ABC

10/06/2018

Tirada: 121 283 Categoría: Inf General
Difusión: 83 609 Edición: Empresa
Audiencia: 437 000 Página: 14

AREA (cm2): 642,7 OCUPACIÓN: 72,4% V.PUB.: 19 150€ UNIVERSIDAD

Ciberseguridad, el elemento competitivo por explotar

El blindaje de la información digital se ha convertido en un factor diferencial para las empresas. Sin embargo, un año después de la crisis del WannaCry, y a pesar de la nueva ley de protección de datos, aún tienen mucho trabajo por hacer

133.000 dólares
Fue el coste de media para las empresas que sufrieron un ciberataque en 2017. Casos como el que sufrió la naviera Maersk pueden disparar los costes hasta los 300 millones.

1% PIB mundial
Es el impacto generado por el cibercrimen en todo el mundo en 2017. Una cifra que creció un 0,2% respecto al año anterior y que para este 2018 tiene visos de continuar en alza.

17 horas al año
Es la media que las compañías españolas estuvieron obligadas a parar sus operaciones por culpa de los ataques informáticos. La inactividad conlleva costes elevados a las empresas.

JORGE AGUILAR

La carrera por la digitalización de las empresas ha traído numerosos cambios a la sociedad en los últimos años, muchos de ellos beneficiosos. Sin embargo, también se ha convertido en un arma para el crimen organizado, que ve en la red un espacio infinito para lucrarse a través del robo de datos que manejan las propias compañías. A raíz del ciberataque mundial del pasado año, provocado por el ransomware «WannaCry», estas comenzaron a tomar conciencia de la importancia de la ciberseguridad. Tal es así que según estima Sophos en un estudio, el coste medio para las empresas que sufrieron un ciberataque en 2017 fue de 133.000 dólares, aunque en casos como el sufrido por la naviera Maersk las pérdidas se dispararon hasta los 300 millones. Estos costes engloban los rescates que exigen los ciberdelincuentes, así como el tiempo de inactividad y la pérdida reputacional, entre otros. Aquí en España, los ataques informáticos provocaron que de media las compañías estuvieran inactivas 17 horas.

La seguridad de las propias empresas está empezando a ser un elemento diferenciador de suma importancia. Así, para los inversores la ciberseguridad es el rasgo que más valoran. No es para menos, ya que el número de ciberataques no ha parado de crecer año tras año. Se calcula que en 2017 el impacto generado por el cibercrimen llegó a la cota del 1% del PIB mundial, un 0,2% más que el año anterior. Para ponerle freno, las empresas están poniendo todo su empeño, pero aún no es suficiente. «Todavía muchas empresas no están adoptando tecnologías para poder protegerse de estos ataques», explica Ricardo Maté, director general de Sophos Iberia.

Peligros
El crimen organizado ve en la red un espacio infinito para lucrarse

Además, esta traba es más profunda cuanto más pequeño es el tamaño de la compañía, no tanto por escasez de recursos para realizar la inversión necesaria sino por la falta de formación o información de las mismas. «El problema no reside tanto en el coste a la hora de adquirir un servicio o producto de ciberseguridad, sino en ser consciente de la necesidad del mismo», apuntan desde Ametic, la patronal representante del sector de la industria tecnológica digi-

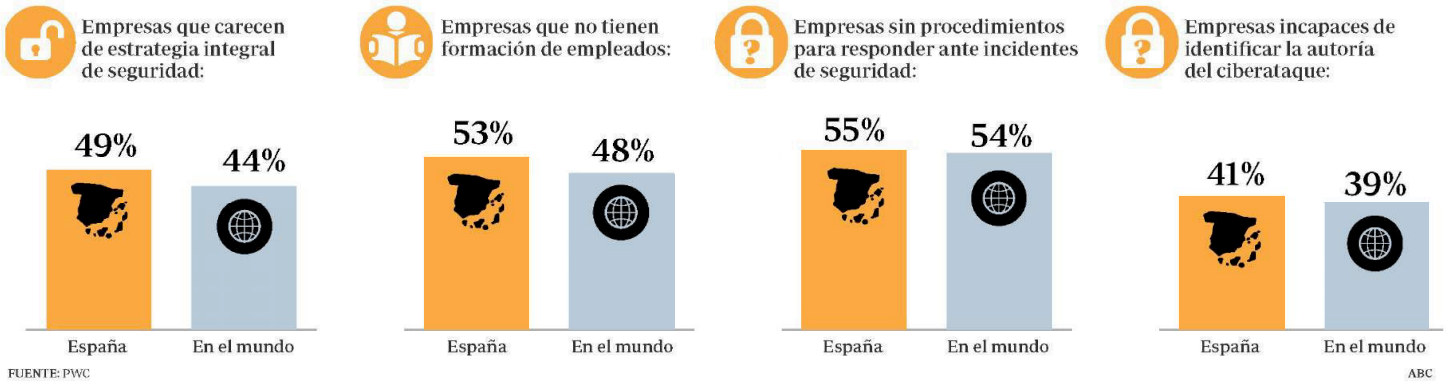
ABC

Tirada: 121 283 Categoría: Inf General
Difusión: 83 609 Edición: Empresa
Audiencia: 437 000 Página: 15

10/06/2018

AREA (cm2): 759,1 OCUPACIÓN: 85,5% V.PUB.: 21 524€ UNIVERSIDAD

Preparación en ciberseguridad de las empresas



FUENTE: PWC

ABC

tal en España. Aquí en España esta circunstancia se convierte en un problema serio, ya que nuestro tejido empresarial está conformado en más de un 99% por pymes y micropymes.

Problema global

A pesar de esa problemática, la situación española en esta materia es destacada. De hecho, según los datos del Global Cibersecurity Index, índice que elabora anualmente la International Telecommunication Union (ITU), España ocupa el puesto 19º a nivel mundial y 9º puesto en Europa. Por tanto, nuestro país se enmarca dentro del grupo de Estados referentes en ciberseguridad. Sin embargo, estos buenos números guardan otra lectura menos positiva. En materia de ciberseguridad el nivel global de los países es todavía muy mejorable. Así, según un estudio de la consultora PwC, el 49% de las empresas nacionales reconocen que no tienen una estrategia integral de seguridad, mientras que la media mundial es del 55%.

El mismo estudio revela que el 55% de las compañías nacionales no tiene procedimientos para responder ante los incidentes de seguridad, un punto porcentual más que las empresas del mundo, mientras que la incapacidad de identificar la autoría de los ataques es del 41% en España por el 39% global.

Aun así, en estas comparaciones, los expertos matizan que hay que separar a las empresas privadas de las administraciones públicas. «El nivel que tiene España en la parte privada está equiparable al que puede tener Estados Unidos o Inglaterra. En el ámbito de la administración es cierto que se requieren mayores inversiones. La dotación que tiene nuestro país en comparación con la que pueden tener Francia, Inglaterra y el resto de nuestros vecinos europeos es mucho menor», puntualiza Jesús Romero, responsable de ciberseguridad y auditoría de Riesgos en PwC. Sobre ello, Maté añade que «no se están incrementando los fondos, por lo que las administraciones deben protegerse como pueden con el mismo dinero que había antes de esas amenazas».

La buena situación del sector privado genera una oportunidad para España de afianzarse como referente en ciberseguridad. Un hecho que podría ayudar a reforzar la competitividad de estas. «Si las empresas respetan los datos, serán más confiables», analiza Marco Lozano, coordinador de los servicios de ciberseguridad de Incibe. Esta afirmación se asienta también en que más de un 70% de consumidores se plantearía cambiar de empresa si no se cuidan sus datos.

Desde la patronal tecnológica Ametic insisten en que «la ciberseguridad es y será cada vez más un elemento determinante en la capacidad de posicionamiento de la empresa frente a su competencia». A todo este cóctel se suma la nueva directiva europea de protección de datos, de obligado cumplimiento, que entró en vigor el pasado 25 de mayo y viene a sustituir a la ley orgánica de protección de datos (LOPD). Entre sus principales novedades destacan la desaparición del consentimiento tácito y la obligación de que las empresas designen a un delegado de protección de datos.

De no cumplirlas, pueden sufrir severas sanciones, incluso si la compañía no tiene sede dentro de la Unión Europea. En concreto, si se infringe la ley, las multas pueden ser de 20 millones de euros o del 4% de la facturación anual.

Escasez de información

Aunque ha habido dos años para prepararse con la nueva directiva de protección de datos, desde Ametic reconocen que «hay preocupación por la insuficiente información que tienen los usuarios, colectivo constituido en su mayoría por pymes y micropymes que no son conscientes del impacto que tiene la entrada en vigor de la nueva ley».

Desde otro punto de vista, también hay analistas que creen que esta nueva directiva hará mucho bien a España en un periodo de medio plazo. «Al ser obligatorio, las empresas van a poner el foco y se van a preocupar. Va a ayudar a su madurez», sentencia Romero.

El mercado laboral necesitará cubrir unos 80.000 empleos para 2020

La vertiginosa vorágine de sofisticadas amenazas en la red ha conllevado una actualización de las empresas y la creación de nuevos puestos de trabajo. La ciberseguridad es uno de los temas centrales de los negocios a la hora de estructurar su organigrama. Sin embargo, todavía la oferta de personal cualificado es muy escasa, al ser todo muy novedoso. Las compañías demandan perfiles expertos en ciberseguridad, pero todavía tendrán que pasar varios años hasta que la oferta nutra completamente las necesidades de las empresas. Así, la Comisión Europea estima que en el año 2020 en Europa puede haber una demanda de perfiles digitales sin cubrir en torno a 500.000 puestos, unos 80.000 en España.
La solución para los expertos tiene su punto de partida en la formación universitaria. Además, la necesidad de cubrir puestos de trabajo puede colocar a la formación en ciberseguridad como una de las más atractivas para los jóvenes. «La inversión de medios materiales y humanos tanto por parte de la industria como de la administración pública en la formación de nuevos perfiles profesionales y la creación de titulaciones adaptadas a las necesidades actuales en ciberseguridad ha dejado de ser una opción para ser en una necesidad», explican desde Ametic.

SANCIONES

Incumplir la nueva ley de protección de datos acarrea multas de 20 millones o del 4% de facturación anual

RASGO DIFERENCIAL

Más de un 70% de clientes se plantearía cambiar de empresa si no se cuidan sus datos personales