¿Están preparadas las empresas españolas ante posibles ciberataques?

Joan Puig
Gerente de Riesgos Tecnológicos de Deloitte

La presencia de noticias en los medios relativos a ciberataques a las empresas ya no es algo anecdótico o excepcional. Las técnicas de ataque utilizadas, o las motivaciones del ataque pueden diferir, pero los ataques a través de este canal, el ciberespacio, están a la orden del día, ya que la información y los sistemas de las empresas cada vez están más expuestos. Hemos pasado de aislar y proteger la red interna de la empresa, a acompañar a los empleados en su vida social, en los usos cotidianos que hacen de la tecnología. Además de las medidas técnicas, la ciberseguridad, también requiere la concienciación de los empleados y de la sociedad en general.

La publicación de un tweet con información falsa, el robo de propiedad intelectual, el ataque informático a la web o a los sistemas de la empresa o la pérdida o sustracción de un teléfono móvil o tablet causan impactos económicos reales. Razón por la que los ciberataques son el principal riesgo tecnológico para las empresas según el informe anual de Riesgos Globales elaborado por el World Economic Forum de este año.

Para conocer la percepción que las empresas españolas tienen de la ciberseguridad y las medidas que están tomando para protegerse, Deloitte ha realizado una encuesta a 273 empresas españolas, cuyas conclusiones se recogen en el último Barómetro de Empresas correspondiente al segundo semestre de 2012.

De los resultados se desprende que las empresas españolas tienen una preocupación real por la ciberseguridad, pues en un 91% de los casos, la Dirección la considera como un reto importante o muy importante, y en un 77% de ellos, se ha nombrado un responsable de seguridad tecnológica de la organización, aunque esta responsabilidad pueda estar compartida con otras funciones, como responsable de tecnología y sistemas.

El presupuesto asignado a ciberseguridad se verá incrementado en 2013 para cerca de la mitad de los participantes en el estudio. Este se dedicará principalmente a la mejora de las infraestructuras y herramientas de seguridad, así como de la capacidad de detección de incidentes, seguidas de cerca por la realización de análisis de vulnerabilidades y auditorías de seguridad.

Todo ello demuestra que los nuevos retos globales de ciberseguridad no son ajenos a las empresas españolas. Estas están emprendiendo acciones para estar adecuadamente preparadas para prevenir y detectar futuros ciber incidentes. El siguiente paso en esta cibercarrera será la preparación para dar respuesta a estos incidentes. Ya que si bien los incidentes de seguridad no se han generalizado, un 29% de los participantes indica haber registrado algún impacto de carácter operativo, y un 11% han identificado incidentes con un impacto económico directo, que en algún caso se ha estimado en superior a los cien mil euros.

Por ello, es recomendable no limitar las iniciativas a medidas de carácter preventivo. La certeza de que un incidente puede ocurrir si un atacante dispone de la suficiente motivación o recursos hace conveniente entrenar la propia capacidad de respuesta ante un ciberincidente, formando a los propios técnicos y directivos y desarrollando las capacidades para coordinar acciones de mitigación del daño y para realizar una investigación interna analizando los sistemas afectados.