Nuevo informe del ONTSI

La facturación del subsector de ciberseguridad alcanzó casi los 600 millones de euros en 2014

- El número de empresas activas en el subsector es de 533 y dan empleo a 5.808 personas.
- Según el informe del ONTSI, en el que ha colaborado el INCIBE, el año pasado el número de incidentes en ciberseguridad de las empresas españolas se incrementó un 200%. En el caso de los ciudadanos el aumento fue casi del 80%.
- Las empresas españolas superarán en 2019 los 1.000 millones de euros de gasto en ciberseguridad.

Madrid, 13 de mayo de 2016. La facturación de las empresas españolas del subsector de la ciberseguridad estuvo próxima en 2014 a los 600 milllones de euros, según recoge el informe de "Caracterización del subsector y el mercado de la ciberseguridad", realizado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), del Ministerio de Industria, Energía y Turismo, que gestiona la entidad pública Red.es, en colaboración con el Instituto Nacional de Ciberseguridad (INCIBE).

El número de empresas activas en este subsector alcanzaba en 2014 la cifra de 533, en su mayoría incluidas en las ramas de actividades informáticas. Estas empresas daban trabajo a 5.808 personas, y prácticamente la totalidad del empleo (99,5%) se concentraba en las del sector TIC:

En cuanto a la facturación total del subsector, ésta era de 598,2 millones de euros. La mayor parte de los ingresos (el 98,9%), aportados por las empresas que pertenecen al sector TIC, principalmente empresas que ofrecen servicios relacionados con las tecnologías de la información y la informática (35%), la consultoría informática (28%) y la programación informática (23%).

Por otra parte, la inversión en ciberseguridad ascendía a 79 millones de euros. Y en este caso, también, su distribución situaba a las empresas pertenecientes al sector de Servicios TIC como las que mayor inversión han llevado a cabo, con 77,8 millones de euros y un peso sobre el total del 98,5%.

Respecto de los bienes de ciberseguridad y confianza digital, cabe destacar la comercialización de herramientas de cortafuegos (*firewall*), con un total de ventas

de 41,9 millones de euros, y las soluciones de *Anti-Malware* y anti-fraude, con una facturación de 33,3 y 29,1 millones de euros respectivamente.

En cuanto a los servicios, destacan los relativos a la externalización de los servicios de ciberseguridad, con 55,6 millones de euros. Le siguen en importancia los servicios de continuidad y contingencia de negocio (20,2 millones de euros) y otros servicios de ciberseguridad y confianza digital (18,9 millones de euros).

La oferta de servicios *freemium* se perfila como nuevo modelo de negocio

La creciente demanda en prácticamente todos los sectores empresariales y en la Administración Pública de productos de ciberseguridad, trae consigo una configuración del subsector caracterizada por la aparición de una serie de agentes con productos y modelos de negocio diferenciados. Entre ellos se incluyen las empresas de servicios especializados que ofrecen soluciones integrales de ciberseguridad, de ciberdefensa - protección de información crítica y la integridad de los servicios públicos- para las Administraciones Públicas o a medida para sectores privados concretos. Es de reseñar también el potencial de las *start-ups* dedicadas a seguridad y el cambio que están experimentando empresas sin relación tradicional con el subsector que incluyen en su oferta servicios relacionados con el mismo.

En cuanto a los modelos de negocio identificados se incluyen la oferta de bienes y servicios *freemium*, así como productos gratuitos en los que se cobra por el servicio de adaptación, instalación y configuración de dicho producto.

Las empresas españolas sufrieron el año pasado un 200% más de incidentes de ciberseguridad que en 2014

El número de incidentes registrados en las empresas españolas hasta noviembre de 2015 (39.985), se incrementó un 200% en relación al año anterior, según los datos facilitados por el CERT de Seguridad e Industria de INCIBE que recoge el informe. En el caso de las infraestructuras críticas –que proporcionan servicios esenciales a la sociedad, como abastecimiento de energía, agua, entidades financieras o empresas de telecomunicaciones- el número de incidentes fue de 111, lo que supone un incremento del 71%. Sin embargo, el aumento en los incidentes en el resto de entidades fue sustancialmente mayor, en concreto, se triplicó, pasando 13.236 en 2014, a 39.874 en noviembre de 2015

Atendiendo a la tipología de incidentes, los más frecuentes son los relacionados con el acceso indebido y la intrusión tanto en infraestructuras críticas (49) como en las que no lo son (12.859). Se contemplan dentro de esta categoría el acceso a cuentas privilegiadas y no privilegiadas o la desfiguración del servidor web en

cuanto a cambio de apariencia (*defacement*). Les siguen, por cantidad, los incidentes catalogados como contenido malicioso, habiéndose registrado 31 en las infraestructuras críticas y 12.186 en el resto, donde también se detectó un elevado número de ataques relacionados con fraudes (11.782).

En cuanto a las soluciones de ciberseguridad adoptadas por las empresas destacan la autenticación mediante contraseña segura -implantada en más de la mitad (61,8%)- y la realización de copia de seguridad de los datos (43,5%). Mientras que el 56,1% de las grandes empresas (más de 250 empleados) posee personal propio para la gestión de la ciberseguridad y protección de los datos, en el caso de las pymes de 10 a 49 empleados, el 59,79% recurre a proveedores externos. Las empresas españolas gastaron en 2014 en ciberseguridad 743,7 millones de euros, un 2,3% más que en el año anterior.

Tres de cada cuatro usuarios de *smartphones* destaca el *spam* como principal incidencia

El número de incidentes sufridos por los ciudadanos, según los datos facilitados por el INCIBE, hasta noviembre de 2015, alcanza la cifra de 2.560, habiéndose incrementado este número, con respecto al año anterior, un 79,9%. Los incidentes con criticidad alta son los más numerosos (1.772) y, atendiendo a su tipología, destacan los relacionados con contenido malicioso (1.494) y con el fraude (594). Por el contrario, los menos numerosos (2) son los relacionados con la seguridad y confidencialidad de la información. Teniendo en cuenta a los usuarios de *smartphones*, la principal incidencia declarada es el *spam* (78,2%), aunque solo un 10,5% reseñaron haber sufrido algún perjuicio económico.

En el año 2015, se redujo un 4% relación al año anterior el porcentaje de personas (77,4%) que utilizan cualquier tipo de software de seguridad de TI o herramienta (anti-virus, anti-*spam*, *firewall*, etc.), con el fin de proteger datos privados y el ordenador personal. Sin embargo, en 2014 se incrementó en 1,1% el gasto en seguridad que alcanzó los 49,7 millones de euros.

El robo de información de alto valor, principal objetivo de los ciberataques en las Administraciones Públicas

El informe también recoge datos relativos a la evolución de los incidentes en ciberseguridad experimentados por las Administraciones Públicas, en este sentido, en 2014 se detectaron 12.916 incidentes, lo que supone un incremento del 78% en relación al ejercicio anterior (inferior al incremento del 82% experimentado entre 2012 y 2013).

El 11% de los incidentes registrados fueron catalogados con criticidad entre muy alta y crítica –afectaron a los sistemas de la organización y a su información

sensible-. Destacan los incrementos experimentados en relación al año anterior por los incidentes de criticidad alta (405%) y crítica (247%).

El principal objetivo de los ciberataques es el robo de información de alto valor, que permite al atacante una mejora de su situación geopolítica o económica o como forma de negocio para grupos perfectamente organizados que subastan la información conseguida al mejor postor.

En cuanto al tipo de incidentes que están apareciendo, la introducción de código dañino en los sistemas (con niveles muy bajos de detección por parte de las empresas antivirus), las intrusiones mediante ataques a páginas web con el fin de robar información, así como el contacto con IPs maliciosas, fueron algunos los incidentes más recurrentes sufridos por la Administración.

La Administración General del Estado y los distintos ministerios invirtieron 3,48 millones de euros en 2014 en *hardware* de seguridad, mientras que la inversión realizada en *software* fue de 6,71 millones de euros.

Las empresas incrementarán el gasto en ciberseguridad en 5 años un 36%

Según apunta el informe del ONTSI, en los próximos años se prevé en España, al igual que a nivel mundial y el resto de países de Europa Occidental, un incremento en la demanda de productos de ciberseguridad motivada por el aumento de las ciberamenazas, el incremento de la regulación en materia de ciberseguridad y la aparición de nuevos productos acompañada de un mayor acceso a los mismos.

La previsión de aumento del gasto en ciberseguridad por parte de las empresas españolas en el periodo comprendido entre 2014 y 2017 es del 22%, y asciende al 36% si se toma como referencia el gasto previsto hasta 2019. Ambos incrementos son algo inferiores al 32% y 53% previstos de media a 3 y 5 años, respectivamente, para los países de Europa Occidental. En 2014 el gasto realizado por las empresas españolas se situaba en 744 millones de euros y la previsión es que en 2019 se alcancen los 1.014 millones.

A diferencia de las empresas, en el caso de los ciudadanos, España se sitúa en cabeza del resto de países europeos en previsión de aumento de gasto tanto a 3 años (6,7%) como a 5 años (11,1%), siendo aquí el incremento medio previsto en Europa Occidental del 6,2% y el 9%, respectivamente. El gasto realizado por los españoles en seguridad en 2014 era de 49,7 millones de euros y en 2019 se prevé que supere los 55,2 millones.

Más información:
Carmen Melgar / Xescu Prats / Blanca Gutiérrez
prensa@red.es
91 212 76 20

Consulta el informe completo:

http://www.ontsi.red.es/ontsi/es/estudios-informes/caracterizaci%C3%B3n-del-subsector-y-el-mercado-de-la-ciberseguridad-2015