6 de febrero, Día Mundial Internet Segura

5 recomendaciones básicas de seguridad para proteger a las pymes de los ciberataques más sofisticados con IA en 2024

- *7 de cada 10 ciberataques se dirigen a pymes, y 8 de cada 10 brechas de seguridad se producen por errores humanos.*
- *6 de cada 10 pymes afirman no contar con capacidad para afrontar los desafíos de seguridad emergentes en el ámbito de la Inteligencia Artificial (IA) y el Aprendizaje Automático (AA).*
- *Formar a los empleados, utilizar al proveedor cloud como apoyo clave para minimizar el riesgo, realizar análisis de vulnerabilidades, disponer de varias capas de seguridad y generar contraseñas robustas son algunas de las recomendaciones básicas que apuntan desde acens.*

Madrid, lunes 5 de febrero de 2024.- 7 de cada 10 ciberataques tienen como objetivo a una PYME con un coste medio de 35.000 €, además de suponer el cierre de negocio de 6 de cada 10 y el daño reputacional, según datos del estudio 'Panorama actual de la ciberseguridad en España: retos y oportunidades para el sector público y privado' de Google. Ante este contexto, y con motivo del **Día Mundial de Internet Segura** que se celebra el 6 de febrero, acens Part of Telefónica Tech (www.acens.com), ha querido compartir algunos consejos de protección para la pyme y medidas para garantizar la continuidad del servicio y la recuperación de información ante desastres.

El desarrollo de la IA conllevará importantes eficiencias en los negocios, pero para muchos puede suponer un riesgo en materia de ciberseguridad. "*La rápida evolución de la IA ha transformado radicalmente la forma en la que interactuamos con la tecnología. Sin embargo, esta revolución tecnológica no está exenta de riesgos, como pueden ser los ataques de adversarios en modelos de IA y la recopilación y procesamiento de grandes conjuntos de datos para* ***entrenar modelos de IA,*** *en la que garantizar prácticas sólidas de privacidad y seguridad de datos es esencial para mitigar estos peligros. En el horizonte de las amenazas cibernéticas, la tecnología deepfake se presenta como un arma potencialmente devastadora*", explica Manuel Prada, Responsable de Seguridad IT en acens.

Las empresas continúan afrontando una fuerte presión ante el incremento de los riesgos de ciberseguridad, pero en el caso de las **pymes esta presión es mayor si tenemos en cuenta que muchas no cuentan con un CIO** o responsable de seguridad ni implementan protocolos básicos de seguridad. Hay múltiples problemas y factores que contribuyen a aumentar los riesgos actuales en la seguridad informática y cloud, pero según el equipo de IT de acens aunque el riesgo cero no exista, hay dos factores que pueden ayudar a la pyme a minimizar los riesgos asociados a un ciberataque:

1. El factor humano, pues 8 de cada 10 brechas de seguridad se producen por un error humano.
2. Contar con un proveedor cloud seguro.

Para minimizar los riesgos, desde acens aconsejan, en primer lugar, la formación y explicaciones al personal "*sobre todo en lo relativo al correo electrónico y medidas de precaución en su uso. En este sentido es aconsejable la realización de* ***campañas phishing de simulación a los empleados*** *con el fin de que estén en alerta y sean capaces de reconocer con antelación un ciberataque",* apunta Prada.

La seguridad en la autenticación es otra de las claves para acens; por eso, más allá de un sistema doble de autenticación para el acceso de usuarios, desde la tecnológica recomiendan **cuidar la generación de contraseñas seguras con más de 8 caracteres que incluyan letras, números y signos** para el acceso de los usuarios a aplicaciones corporativas. "*La causa de la mayoría de las intrusiones no autorizadas en servidores sigue siendo la elección de una contraseña débil*", recuerda Manuel Prada, responsable IT en acens.

Entre las medidas de protección que puede tomar una pyme, desde acens remarcan, además, la conveniencia de **realizar análisis de vulnerabilidades del sistema de seguridad o pentesting. "***Los datos alojados o los recursos asociados a un servicio habrán de estar protegidos por diferentes capas de seguridad lógica, y en todas ellas hay que realizar los ajustes oportunos para evitar accesos no autorizados y, para ello, es conveniente tener un análisis de vulnerabilidades del sistema de seguridad. En nuestro caso reforzamos la seguridad física de **nuestro CPD con 12 capas de seguridad***", explica Manuel Prada.

Prada explica también cómo "*además de implementar medidas de seguridad local, la pyme cuenta con un importante apoyo en su proveedor en la nube. Contratar servicios en la nube es fácil y fiable, por eso es importante que la pyme seleccione a un **proveedor cloud seguro al que debería exigir que responda a criterios específicos de seguridad** como: ¿Qué garantías de confidencialidad y protección de datos me ofrece?, ¿Qué tipo de medidas de seguridad física implementa en **Data Centers**? Control de acceso, vigilancia 24×7, CCTV, acceso biométrico para garantizar que únicamente accede el personal autorizado… ¿Qué garantías ofrece de disponibilidad, acceso a los datos, capacidad del sistema de soportar datos y recuperarse ante incidentes? Sistemas de alimentación ininterrumpida, climatización, detección y extinción de incendios, sistemas tolerantes a fallos, grupo electrógeno, etc.".*

Por último, realizar actualizaciones continuas de software, así como **copias de seguridad** **de manera regular, especialmente de los datos críticos,** es otra de las recomendaciones que recuerdan desde acens. "*Un error muy común es instalar aplicaciones web y no realizar un seguimiento de las actualizaciones de seguridad. En el contexto actual, tanto empresas como proveedores de servicios deben tener soluciones de ciberseguridad y planes de resiliencia. Pero además de proteger los datos, es crítico estar preparados para mitigar los posibles daños ante una pérdida de datos y para ello es conveniente disponer de un backup de la información automático y fiable en la nube, que posibilite un plan de contingencia rápido en caso de fallo de los servidores de la empresa*", concluye Prada.

Puedes encontrar más información sobre Cloud Hosting, Internet y Tecnología en el **Blog** de acens. También puedes suscribirte al boletín de noticias **aceNews**, ver vídeos en **acens.tv**, apuntarte a cursos gratuitos en **Formacionacens.com** y seguirnos en **Facebook** (acenstec), **Twitter** (@acens), **Instagram** (@acens_com) e **iVoox** (acens Podcast).

Acerca de acens:

acens Part of Telefónica Tech, es pionera en el desarrollo de soluciones Cloud para pequeñas y medianas empresas a las que ofrece soluciones flexibles, seguras y eficaces, tanto en entornos de cloud privados como en públicos y mixtos. Comenzó su actividad en 1997 y en la actualidad ofrece sus servicios en España, Brasil, Perú y México. Además, posee dos Data Centers en España con más de 6.000 metros cuadrados y su cartera de clientes supera los 160.000.
https://www.acens.com/

Acerca de Telefónica Tech:

Telefónica Tech es la empresa líder en transformación digital. La compañía ofrece una amplia gama de servicios y soluciones tecnológicas integradas en Ciberseguridad, Cloud, IoT, Big Data y Blockchain.

https://telefonicatech.com/es

Para más información:
Noizze Media para acens
Carmen Tapia / Ricardo Schell
ctapia@noizzemedia.com / ricardo.schell@noizzemedia.com
646 892 883 / 699 983 936

acens
Inma Castellanos
inma@acens.com