# Crece la planificación en ciberseguridad, pero la contención de los ataques disminuye, según un estudio de IBM

• El estudio revela que el uso de más herramientas de seguridad conduce a una respuesta menos eficaz de la seguridad en la empresa
• La mayoría de las organizaciones no tiene un plan específico para los ataques comunes y emergentes. La capacidad de contener un ataque ha disminuido en un 13%

**Cambridge (Mass.), 3 de julio de 2020.** IBM (NYSE: IBM) Security ha anunciado los resultados de su estudio anual Cyber Resilient Organization Report, que examina la eficacia de las empresas en la preparación y respuesta a los ciberataques. El estudio revela que, mientras que las organizaciones han mejorado lentamente en su capacidad de detectar y responder a los ciberataques en los últimos cinco años, su capacidad de contener un ataque ha disminuido en un 13% durante este mismo período.

> *"Aprovechar las tecnologías interoperables y la automatización puede ayudar a superar los retos de complejidad y acelerar el tiempo que se tarda en contener un incidente"*

Según la encuesta, de alcance global, los esfuerzos en materia de seguridad se vieron obstaculizados por el uso de demasiadas herramientas, así como por la falta de planes estratégicos específicos para los tipos de ataque más comunes. Aunque la planificación para la respuesta de seguridad está mejorando poco a poco, la gran mayoría de las organizaciones (74%) sigue informando de que sus planes son ad hoc, se aplican de forma incoherente o que carecen de una guía concreta con los pasos a seguir.

El quinto informe Cyber Resilient Organization Report, basado en una encuesta mundial realizada por el Instituto Ponemon y patrocinada por IBM Security, aporta datos realmente reveladores:

- **Una mejora significativa en seguridad**: En los últimos cinco años, más organizaciones han adoptado planes formales de respuesta de seguridad en toda la empresa; creciendo del 18% de los encuestados en 2015, al 26% en el informe de este año.

- **Se necesitan manuales de estrategia**: Incluso entre aquellos que cuentan con un plan de respuesta de seguridad formal, sólo un tercio ha desarrollado guías específicas para los tipos de ataque más comunes, como el *ransomware*.

- **La complejidad dificulta la respuesta**: La cantidad de herramientas de seguridad que una organización utiliza, tiene un impacto negativo en múltiples categorías del ciclo de vida de la amenaza. Las organizaciones que utilizan más de 50 herramientas de seguridad pierden un 8% en su capacidad de detección y un 7% en su capacidad para dar respuesta a un ataque, respecto a las empresas que tenían menos herramientas.

- **Mejor planificación, menos interrupciones**: Las empresas con planes formales de respuesta de seguridad aplicados en toda la empresa tenían muchas menos probabilidades de experimentar una interrupción significativa como resultado de un ciberataque; en los últimos dos años, sólo el 39% de estas

empresas con planes formales de respuesta experimentaron un incidente de seguridad importante, frente al 62% de las empresas que tuvieron algún incidente por no contar con uno formal/congruente.

"Aunque cada vez más organizaciones se toman en serio la planificación de la respuesta a los incidentes, la preparación para los ciberataques no es una actividad unívoca y acabada", ha indicado Wendi Whitmore, Vicepresidenta de IBM X-Force Threat Intelligence. "Las organizaciones también deben centrarse en probar, practicar y reevaluar sus planes de respuesta regularmente. Aprovechar las tecnologías interoperables y la automatización también puede ayudar a superar los retos de complejidad y acelerar el tiempo que se tarda en contener un incidente".

**Un mayor número de herramientas empeora la capacidad de respuesta**

El estudio también determinó que un exceso de instrumentos de detección de ciberamenazas puede en realidad obstaculizar la capacidad de las organizaciones para hacer frente a los ataques. Los encuestados estimaron que su organización utilizaba más de 45 herramientas de seguridad diferentes de media, y que cada incidente al que respondían requería una coordinación entre unas 19 de ellas.

Estos hallazgos sugieren que la adopción de más herramientas no mejora necesariamente los esfuerzos de respuesta de seguridad, de hecho, puede hacer lo contrario. El uso de plataformas abiertas e interoperables, así como las tecnologías de automatización, pueden ayudar a reducir la complejidad de la respuesta a través de herramientas desconectadas. El 63% de las organizaciones aseguró que el uso de herramientas interoperables les ayudó a mejorar su respuesta a los ciberataques.

**La importancia de un plan estratégico actualizado y una mejor planificación**

La encuesta revela que, incluso entre las organizaciones con un plan formal de respuesta a incidentes de ciberseguridad (CSIRP), un 52% nunca habían revisado o probado su plan de respuesta, lo que sugiere que muchas empresas confían en planes anticuados que no reflejan el panorama actual de las amenazas.

El informe de este año también ofrece pruebas claras de que las organizaciones que invierten en la planificación formal tienen más éxito en la respuesta a los incidentes. Entre las empresas con un CSIRP aplicado de manera consistente en todo el negocio, sólo el 39% experimentó un incidente que resultó en una interrupción significativa de la organización en los últimos dos años, en comparación con el 62% de los que no tenían un plan formal en marcha.

Otros factores que impactaron positivamente en la respuesta a los ataques fueron las habilidades del personal de seguridad y la tecnología. El 61% de los encuestados atribuyó la contratación de empleados cualificados como una de las razones principales para aumentar la resistencia.

**Acerca del estudio**

Realizado por el Ponemon Institute y patrocinado por IBM Security, el informe 2020 Cyber Resilient Organization Report es la quinta entrega que versa sobre la capacidad de las organizaciones para prepararse adecuadamente para los ciberataques y gestionarlos. La encuesta presenta los conocimientos de más de 3.400

profesionales de la seguridad y la tecnología de la información de todo el mundo, incluido Estados Unidos, India, Alemania, Reino Unido, Brasil, Japón, Australia, Francia, Canadá, la ASEAN y Oriente Medio

**Acerca de IBM Security**

IBM Security ofrece una de las carteras más avanzadas e integradas de productos y servicios de seguridad empresarial. Estas soluciones permiten a las organizaciones gestionar eficazmente el riesgo y defenderse contra las amenazas emergentes. IBM opera una de las organizaciones de investigación y desarrollo de seguridad más amplias del mundo, monitoriza 70.000 millones de eventos de seguridad al día en más de 130 países y se le han concedido más de 10.000 patentes de seguridad en todo el mundo.

For further information: Patricia Torralba Comunicación Externa patricia.torralba@es.ibm.com tlf.- 637 804 148