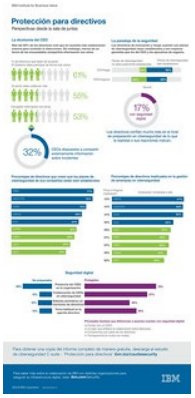
Los directivos no combaten la ciberdelincuencia de un modo eficaz

• Según un estudio de IBM, no tienen claro quién es su auténtico adversario en la ciberdelincuencia

• Falta coordinación entre los directivos de las áreas de negocio y los directores de seguridad

Madrid - 26 feb 2016: Una gran mayoría de los directivos no tiene claro quién es el auténtico ciberdelincuente y cómo combatirlo de un modo más eficaz. Ésta es una de las conclusiones del estudio de IBM (NYSE:IBM) "Seguridad para la alta dirección. Perspectivas de ciberseguridad", para cuya elaboración se ha encuestado a más de 700 altos directivos, de 18 sectores y 28 países. En el informe se ha excluido la opinión del propio director de seguridad o CISO (Chief Information Security Officer) para obtener una imagen más fiel de lo que piensa el resto de la alta dirección acerca de la ciberseguridad.



El estudio desvela que en las empresas hay confusión en cuanto a quiénes son los verdaderos adversarios en la ciberdelincuencia: el 70% de los directivos cree que la principal amenaza procede de posibles empleados corruptos. Sin embargo, según un informe de Naciones Unidas 1, el 80% de los ciberataques procede de organizaciones de crimen organizado. Aunque –según el estudio– el 54% de los encuestados admite que el crimen organizado es una de sus principales preocupaciones, un porcentaje similar concede la misma importancia a la competencia.

Según el estudio, la ciberseguridad es una de las principales preocupaciones en las empresas –así lo atestigua el 68% de los directivos 2––. Sin embargo, el informe desvela que no hay suficiente implicación y coordinación entre los directivos de las diferentes áreas de la empresa y los directores de seguridad o CISOs. Los departamentos de marketing, recursos humanos y finanzas son los principales objetivos de los ciberdelincuentes ya que gestionan parte de la información más confidencial de los clientes y empleados y manejan las finanzas corporativas. Sin embargo, de acuerdo con la encuesta, aproximadamente un 60% de los directores financieros, de recursos humanos y de marketing reconoce que no está, y por extensión sus departamentos tampoco, involucrados de manera activa en la estrategia y puesta en práctica de la ciberseguridad. Por ejemplo, solo el 57% de los directores de recursos humanos organiza cursos de formación en materia de ciberseguridad para empleados de su organización, un primer paso clave para que éstos se involucren.

El informe, realizado por el Institute for Business Value de IBM, revela también que más del 50% de los consejeros delegados entrevistados coincide en que para combatir la ciberdelincuencia es necesario colaborar. Irónicamente, solo un tercio de ellos ha expresado su voluntad de compartir externamente información de su organización relativa a los incidentes sobre ciberseguridad. Esto pone de manifiesto que hay bastante resistencia a colaborar de forma coordinada y generalizada; mientras tanto los hackers siguen perfeccionando su capacidad para compartir información en tiempo real a través de la Red Oscura o Dark Web.

Por otro lado, los consejeros delegados hacen hincapié en que los agentes externos han de hacer más. Reclaman una mayor supervisión gubernamental, por un lado, y una mayor colaboración y cruce de información

transfronteriza, una dicotomía que debe ser resuelta. “El mundo de la ciberdelincuencia está evolucionando rápidamente pero muchos altos directivos no han actualizado sus conocimientos sobre las amenazas existentes”, ha afirmado Caleb Barlow, vicepresidente de IBM Seguridad. “Se debería involucrar de forma más proactiva a los directores de marketing, recursos humanos y finanzas –algunos de los departamentos que custodian los datos más importantes de una empresa- en la toma de decisiones de los directores de seguridad”, añade.

Lo que pueden hacer las empresas

Un 94% de los directivos entrevistados cree que existe la posibilidad de que su compañía sufra algún incidente importante relacionado con la ciberseguridad en los próximos dos años. De acuerdo con el estudio de IBM, el 17% de los entrevistados se siente preparado y capaz de responder a estas amenazas. IBM ha identificado cuáles son los encuestados que mejor están preparados para hacer frente a las amenazas de seguridad. A este grupo se les denomina en el estudio como “ciberseguros”. Este grupo se caracteriza porque la probabilidad de que haya incorporado la colaboración e involucración de los directivos en el programa de ciberseguridad dobla a la del resto. También es el doble de probable que consideren la ciberseguridad un asunto habitual en los comités de dirección.

Consejos “ciberseguros” para las empresas

• Conocer el riesgo. Es importante calcular los riesgos del ecosistema, llevar a cabo evaluaciones de seguridad, dar formación a los empleados e incorporar la seguridad en el plan de riesgos de la empresa.

• Colaborar, formar y capacitar. Establecer un programa de gobierno de la seguridad, capacitar al CISO para llevarlo a cabo, comentar periódicamente el programa de ciberseguridad en las reuniones directivas e involucrarlos en el desarrollo de un plan de respuesta ante incidentes.

• Vigilancia y rapidez en la gestión del riesgo. Implementar una monitorización continuada de la seguridad, aprovechar los análisis forenses de los incidentes, compartir y utilizar la analítica de la información sobre amenazas para proteger el entorno, conocer dónde residen los recursos digitales de las organizaciones y crear y aplicar políticas de ciberseguridad acordes con sus necesidades. Puede acceder a más información sobre el estudio aquí.

1. “Comprehensive Study on Cybercrime 2013” por UNODC (United Nations Office on Drugs and Crime)

2. “Redefining Boundaries: Insights from the Global C-suite Study.” IBM Institute for Business Value. Noviembre de 2015. http://www-935.ibm.com/services/c-suite/study/study/