Cada brecha de seguridad cuesta a las empresas 3,86 millones de dólares de media

Según el informe, "2020 Cost of a Data Breach Report" de IBM y Ponemon Institute

Según IBM, los datos personales de los clientes estuvieron expuestos en el 80% de las infracciones analizadas

La IA y la automatización reducen significativamente los costes provocados por estas infracciones

Según un estudio de IBM, más de la mitad de los empleados que trabajan desde casa, debido a la pandemia, no han recibido nuevas directrices sobre cómo manejar la información personal de los clientes

IBM Security ha anunciado los resultados de un estudio global que examina el impacto financiero de las filtraciones de datos y brechas de seguridad. Entre las principales conclusiones revela que estos incidentes cuestan a las empresas 3,86 millones de dólares de media. Basándose en un análisis exhaustivo de las filtraciones de datos sufridas por más de 500 organizaciones de todo el mundo, el 80% de estos incidentes tuvieron como resultado la exposición de la información de identificación personal de los clientes (PII), este tipo de infracción, además, fue la más costosa para las empresas.

> *"Cuando se trata de la capacidad de las empresas para mitigar el impacto de una violación de datos estamos empezando a ver una clara ventaja de las empresas que han invertido en tecnologías automatizadas"*

En la actualidad, el trabajo en remoto y las operaciones comerciales que utilizan infraestructuras cloud pone en mayor riesgo a las empresas que no tienen los sistemas de seguridad adecuados. El informe revela las pérdidas económicas que las organizaciones pueden sufrir si estos datos se ven comprometidos. Según un otro estudio de IBM, más de la mitad de los empleados que trabajan desde casa, debido a la pandemia, no han recibido nuevas directrices

sobre cómo manejar la información personal de los clientes.https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

El informe "2020 Cost of a Data Breach Report", patrocinado por IBM Security y llevado a cabo por el Ponemon Institute, está basado en entrevistas en profundidad con más de 3.200 profesionales de la seguridad en organizaciones que sufrieron una violación de datos durante el año pasado. Algunos de los principales hallazgos del informe de este año incluyen:

- **Smart Tech reduce los costes de la infracción a la mitad:** El coste de las compañías que han desplegado completamente las tecnologías de automatización de seguridad (que aprovechan la IA, la analítica y la orquestación automatizada para identificar y responder a los incidentes de seguridad) fue menor en comparación con aquellos que no utilizaban estas herramientas - $2,45 millones frente a $6,03 millones de media.
- **Pagar un recargo por credenciales comprometidas:** Los incidentes en los que los atacantes accedieron a las redes corporativas mediante el uso de credenciales robadas o comprometidas costaron a las empresas casi un millón de dólares más en comparación con el promedio mundial - alcanzando los 4,77 millones de dólares por cada filtración de datos. La explotación de las vulnerabilidades fue la segunda causa principal más costosa de las brechas de seguridad (4,5 millones de dólares).
- **Los costes de las grandes brechas de seguridad se disparan:** Las violaciones en las que se comprometieron más de 50 millones de registros o datos personales provocaron que los costes se dispararan a 392 millones de dólares en comparación con los 388 millones del año anterior. Las infracciones en las que se expusieron entre 40 y 50 millones de registros costaron a las empresas un promedio de 364 millones de dólares, un aumento de 19 millones de dólares en comparación con el informe de 2019.
- **Ataques de Estado - Las brechas más dañinas** : Las violaciones de datos que tienen su origen en los ataques de los estados fueron las más costosas, en comparación con otros actores examinados en el informe. Los ataques de los estados supusieron un coste de 4,43 millones de dólares por violación de datos, superando tanto a los ciberdelincuentes que realizan estos ataques con motivos financieros como a los hacktivistas.

"Cuando se trata de la capacidad de las empresas para mitigar el impacto de una violación de datos estamos empezando a ver una clara ventaja de las empresas que han invertido en tecnologías automatizadas", señala Wendi Whitmore, vicepresidente de IBM X-Force Threat Intelligence. "En un momento en que las empresas están ampliando su huella digital a un ritmo acelerado y la escasez de talento de la industria de la seguridad persiste, los equipos se ven desbordados al tener que asegurar más dispositivos, sistemas y datos. La automatización de la seguridad está resolviendo esta carga, no sólo permitiendo una respuesta más rápida a las infracciones, sino también una respuesta significativamente más rentable".

Acerca del estudio

El informe anual sobre el coste 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 coste, 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 de 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 Núñez Canal Comunicación Externa Tel.: 637893754 patricia.nunez@es.ibm.com