Seguridad Informática: la asignatura pendiente de las empresas españolas

El día 30 de noviembre se conmemora **Día Internacional de la Seguridad Informática**; una celebración que nació en 1998 de la mano de la Association for Computing Machinery con el fin de enseñar a los internautas hábitos que garantizasen su seguridad en la red. Sin embargo, y según las últimas cifras del análisis del comparador de seguros Acierto.com, esta continúa siendo la asignatura pendiente de los ciudadanos y empresas españoles.

Sí, porque **9 de cada 10 desconocen cómo crear una contraseña adecuada**, y no solo eso, sino que la mayoría tiene la misma para todas sus cuentas y no la actualiza jamás. Solo el 20% lo hace cada medio año y hasta 2 de cada 5 obvian de forma consciente las actualizaciones de su equipo, un punto clave para alejarse de los virus y de otros problemas. No resulta extraño de este modo, que más de la mitad de los españoles se haya visto afectado por un problema de este tipo. El

más común es el malware, protagonista de 1 de cada 5 infecciones. El phishing -suplantaciones de identidad- ocupa el último puesto de este ranking, con un 2% de los casos.

El asunto cambia si nos centramos en las compañías, cuyos incidentes más graves suelen estar relacionados con el ransomware y el robo de información en general. En este primero, el ciberdelincuente restringe el acceso a los equipos de la compañía y exige un pago para devolverlos a la normalidad.

La ciberseguridad en las empresas españolas

El caso más acuciante es el de aquellas empresas que gestionan grandes dosis de datos -centros médicos, operadores con ingentes cantidades de información de sus usuarios, etcétera-. Sin embargo, **los ataques a empresas se han incrementado en hasta un 60% durante el último año**, especialmente aquellos que tienen que ver con la filtración de datos y con las PYMES. Los delitos dirigidos a estas últimas han crecido hasta un 130% en el periodo referido.

Razón de más para **contratar un seguro contra hackers o ciberseguro.** Se trata de un tipo de póliza emergente que cubre al asegurado frente a ataques de este tipo con el objetivo de protegerles tanto online como offline, y suelen incluir coberturas por ciberataques pero también por robo y pérdida de archivos, incumplimiento de la LOPD, filtraciones de datos, y similares. Otras coberturas habituales -aunque depende de la entidad- son la de pérdida de beneficios, gastos de defensa por multas, asistencia informática y acceso a un equipo de gestión de crisis.

En Estados Unidos, de hecho, el 85% de las empresas medianas cuenta con un ciberseguro de esta clase. Aquellas que carecen de uno alegan que se trata de un producto demasiado caro. En nuestro país, las principales compañías que los contratan, de hecho, cuentan con una facturación superior a los 100 millones de euros anuales. No obstante y tras la implantación de la nueva LOPD, el número de adeptos a estos seguros está creciendo y **son cada vez más las aseguradoras que ofrecen planes a medida de sus clientes.**

Respecto a esos riesgos y más concretamente; los más frecuentes son el robo de

identidad, los fraudes “amistosos” -el cliente se queda el producto a coste cero después de decirle al banco que la compra no se ha autorizado-, el reshipping -el delincuente compra con una tarjeta robada y usa una “mula”-, account takeover -se roban los datos del cliente -, etcétera. La triangulación nociva también es habitual. Aquí lo que ocurre es que el cliente adquiere el producto a través de una tienda pirata y esta lo re-encarga a una tienda legal pero paga con una tarjeta robada.

Dicho lo cual, un ciberseguro no debería sustituir en ningún caso, la implantación de medidas de seguridad y educación de los empleados en la materia que nos ocupa. Sí, porque no basta con mitigar y atajar los efectos de un ciberataque, sino que **resulta imprescindible prevenirlos mediante el establecimiento de protocolos de seguridad** que deberían incluir, más allá de la tecnología adecuada, planes formativos concretos. Y es que, finalmente, son esos usuarios que ignoran cómo crear una contraseña segura, los que forman parte del entramado empresarial.