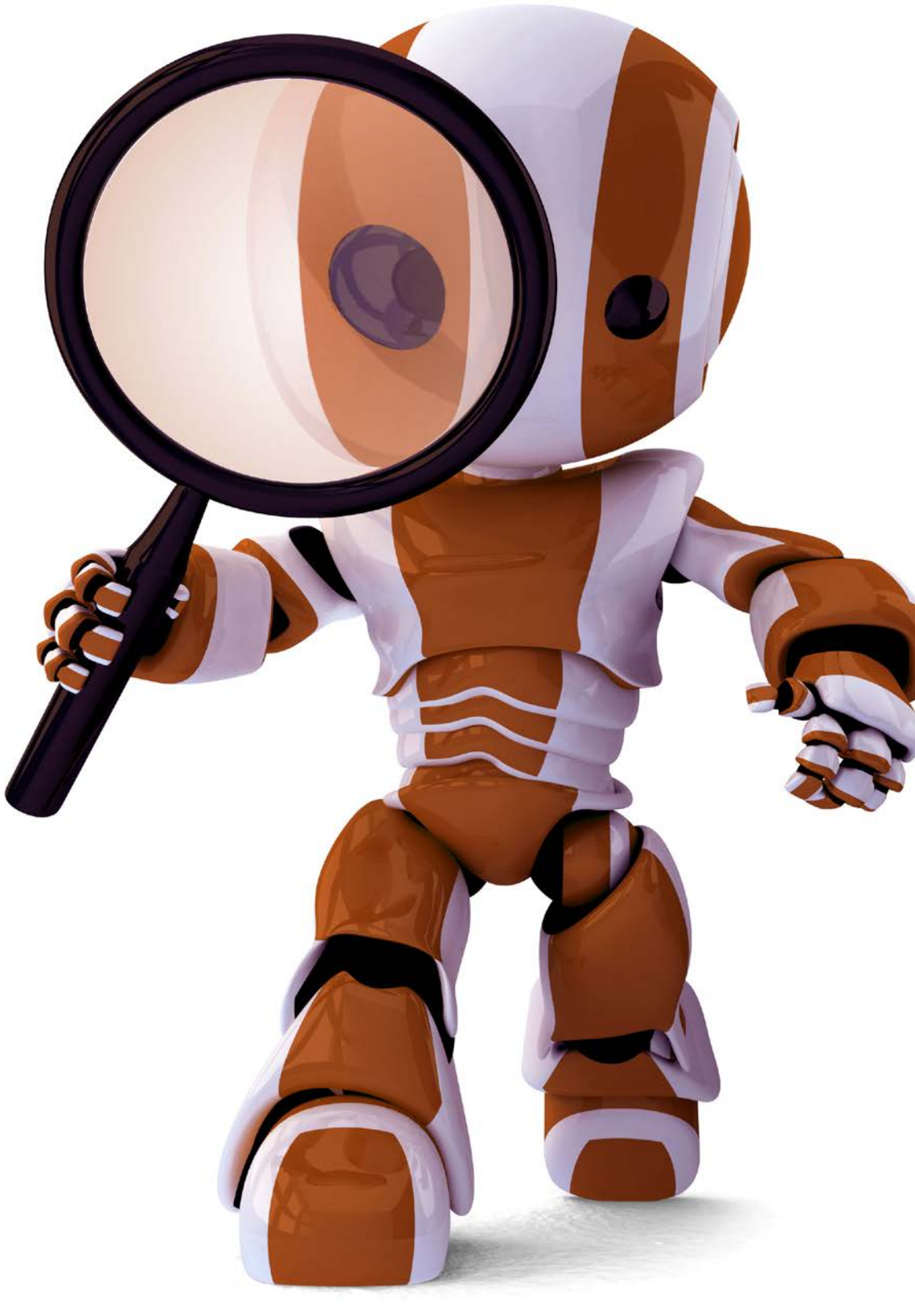
Texto
R. Contreras

EL RESPONSABLE DE SEGURIDAD ADQUIERE RELEVANCIA EN EL MUNDO HÍBRIDO

Retrato robot de un CISO

<< La ciberseguridad es un tema que desborda por todos los lados; la lluvia permanente de ciberataques de grueso calibre, que acosa a todo tipo de organizaciones, sin distinción de tamaño o tipología, ha hecho que los focos se dirijan directamente a un directivo que, hasta no hace mucho tiempo, estaba considerado de 'segunda fila', pero al que ahora se le exige que sea el superhéroe que nos libere de las cadenas del malware. Es el nuevo Hércules que tiene que soportar las columnas corporativas y conseguir que los daños sean los mínimos para el negocio.



Ya no vale la expresión 'el peligro está ahí fuera' y, por suerte (tal vez por escarmiento), los ejecutivos de las grandes compañías están aprendiendo que hay que establecer las barreras a todos los niveles. Pero el tema no va tan rápido como sería de desear, según un estudio de Trend Micro, el 90% de los responsables de la toma de decisiones de TI afirma que su empresa estaría dispuesta a comprometer la ciberseguridad en favor de la transformación digital, la productividad u otros objetivos. Además, el 82% se ha sentido presionado para minimizar la gravedad de los riesgos cibernéticos ante su junta directiva.

"Los responsables de TI se autocensuran ante sus consejos de administración por miedo a parecer repetitivos o demasiado negativos, y casi un tercio afirma que esta es una presión constante. Pero esto solo perpetuará un círculo vicioso en el que los directivos siguen ignorando su verdadera exposición al riesgo", afirma José de la Cruz, director técnico de Trend Micro Iberia.

El papel del CISO

Aquí es donde entra en juego el CISO y su rol como garante de las políticas de seguridad de la compañía. Miguel Carrero, Vice President, Strategic Accounts & Security Service Providers de WatchGuard-Cytomic, define su papel de la siguiente forma: "El CISO es la figura que en una compañía lidera la seguridad de la información, siendo el máximo responsable de velar por garantizar la protección del activo más importante de cualquier entidad, especialmente en un mundo en el que no dejan de aumentar los riesgos relacionados con la seguridad. Este activo no es otro que la información y los sistemas".

Pero ¿cuál sería su retrato robot?, ¿qué características debe tener un CISO ante el panorama actual tan exigente? Miguel Carrero explica la transformación acelerada de su estatus: "El rápido avance tecnológico y la relevancia de esta figura ha hecho que el perfil del CISO evolucione; así, de la persona operativa con un perfil más técnico que protegía los datos aplicando las soluciones de seguridad necesarias, se pasa a un perfil más directivo que está cada vez más involucrado en la toma de decisiones y que cada vez tiene más peso en la definición de la estrategia corporativa en las organizaciones". El alineamiento del negocio y la ciberseguridad es algo crítico, pues es un tema de equilibrio y manejo del riesgo, y no únicamente de componentes tecnológicos.

Para Fernando Serrano, responsable del departamento de Seguridad de acens, "es importante contar con formación técnica, ya que debe tener un conocimiento profundo de las tecnologías utilizadas para tratar la información. Debe estar al día de tendencias en tecnología en general y en tecnología de seguridad en particular, ya que, en estos momentos, con amenazas tan cambiantes, está surgiendo continuamente tecnología de protección y análisis nueva". En suma, es clave tener formación y conocimiento para el análisis de los riesgos, así como tener amplio conocimiento en todo lo referente al derecho tecnológico y cómo puede afectar a la seguridad de una compañía, "pero sobre todo debe tener un profundo conocimiento del negocio y sus procesos, manteniendo un contacto continuo con todas las áreas de la empresa".

Neil Thacker, CISO EMEA de Netskope, destaca el aspecto autodidacta de esta función, dado que "no existía cuando la mayoría de las personas que la desempeñan actualmente estaban eligiendo sus opciones de educación superior al salir del instituto, por lo que aquellos que la ostentan, provienen de una variedad de orígenes". Más comunes que las titulaciones específicas son las certificaciones, que se han desarrollado más rápidamente que los cursos de grado y pueden añadirse al CV durante el transcurso de la carrera. Las certificaciones tienen un periodo de validez y deben mantenerse al día. Los CISO suelen estar acreditados como CISSP (Certified Information Systems Security Professional) o CISM (Certified Information Security Manager), y los más prácticos pueden ser también CEH (Certified Ethical Hacker). "Personalmente, estoy en posesión de las certificaciones mencionadas anteriormente y también soy CIPP/E (miembro certificado de la Asociación Internacional de Profesionales de la Privacidad)", ilustra Thacker.

Consideración del CISO dentro de la empresa

No obstante, el camino del CISO no es precisamente un lecho de rosas, pues no está considerado todo lo bien que sería de desear y no cuenta en los planes de muchas compañías. Un estudio reciente de Netskope revela que alrededor de una cuarta parte de las organizaciones europeas no cuenta con un CISO y que existen muchas diferencias en cuanto a sus funciones, entre una organización y otra. Las

"Mientras que en el pasado el departamento de seguridad podía gestionar el perímetro de la red, esto ya no es un modelo viable con la nube"

¿CÓMO DEBE SER LA RELACIÓN DEL CISO CON EL CEO, EL CIO Y DEMÁS C?

MIGUEL CARRERO, VICE PRESIDENT, STRATEGIC ACCOUNTS & SECURITY SERVICE PROVIDERS WATCHGUARD-CYTOMIC

Para que la ciberseguridad se convierta en una cuestión de la junta directiva, la dirección debe llegar a considerarla como un verdadero factor de negocio. En este sentido, el CISO debe ser uno más en los procesos de toma de decisiones. Hay ventajas e inconvenientes en el departamento de seguridad (y el CISO) dentro o en paralelo al de T. Esta es una decisión organizativa, masa crítica y manejo del talento en la organización.

NEIL THACKER, CISO EMEA DE NETSKOPE

La colaboración es la clave de la eficacia. Existe el riesgo, cuando se desempeña el papel de CISO, de convertirse fácilmente en un detractor, frenando siempre los planes de los demás en un esfuerzo por minimizar el riesgo. Una relación productiva entre el CISO y otros ejecutivos de nivel C garantiza que la seguridad se convierta en un facilitador. Con una mano experimentada en la gestión de la exposición al riesgo, las organizaciones pueden innovar y crecer.

FERNANDO SERRANO, RESPONSABLE DEL DEPARTAMENTO DE SEGURIDAD DE ACENS

La figura del CISO debe establecer relaciones estrechas y de colaboración con el resto de las áreas, evitar en la medida de lo posible el conflicto y servir de enlace muchas veces entre negocio y las áreas técnicas, siendo firme pero no inflexible en las decisiones. Es importante que tenga el máximo apoyo de la gerencia de la compañía y por tanto debe ser una figura situada lo más cerca posible del CEO.

"El mayor reto para el CISO es mantenerse actualizado sobre estos nuevos riesgos y amenazas"

empresas de los sectores que tienen un alto conocimiento de los riesgos cibernéticos son más propensas a tener un CISO, y cuanto mayor sea la comprensión de los riesgos, mayor será la consideración del mismo. Neil Thacker explica esta irregular circunstancia: "El CISO es un puesto de nivel directivo y su función se considera tradicionalmente defensiva en lugar de innovadora, aunque una estrecha relación de trabajo con el CIO y otros compañeros puede disolver rápidamente esta idea errónea y el CISO pasa a ser reconocido como un facilitador y una parte importante del éxito general de la empresa".

Las dimensiones oceánicas del cibercrimen harán por su inercia que el papel de CISO suba como la espuma. Según Global Markets, en 2024, el mercado de la ciberseguridad será una industria de 300.000 millones de dólares; se estiman 6.000 millones de dólares en daños de ciberseguridad solo en este año 2021 (Forbes); y se observa que las empresas tardan unos 6 meses en detectar una brecha de datos (Zdnet). "Este directivo ha pasado de ser un mero asesor, a tener un puesto con muchísima más responsabilidad para convertirse en asesor de seguridad de confianza y tomador de decisiones al más alto nivel, estando especializado en gestión de riesgos, privacidad y cumplimiento, y protección de datos", asegura el portavoz de WatchGuard-Cytomic.

Resulta evidente que la digitalización añade un plus a este cóctel ya de por sí explosivo. Fernando Serrano de acens señala que "la digitalización supone retos de muchos tipos (económicos, personales, sociales etc...) y también supone retos en la seguridad de la información. Proporciona ventajas considerables, pero aña-

de escenarios nuevos con nuevas amenazas. El mayor reto para el CISO es mantenerse actualizado sobre estos nuevos riesgos y amenazas que pueden afectar a la seguridad del entorno, tratando de protegerse lo máximo posible o estar preparado si la protección no ha funcionado". Desde su punto de vista, esta preparación no solo consiste en implantar la última tecnología, también en regular, estableciendo normativas y procedimientos basados en estándares reconocidos, y si es posible revisados y certificados por terceros especialistas que puedan dar una visión externa de la situación.

La nube

En este punto, Thacker incide en la nube como principal reto: "Mientras que en el pasado el departamento de seguridad podía gestionar el perímetro de la red y mantener alejados a los perpetradores de las amenazas, esto ya no es un modelo viable con la nube. Las organizaciones han adoptado la nube pública y privada y el perímetro es un concepto del pasado. Hoy en día, los CISO se enfrentan al reto de garantizar la seguridad de los datos, cuando los datos en cuestión existen dentro de (y se comparten entre) terceros proveedores de servicios en la nube, y el usuario legítimo podría estar accediendo a ellos desde un dispositivo privado compartido, a través de una red pública compartida".

Es indiscutible que la importancia del CISO seguirá creciendo en las empresas, cada vez se le percibe más como "un asesor de seguridad de la información en el consejo de administración, un gestor de riesgos que analiza las probabilidades de riesgo e impacto en la postura de la empresa sobre los frameworks conocidos y que determina el impacto empresarial en la privacidad y el cumplimiento normativo". Miguel Carrero resume perfectamente la proyección del CISO dentro las organizaciones: "El CISO debe ser más una figura inspiradora que tenga capacidad para participar en el establecimiento de la visión corporativa, eliminar la ambigüedad, capacitar a sus equipos y eliminar sus obstáculos, dotando a la compañía de las soluciones y procedimientos necesarios que ayuden a tener visibilidad integral del negocio y le permitan reaccionar ante cualquier incidente de seguridad. El CISO debe, además, ser un elemento catalizador de la concienciación del valor de la seguridad y la necesidad de ser una tarea compartida por todos"; sin duda uno de sus grandes retos. ■