30% de trabajadores aún tiene acceso a los archivos de su anterior empresa

Las empresas se exponen a un mayor riesgo de pérdida de datos, si no ponen freno a determinadas acciones de sus empleados, tanto antiguos como actuales. Hasta un 30% de los trabajadores que ya no trabaja en una compañía sigue teniendo acceso a archivos y documentos, aunque ya no estén en plantilla, lo que pone en riesgo la integridad de los datos y la supervivencia de la empresa, según el informe –'Sorting out digital clutter in business' (Eliminando el desorden digital en los negocios). Además, los antiguos empleados también pueden utilizar estos datos para su propio beneficio, por ejemplo, en un nuevo puesto de trabajo, o pueden borrarlos o dañarlos accidentalmente. Como resultado, la recuperación de datos requerirá tiempo y esfuerzo que se podría emplear en tareas empresariales más útiles.

Las empresas hoy en día navegan en un mar de archivos digitales, utilizan aplicaciones de colaboración, documentos online y servicios para compartir archivos, lo que puede dificultar el seguimiento de dónde residen los datos, quién tiene acceso a ellos, cuándo y cómo. Este desorden digital no supone solo un quebradero de cabeza organizativo, sino que también podría suponer una desventaja o incluso una amenaza para las empresas.

Entre los encuestados, un 75% admitió haber trabajado con documentos que contienen diferentes tipos de datos confidenciales.

La sospecha ante un acceso no autorizado a los archivos de trabajo puede proceder de la parte menos obvia: los trabajadores que ya no están en la empresa pero que no han sido dados de baja del servicio de correo electrónico corporativo, de la aplicación de mensajería o de los documentos de Google. La situación es especialmente preocupante, ya que estos activos pueden estar protegidos por derechos de autor o

incluir datos confidenciales que, si se divulgan, podrían ser utilizados por los ciberdelincuentes o los competidores en su propio beneficio.

De hecho, entre los trabajadores que participaron en el estudio, el 75% admitió haber trabajado con documentos que contienen diferentes tipos de datos confidenciales. Asimismo, algo menos de la mitad, (45%) encontró accidentalmente información confidencial sobre salarios e incentivos mientras trabajaban. Si un empleado puede encontrarse de forma fortuita con este tipo de información sensible, también lo puede hacer un hacker.

El desorden de datos digitales también hace que los empleados necesiten más tiempo para encontrar un documento o los datos correctos almacenados en diferentes lugares. Así, el 60% de los encuestados ha tenido dificultades para localizar un documento o archivo mientras trabajaba. En cuanto a utilizar el mismo dispositivo para el trabajo y el uso personal es habitual para el 50% de los encuestados, lo que significa que la información puede duplicarse o quedar obsoleta, causando confusión y posibles errores en el trabajo. Este desorden digital también puede comprometer los datos si caen en manos de un tercero, o incluso de un competidor, además de otras implicaciones graves, sanciones y demandas por parte de los clientes como resultado de la violación de un acuerdo de confidencialidad (NDA) o de la legislación de protección de datos.

El problema del acceso a los activos también se pone de manifiesto por el hecho de que cerca de un tercio (32%) de los trabajadores admite compartir sus credenciales de usuario y contraseña con un compañero. En la cultura actual de espacios abiertos y formas colaborativas de trabajo en la oficina, los empleados tienden a no poner límites y a compartirlo todo con sus colegas, desde clips e ideas, hasta escritorios, tareas e incluso dispositivos. Los malos hábitos relacionados con las contraseñas y esta actitud de "laissez-faire" hacia los datos corporativos sensibles pueden parecer bastante inofensivos y pueden no conducir directamente a una infracción; sin embargo, apuntan a la necesidad de una educación más amplia acerca de los riesgos.

Los archivos digitales en desorden y el acceso incontrolado a los datos a veces pueden dar lugar a brechas y ciber incidentes pero, en la mayoría de los casos, es probable que se

produzcan interrupciones en el trabajo, pérdida de tiempo y de energía asociada con la recuperación de los archivos perdidos. Para las empresas especialmente las pequeñas en desarrollo que se esfuerzan por ser eficientes y competitivas la situación es muy poco deseable. La lucha contra el desorden, la gestión cuidadosa de los derechos de acceso y el uso de soluciones de ciberseguridad no se limitan solo a la protección contra las ciber amenazas.

Para asegurar que el desorden digital no opaca las prácticas de seguridad de datos, es importante tener estas medidas en cuenta:

- Establecer una política de acceso para los activos de la empresa, incluidos los buzones de correo electrónico, las carpetas compartidas y los documentos online: todos los derechos de acceso deben cancelarse tan pronto como el empleado haya abandonado la empresa.

- Recordar de forma periódica al personal las normas de ciberseguridad de la empresa, para que entiendan lo que se espera de ellos y se conviertan en algo natural.

- Utilizar el cifrado para proteger los datos corporativos almacenados en los dispositivos. Realizar copias de seguridad de los datos para garantizar que la información esté a salvo y sea recuperable, en caso de que ocurra un incidente.

- Fomentar buenos hábitos de contraseñas entre los empleados, como no utilizar los datos personales o compartirlos con alguien dentro o fuera de la empresa. La función de administrador de contraseñas de un producto de protección puede ayudar a mantener las contraseñas seguras y los datos confidenciales a salvo.

- Si está acostumbrado a trabajar con servicios cloud, se puede elegir una solución de ciberseguridad cloud que se adapte al tamaño de la empresa.

Fuente de información:
https://www.revistabyte.es