Las cuentas comprometidas de los empleados son el principal coste que tienen que pagar las empresas por las brechas de seguridad

• Las credenciales robadas o comprometidas y las malas configuraciones de la nube fueron las causas más comunes de una brecha de seguridad, representando casi el 40% de los incidentes

• Asimismo, el informe señala que el 70% de las empresas que adoptaron el teletrabajo en medio de la pandemia esperan que exacerbe los costes de la filtración de datos

adrid, 20 de agosto de 2020 - IBM Security ha anunciado la segunda parte de los resultados de un estudio obal que examina el impacto financiero de las filtraciones de datos y brechas de seguridad. Entre las incipales conclusiones revela que las cuentas comprometidas de los empleados son la causa principal del coste ıe han de pagar las empresas por la violación de datos.

redenciales de empleados y nubes mal configuradas - Punto de entrada de los atacantes

ıs credenciales robadas o comprometidas y las malas configuraciones de la nube fueron las causas más ımunes de una brecha de seguridad, representando casi el 40% de los incidentes. Con más de 8.500 millones de gistros expuestos en 2019, y teniendo en cuenta que los atacantes utilizan correos electrónicos y contraseñas eviamente expuestos en una de cada cinco infracciones estudiadas, las empresas están replanteando su trategia de seguridad mediante la adopción de un enfoque de confianza cero, reexaminando la forma de tenticar a los usuarios y el grado de acceso que se les concede.

simismo, la continua lucha de las empresas para afrontar la complejidad de la seguridad -un factor con gran ste para las principales infracciones- está contribuyendo a que las malas configuraciones de la nube se nviertan en un reto de seguridad cada vez mayor. El informe de 2020 reveló que los atacantes utilizaban las nfiguraciones erróneas de la nube para violar las redes en casi el 20% de las ocasiones, lo que aumentaba los stes que esto supone a las empresas por la violación de datos en más de medio millón de dólares, nvirtiéndolo en el tercer vector de infección inicial más caro examinado en el informe.

ɔs ataquues de estado son los más fuertes

pesar de representar sólo el 13% de las infracciones, los actores gubernamentales fueron el tipo de adversario ás dañino según el informe de 2020, lo que sugiere que los ataques con motivación financiera (53%) no se ıducen en mayores pérdidas financieras para las empresas. La naturaleza altamente táctica, la longevidad y las aniobras de sigilo de los ataques respaldados por un estado, así como los datos de alto valor que se atacan, a enudo resultan ser un compromiso mayor para las víctimas, lo que aumenta los costes de las infracciones a una

edia de 4,43 millones de dólares.

e hecho, en Oriente Medio, que históricamente experimenta una mayor proporción de ataques de estado en mparación con otras partes del mundo, experimentó un aumento por encima del 9% anual en su coste medio bido a estas filtraciones de datos, lo que lo convierte en el segundo coste más alto (6,52 millones de dólares) tre las 17 regiones estudiadas. De manera similar, el sector energético, una de las industrias más atacadas por s estados, experimentó un aumento del 14% en los costes a causa de estas filtraciones año tras año, con un omedio de 6,39 millones de dólares.

as tecnologías de seguridad avanzadas, una opción inteligente para los negocios

informe también pone de relieve la creciente brecha en los costes de las infracciones entre las empresas que plementan tecnologías de seguridad avanzadas y las que se han quedado atrás, revelando una diferencia de orro de costes de 3,58 millones de dólares para las empresas con automatización de seguridad totalmente splegada frente a las que aún no han desplegado este tipo de tecnología. La diferencia ha aumentado en 2 illones de dólares.

tiempo de respuesta a las infracciones es significativamente más corto, lo que contribuye a que los costes de s infracciones sean menores para las empresas debido a la automatización de la seguridad completamente splegada. El informe señala que la IA, el aprendizaje automático, el análisis y otras formas de automatización la seguridad están permitiendo a las empresas responder a las infracciones un 27% más rápido que las mpresas que aún no han desplegado la automatización de la seguridad - estas últimas requieren en promedio 74 as adicionales para identificar y contener una infracción.

preparación para la respuesta a incidentes (IR) también sigue influyendo en gran medida en las consecuencias ancieras de una infracción. Las empresas que no disponen de un equipo de RI ni prueban sus planes de RI nen un coste promedio de 5,29 millones de dólares por infracción, mientras que las empresas que disponen de equipo de RI y utilizan simulaciones para probar sus planes tienen un coste de 2 millones de dólares menos r infracción, lo que reafirma que la preparación supone un importante rendimiento de la inversión en berseguridad.

lgunas conclusiones adicionales del informe de este año incluyen:

- **El riesgo del trabajo a distancia tendrá un coste -** Con modelos de trabajo híbridos que crean entornos menos controlados, el informe señala que el 70% de las empresas que adoptaron el teletrabajo en medio de la pandemia esperan que exacerbe los costes de la filtración de datos.
- **Los CISOs fallaron por filtraciones, a pesar de su limitado poder de decisión:** El 46% de los encuestados dijeron que su CISO/CSO es el responsable de la brecha, a pesar de que sólo el 27% declaró que el CISO/CSO es el responsable de la política de seguridad y de la toma de decisiones

tecnológicas. El informe encontró que el nombramiento de un CISO se asoció con 145.000 dólares de ahorro de costes frente al coste medio de una infracción.

- **Las reclamaciones de la mayoría de los negocios ciber asegurados son con cargos a terceros.** El informe constata que las infracciones en las organizaciones con ciber seguros cuestan de promedio casi $200,000. De hecho, de las organizaciones que tienen sus ciber seguros, el 51% lo usan para cubrir los honorarios de consultoría y servicios legales de terceros. Mientras que el 45% de las organizaciones lo emplean para los costes de reparación de los afectados. Menos de un 10% de las reclamaciones son para cubrir el costo de secuestro de datos y extorsión.
- **Perspectivas regionales e industriales:** Mientras que los Estados Unidos continuaron experimentando los costes más altos de violación de datos en el mundo, con un promedio de 8,64 millones de dólares, el informe encontró que los países escandinavos experimentaron el mayor aumento año tras año en los costos por filtración de datos, observando un aumento de cerca del 13%. El sector de la salud continuó incurriendo en los costes más altos, con 7,13 millones de dólares de media, un aumento de más del 10% con respecto al estudio de 2019.

Acerca del estudio

El informe anual sobre el costo de las violaciones de datos se basa en un análisis a fondo de las violaciones de datos en el mundo real que tuvieron lugar entre agosto de 2019 y abril de 2020, teniendo en cuenta cientos de factores de costo, entre ellos las actividades jurídicas, reglamentarias y técnicas para la pérdida de valor de la marca, los clientes y la productividad de los empleados. Para descargar una copia del Informe sobre el Costo de una Violación de Datos en 2020, por favor visite: ibm.com/databreach

Acerca de la seguridad de IBM

IBM Security ofrece una de las carteras más avanzadas e integradas de productos y servicios de seguridad empresarial. La cartera, respaldada por la investigación de renombre mundial de IBM X-Force®, permite a las organizaciones gestionar eficazmente el riesgo y defenderse contra las amenazas emergentes. IBM opera una de las organizaciones de investigación, desarrollo y entrega 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. Para obtener más información, visite www.ibm.com/security, siga @IBMSecurity en Twitter o visite el blog de IBM Security Intelligence.

For further information: Patricia Torralba Comunicación Externa patricia.torralba@es.ibm.com Tlf.-637804148