riesgo en términos cualitativos, pero los parámetros en dinero contante y sonante tendrán más impacto entre la dirección y los miembros del consejo de administración.

Además, es fundamental que todas las partes interesadas hablen el mismo idioma. La tolerancia a riesgos que los dirigentes de la empresa expresan durante la planificación no siempre se corresponde con su tolerancia a riesgos real. Piense en elaborar escenarios realistas con la dirección y los miembros del consejo de administración para asegurarse de que logra el verdadero anhelo de su empresa para el riesgo.

Principales marcos de ciberseguridad

NIST

Marco de ciberseguridad del NIST

El NIST es una división del Departamento de Comercio de Estados Unidos que proporciona consejos sobre la gestión de riesgos de ciberseguridad y la mejora de las comunicaciones internas y externas sobre ciberseguridad.

NISTIR 8286: Identificación y estimación de riesgos de ciberseguridad para la gestión de riesgos de la empresa

Este documento se centra en la gestión de riesgos de ciberseguridad a nivel de grandes empresas en el contexto de la misión y objetivos estratégicos.

People-Centric Security Framework (PCSF)

Desarrollado por Proofpoint siguiendo un proceso transparente y basado en el consenso, que incluye interesados privados y públicos, este marco tiene como objetivo favorecer mejores prácticas en cuanto a riesgos asociados a las personas y ayudar a las organizaciones a proteger la confidencialidad, la integridad y la disponibilidad de sus entornos.

SECCIÓN 3

Mitigación de riesgos

Una vez que ha identificado su exposición a amenazas y su tolerancia a riesgos, debe evaluar sus protecciones actuales frente a ellos.

Mucho más que tecnologías

Puede que tenga la tentación de examinar los riesgos desde el punto de vista de su pila tecnológica actual. Todo el mundo conoce los indicadores de rendimiento clave (KPI), como el tiempo de detección, el tiempo de respuesta y tiempo de corrección.

Estos indicadores son útiles para generar informes de nivel inferior y para comprender el rendimiento diario de las soluciones específicas instaladas. Sin embargo, no son útiles para evaluar y comunicar su posición global frente a riesgos de mayor nivel y sus prioridades empresariales.

Modelado de amenazas

Cuando planifique un presupuesto y lo presente a la dirección, considere el uso de un enfoque de modelado de amenazas para evaluar los indicadores de riesgos clave de su organización y su rendimiento frente a ellos. El modelado de amenazas es un proceso que permite identificar amenazas y cómo se producen, para a continuación priorizar las medidas de mitigación adecuadamente. Frente a los indicadores de rendimiento claves específicos de una solución, el modelado de amenazas le permite comprender los riesgos globales a los que se expone su organización e identificar las lagunas de protección.

El modelado de amenazas le ayudará a identificar lo que está haciendo bien, las áreas en las que debe invertir más y dónde está dispuesto a aceptar un riesgo residual. Puede evaluar una amplia variedad de riesgos de esta manera. Aquí incluimos algunos a tener en cuenta.

Modelado de amenazas en la práctica

A continuación incluimos un ejemplo de cómo funciona el modelado de amenazas en la práctica. Consideremos los riesgos normativos. Las filtraciones de datos forman parte de los escenarios que pueden entrañar riesgos normativos. Y la filtración de datos puede producirse a través de una serie de vectores de amenazas, como:

- Pérdida de datos del correo electrónico
- Transferencia a través de la nube
- Almacenamiento de datos en un disco local
- Uso de soportes extraíbles
- Transferencia de datos a una zona insegura
- Uso de un sitio de intercambio de archivos externo
- Copia y pega manual
- Vulnerabilidades en aplicaciones

Mientras aborda cada uno de estos vectores de filtración de datos, puede evaluar su nivel de protección y decidir cómo solucionar las lagunas.

Si pasa directamente a evaluar el rendimiento de tecnologías específicas, como un agente de seguridad de acceso a la nube (CASB), un agente de protección de endpoint o una red privada virtual (VPN), corre el riesgo de pasar por alto fallos de cobertura de vectores de filtración de datos posible que no cubren estos productos.

Si utiliza el enfoque de modelado de amenazas para evaluar sus indicadores de riesgo claves, puede trazar un dibujo más completo y estratégico de la preparación de su empresa frente a los distintos riesgos.

SECCIÓN 4

Selección de soluciones

Utilizando su evaluación de tolerancia a riesgos y su evaluación de indicadores de riesgos clave, puede identificar las principales áreas que necesitan nuevas inversiones.

Durante el examen de soluciones específicas susceptibles de satisfacer esas necesidades, hágase las siguientes preguntas:

- ¿Mitiga un riesgo particular?
- ¿Resuelve un problema de la empresa?
- ¿Ayuda a mejora la actividad empresarial? (¿Permite la adopción de nuevas herramientas o procesos?)
- ¿Nos permite simplificar y optimizar nuestras operaciones de seguridad?
- ¿Se ajusta a sus objetivos estratégicos y tolerancia a riesgos?

Puede y debe hacerse las mismas preguntas sobre las soluciones existentes. Antes de continuar invirtiendo en una tecnología particular, asegúrese de que sigue respondiendo a sus necesidades.

Cuantificación de la rentabilidad

Para justificar sus inversiones, así como el presupuesto necesario para mantenerlas, ante el consejo de administración, debe cuantificar la rentabilidad de cada solución.

No siempre resulta sencillo cuantificar la rentabilidad de la inversión en soluciones de seguridad, pero puede facilitar la implicación de la dirección. Para ello, es necesario sopesar las ventajas de la solución frente a su coste.

Asegúrese de evaluar los costes ocultos de una solución, por ejemplo:

Hardware

Implementación

Software

Gestión continua

Para cada solución, compare el coste con las ventajas, que pueden incluir la reducción de riesgos y la mejora de la eficacia de la plantilla. Igualmente conviene presentar la opción de no hacer nada detallando la exposición potencial a amenazas y ofreciendo algunos ejemplos.

Por ejemplo, si decide no reducir el impacto del ransomware o el malware, los costes potenciales podrían incluir:

- Interrupción de la actividad
- Pérdida de productividad de usuarios finales
- Tiempo dedicado a la investigación de amenazas y a la creación de informes
- Tiempo dedicado a la neutralización de amenazas
- Tiempo dedicado a tareas manuales, como la eliminación de mensajes de un buzón de correo o la respuesta a mensajes de phishing denunciados

Documentación de riesgos residuales

Asegúrese también de identificar su ciberseguro y su riesgo residual, es decir la exposición a amenazas que permanece después de sus inversiones. Es prácticamente imposible situar a su empresa en riesgo cero y, si fuera posible, probablemente no justificaría el coste. Sin embargo, debería asegurarse de que su riesgo residual respeta el nivel de tolerancia a riesgos de su organización.

SECCIÓN 5

Cálculo y comunicación de los requisitos presupuestarios

Una vez haya determinado sus necesidades presupuestarias y las áreas de inversión, debe comunicar estas necesidades de manera convincente a la dirección y a los miembros del consejo de administración. Probablemente tendrá públicos distintos, concretamente:

- El consejo de administración
- Responsables operativos, como los COO y CIO
- Responsables financieros, como el CFO

Mensaje adaptado

Tiene sentido adaptar el argumento comercial de sus inversiones en seguridad para cada público. Céntrese en el impacto en las áreas de la empresa supervisadas por cada uno de ellos. Básicamente es como decir lo mismo en tres idiomas distintos:

- **El consejo de administración:** cuando se dirija al consejo de administración, insista en la forma en que su plan responde a la toleración a riesgos de la empresa. E identifique el riesgo residual que la empresa está dispuesta a asumir.
- **Responsables operativos:** cuando se dirija al COO o al CIO, insista en el aspecto operativo de su mensaje. Céntrese en las lagunas, las vulnerabilidades restantes y en la forma en que su plan compensará los riesgos para las operaciones empresariales.
- **Responsables financieros:** con el director financiero (CFO), resalte cómo ha equilibrado el gasto o cómo prevé corregir las áreas desequilibradas.

Independientemente del público, comunique la rentabilidad de las soluciones que cuantificó durante la fase de planificación. Ayúdeles a comprender lo que consigue la empresa con el dinero que invierte.

Rentabilidad decreciente

Esté preparado para explicar el concepto de "rentabilidad decreciente". Es posible que tenga que dedicar la misma cantidad a problemas importantes y obvios que a problemas más pequeños y menos evidentes, que también son críticos. Una amenaza aparentemente "menor" puede exponer a la empresa a un riesgo importante, como una fuga de datos, justificando así gastos importantes para compensarlo. Aquí puede volver a hacer referencia a sus cálculos de rentabilidad para poner en contexto el coste de la solución con el riesgo que reduce.

SECCIÓN 6

Gestión de necesidades fuera de ciclo

El proceso presupuestario sigue un ciclo anual o trimestral. Sin embargo, es inevitable que aparezcan problemas fuera del ciclo estándar, como amenazas emergentes o nuevas tácticas de los ciberdelincuentes. Los incidentes inesperados son prácticamente imposibles de evitar, pero puede ofrecer una oportunidad de reevaluar su nivel de seguridad y de replantearse las prioridades de gasto.

Gastos ocultos

No olvide tener en cuenta todos los gastos asociados a cada solución que implemente. La mayoría de las empresas prevén un presupuesto para licencias. Sin embargo, muchas olvidan tener en cuenta el coste del mantenimiento o los recursos necesarios para la solución. Tenga en cuenta esos "gastos ocultos" en la planificación para estar preparado.

SECCIÓN 7

Aceleración del proceso

La elaboración de presupuestos puede convertirse fácilmente en un proceso laborioso y lento. Sin embargo, existen formas de acelerar y facilitar el proceso.

Enfoque estratégico

En primer lugar, asuma plenamente su papel como partner estratégico y recuerde que la función de CISO evoluciona. Identifique los objetivos que persiguen las distintas partes interesadas y ayúdeles a conseguirlos con el mínimo riesgo.

No se limite a las operaciones y al liderazgo técnico y piense cómo puede ayudar a la organización a impulsar la transformación digital y conseguir sus objetivos estratégicos.

Equilibrio entre riesgo y productividad

Recuerde también que no puede eliminar totalmente el riesgo. Como profesional de seguridad, puede que opte por la prudencia en cuanto a la tolerancia a riesgos, pero el consejo de administración y otros dirigentes se inclinarán por encontrar un equilibrio entre exposición a amenazas y objetivos estratégicos. Por ejemplo, la eficacia de su gateway de correo electrónico puede ser del 99,1 %. Sin embargo, basta un solo mensaje de correo electrónico para ser víctima de un ataque de ransomware, lo que deja un riesgo residual del 0,9 %. Este riesgo residual se afronta generalmente incorporando capas de seguridad adicionales, como el aislamiento o la prevención de la pérdida de datos. Todas las partes deben comprender que el riesgo cero no existe.

Encuentre puntos de coincidencia e intente evitar convertirse en el "departamento del no". Su presupuesto y sus planes deberían equilibrar el riesgo respecto a las prioridades de la empresa y minimizar la exposición a amenazas dentro de los límites de toleración a riesgos de la empresa.

Expectativas adecuadas

Por último, modere las expectativas sobre la marcha. La mayoría de los departamentos de una empresa funcionan sobre un modelo de producción, en el que la producción y la rentabilidad mayor son indicadores de rendimiento claves. En cambio, la ciberseguridad se basa en un modelo de resiliencia.

Es decir que al igual que los bomberos reciben su sueldo haya o no un incendio, la ciberseguridad necesita un presupuesto, aunque esto no se traduzca siempre en un aumento de la rentabilidad. Nadie sostendría que los bomberos son innecesarios. A usted corresponde la labor de ayudar a las otras partes implicadas a ver la ciberseguridad de la misma manera.

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentran más de la mitad del Fortune 1000, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.