Ante los constantes ciberataques, es imprescindible el apoyo del Consejo de Administración a los CISOs

- *Los principales incidentes apuntan a falta de apoyo proactivo del Consejo e inversiones cruciales para los CISOs, de acuerdo a la nueva investigación de Trellix*

SAN JOSÉ, Calif. – 29 de Noviembre de 2023 – Trellix, la empresa de ciberseguridad que ofrece el futuro de la detección y respuesta extendidas (XDR), publicó hoy una nueva investigación como parte de la iniciativa Mind of the CISO de la empresa. La investigación 'Mind of the CISO: Detrás de la Brecha', de Trellix, encuestó a los directores de seguridad de la información (CISO) globales, de las principales industrias, para comprender mejor los desafíos únicos que enfrentan después de experimentar un ataque cibernético.

"Aumentar la urgencia y la alfabetización cibernética de su propio Consejo de Administración, es uno de los mayores desafíos del CISO", dijo Bryan Palma, director ejecutivo de Trellix. “La investigación sugiere que la voluntad de muchos Consejos de apoyar la ciberseguridad sólo se produce después de un ataque, pero debería ser al revés”.

La investigación revela a qué se enfrentan los CISO después de un incidente cibernético:

- **Los CISO seguirán siendo reactivos hasta que los Consejos de Administración se vuelven proactivos.** El 95% de los CISO recibe más apoyo del Consejo después de un ataque: el 46% recibe un mayor presupuesto para tecnología adicional, el 42% revisa su estrategia general de seguridad, el 41% implementa nuevos marcos y estándares y el 38% crea nuevos puestos de trabajo y responsabilidades después de un ataque.

"*El mayor aprendizaje es que había que generar conciencia a nivel de la junta directiva... desafortunadamente, tuvo que haber un incidente para lograrlo*", compartió un CISO de una agencia gubernamental australiana.

- **Los CISO enfrentan ataques desde todos los ángulos.** Los ataques de robo de datos (48%), malware (43%) y ataques DDoS (37%) son los más comunes.
- **XDR es una solución viable de prevención de amenazas.** Al menos el 92% de los encuestados está de acuerdo en que es necesario mejorar en las personas, los procesos y la tecnología después de experimentar un incidente cibernético importante. Además, el 95% cree que, si su organización hubiera implementado XDR, se habría evitado el importante evento de ciberseguridad que experimentaron.

"*XDR puede tomar y correlacionar datos de múltiples fuentes y, por lo tanto, reducir los falsos positivos. Vemos menos fatiga de alerta en los equipos de seguridad y XDR nos permite ser proactivos en lugar de defensivos y post facto, otra gran diferencia*", compartió un CISO de una empresa del Reino Unido.

- **Las consecuencias ocultas de los incidentes cibernéticos son las que más afectan a las organizaciones.** No se informó que las consecuencias con costos claros, como la pérdida de ingresos y el aumento de las primas de seguros, tuvieran el mayor impacto. En cambio, los principales impactos incluyen la pérdida de datos

(42%), un estrés significativo para sus equipos de SecOps (41%) y una reputación en declive (39%) como factores clave que impactan negativamente a sus organizaciones.

"*Experimentar un incidente cibernético reforzó el concepto de que debemos estar siempre alerta, no importa qué tan seguros creamos que tenemos las cosas, no importa cuántas herramientas tengamos implementadas, es una batalla constante*", compartió un CISO de una empresa de manufactura con sede en EE.UU.

Para incrementar la participación y el apoyo entre los CISO, Trellix lanzó su iniciativa 'Mind of the CISO' a principios de este año, que abarca un Consejo de CISOs, seminarios web e investigaciones. Para obtener más información sobre estos nuevos hallazgos, el libro electrónico de Trellix '**Mind of the CISO: Behind the Breach**' (en inglés), se puede descargar aquí.

De las 500 encuestas realizadas a nivel mundial para la investigación, 30 de ellas se realizaron en México, de ellas 2 fueron a empresas de energía, petróleo y gas; 11 de manufactura; 10 del sector público; 5 del cuidado de la salud; 1 de servicios financieros y 1 de otros sectores. 12 de las empresas tienen entre 1,000 y 2,999 empleados, 10 empresas entre 3,000 y 4,999 empleados y 8 con 5,000 o más. Sobre las personas que respondieron las encuestas 10 eran directores de seguridad de la información o ciberseguridad (CISO, CSO), 12 eran directores de seguridad de TI, 7 directores de seguridad y 1 director de operaciones de seguridad; de ellos 25 son los responsables directos de la ciberseguridad en la empresa y los otros 5 están involucrados en las decisiones estratégicas. El 77% manifiesta haber tenido varios incidentes importantes de ciberseguridad en los últimos 5 años, mientras que el otro 23% ha tenido un incidente importante.

Metodología

El estudio Trellix, realizado por Vanson Bourne, encuestó a más de 500 CISO globales de empresas con un mínimo de 1.000 empleados en EE.UU., México, Brasil, Reino Unido, Francia, Alemania, Australia, India, Singapur, Emiratos Árabes Unidos, Sudáfrica, Japón y Corea del Sur. Las industrias incluyen energía y servicios públicos, atención médica, sectores públicos, manufactura y producción, y servicios financieros. Todos los encuestados experimentaron al menos un incidente cibernético en los últimos cinco años.