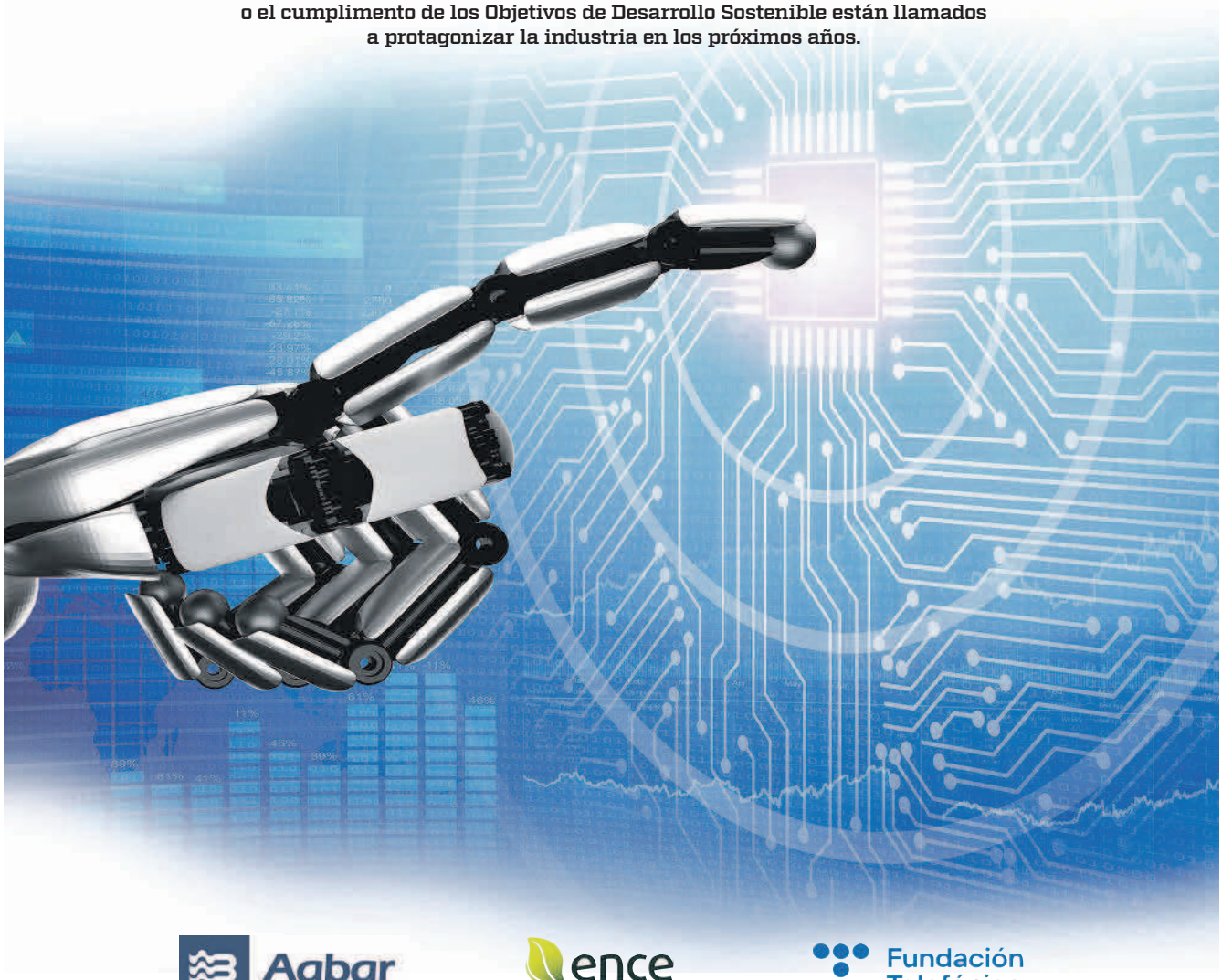
elEconomista

Publicación	El Economista Suplemento, 1	Fecha	30/11/2022
Soporte	Prensa Escrita	País	España
Circulación	50 000	V. Comunicación	65 151 EUR (67,637 USD)
Difusión	30 000	Tamaño	452,98 cm² (72,7%)
Audiencia	52 000	V.Publicitario	7852 EUR (8152 USD)

La ciberseguridad, la nube y el ESG ganan protagonismo

Las nuevas necesidades que están surgiendo, tanto a nivel empresarial como social, tienen en la tecnología su principal aliado. Tendencias como una mayor fiabilidad, una mayor capacidad de almacenamiento y agilidad o el cumplimento de los Objetivos de Desarrollo Sostenible están llamados a protagonizar la industria en los próximos años.



Agbar ence ENERGÍA & CELULOSA Fundación Telefónica

IBERDROLA Santander softonic Unicaja Banco

elEconomista

Publicación	El Economista Suplemento, 8	Fecha	30/11/2022
Soporte	Prensa Escrita	País	España
Circulación	50 000	V. Comunicación	65 151 EUR (67,637 USD)
Difusión	30 000	Tamaño	510,94 cm² (82,0%)
Audiencia	52 000	V.Publicitario	8735 EUR (9068 USD)

UNIÓN PROFESIONAL

CIBERSEGURIDAD EN ESPAÑA, UN PROBLEMA QUE AFECTA A TODAS LAS EMPRESAS

CON LA VISTA PUESTA EN 2025, LA INVERSIÓN EN CIBERSEGURIDAD PODRÍA SUPERAR LA ELEVADA BARRERA DE LOS 2.200 MILLONES DE EUROS, MANTENIENDO RITMOS DE CRECIMIENTO SIMILARES CERCANOS AL DOBLE DÍGITO.

Enrique Espada

La transformación digital, sobre todo en grandes corporaciones y administraciones públicas de nuestro país, es un avance muy positivo en las empresas porque mejora su gestión propia y también la relación con sus clientes, aunque todo escenario de evolución conlleva grandes desafíos, y en este caso es el de la seguridad.

Cualquier entorno digital basado en Internet necesita nuevas y fuertes arquitecturas TI enfocadas exclusivamente a la ciberseguridad. Y es que el incremento de las operaciones digitales de las organizaciones junto con la sofisticación de los ciberdelitos, requieren que las empresas adopten un enfoque nuevo en sus políticas de seguridad informática.

En este sentido, el reciente estudio *Estado de la ciberseguridad en la empresa en España*, realizado por IDC, principal proveedor mundial de inteligencia de mercado, asesoramiento y eventos para los mercados TI, ofrece datos reveladores. Se prevé que el mercado de la ciberseguridad en España aumente en un 7,7% en 2022, llegando a los 1.749 millones de euros. Además, con la vista puesta en 2025, la inversión en ciberseguridad podría superar la barrera de los 2.200 millones de euros, manteniendo ritmos de crecimiento similares cercanos al doble dígito.

Se puede decir, por tanto, que la gran mayoría de organizaciones en plena transformación digital en nuestro país ponen en primer plano la ciberseguridad para proteger sus sistemas e información útil, tal y como explica José Antonio Cano, director de análisis de IDC España, que ha estado "el uso cada vez más creciente de los datos para la mejora de la experiencia del usuario y el avance hacia una organización conducida por datos (*data driven*), plantea la necesidad de repensar las estrategias de ciberseguridad de las compañías, sobre todo teniendo en cuenta que en 2021 hasta un 90% de las empresas en España sufrieron un ciberataque".

Grave problema para las pymes

La siguiente pregunta que deben hacerse las empresas es cómo invertir en ciberseguridad. Y muchas, ya se la han hecho. Tomando como referencia el fideligno estudio, estas son las principales áreas de inversión al respecto: la gestión unificada de amenazas (11,8%), al mismo nivel que la integración de sistemas (11,8%) y los servicios de externalización de redes y *endpoint* (10,6%) son los modelos de gestión en seguridad cibernética más empleados por las compañías españolas, cuyo fin es asegurar el correcto proceso de digitalización que están acometiendo en la actualidad para reducir al máximo el impacto que la transformación del puesto de trabajo supone sobre la gestión de los datos y los procesos de negocio.

Sin embargo, estas prioridades varían según el tamaño de la empresa. Así, mientras que la gran empresa están centrando sus demandas en la gestión unificada de amenazas, la integración de sistemas y los servicios de externalización de redes y *endpoint*, las pymes y autónomos están priorizando la protección de sus dispositivos digitales finales de trabajo, como *smartphones* o tabletas, sobre todo en la venta al detalle, donde la protección del punto final es crítica.

> La gestión unificada de amenazas es el método de seguridad más utilizado

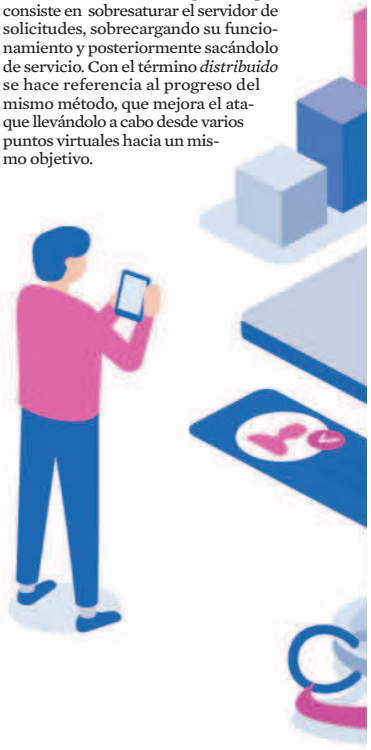
Barracuda Networks ha elaborado un exhaustivo estudio sobre *spear phising* del que se extrae que cualquier trabajador de una pequeña empresa con menos de 100 empleados experimentará un 350% más de ciberataques que un empleado de una empresa grande.

Así pues, las pequeñas y medianas empresas son claramente el gran objetivo de los *hackers* en la actualidad. Y la razón es sencilla; la protección con la que cuentan no suele ser suficiente al no disponer de los mismos medios financieros, técnicos y humanos a los que sí tiene acceso cualquier gran empresa.

El problema tiene solución y está al alcance de cualquier pyme. Para paliar estos ataques, en la actualidad muchas empresas del sector IT ofrecen servicios y soluciones a su alcance. Aunque la oferta es diferente y se adapta a las características de cada pequeño empresario, la denominada como *higiene de ciberseguridad* incluye, normalmente, la supervisión proactiva con visibilidad ampliada para adelantarse a posibles incidencias, la creación de anillos concéntricos de capas de seguridad y una monitorización a tiempo real para la detección de problemas y dar rápida respuesta 24x7x365.

¿Cuáles son los métodos más comunes con los que los *hackers* llevan a cabo estos ciberdelitos? Seguro que en este mismo momento se están cocinando nuevos y sofisticados sistemas informáticos para delinquir por Internet, pero estos son los más habituales.

DoS (*Denial Of Service*) o también DDoS (*Distributed Denial Of Service*). Este tipo de ciberdelito ataca directamente a todo el entorno informático de la empresa en cuestión para dejarlo completamente inaccesible a quien lo use, administradores o usuarios habituales. Lo consigue poniendo en práctica la técnica de la denegación, que consiste en sobresaturar el servidor de solicitudes, sobrecargando su funcionamiento y posteriormente sacándolo de servicio. Con el término *distribuido* se hace referencia al progreso del mismo método, que mejora el ataque llevándolo a cabo desde varios puntos virtuales hacia un mismo objetivo.



elEconomista

Publicación	El Economista Suplemento, 9	Fecha	30/11/2022
Soporte	Prensa Escrita	País	España
Circulación	50 000	V. Comunicación	65 151 EUR (67,637 USD)
Difusión	30 000	Tamaño	493,62 cm² (79,2%)
Audiencia	52 000	V.Publicitario	8471 EUR (8794 USD)

Ransomware. Este *malware* es uno de los más peligros, pues infecta rápidamente los sistemas operativos a partir de un archivo descargado o buscando y explotando algún punto de vulnerabilidad del *software*. Llegados a este punto, el malicioso *software* cifra los archivos del trabajador con una determinada clave y le solicitará su recuperación a cambio de un pago. De esta forma, cualquier organización empresarial puede quedar completamente paralizada ante este ataque hasta que pague el rescate. Esta tipología suponer normalmente doble pérdida económica para la empresa: por un lado el pago por el ciberataque y por otro la recuperación de los sistemas y equipos informáticos afectados.

Phishing. Es un tipo de engaño mediante el que el empleado se dirige a una página web aparentemente de confianza, pero realmente se trata de una *tapadera* para el robo de las contraseñas del entorno informático de las empresas. El *modus operandi* habitual es mediante el envío de correos que en su cuerpo comparten un enlace que dirige a la url trampa. Es muy fácil que cualquier trabajador caiga en ella, pues imitan muy bien a otras más conocidas e incorporan formularios que hacen creer que son oficiales. Como delito es uno de los más graves del código penal, pues si tiene éxito la técnica, el *hacker* acaba suplantando la identidad, las cuentas del usuario e incluso roba dinero si puede.

Virus y gusanos. Ambos son capaces de duplicarse a sí mismos. Es decir, se transmiten replicándose enviando copias a otros equipos para expandirse de forma rápida y peligrosa. Su avance tiene como consecuencia el consumo de ancho de memoria del sistema o del de su banda de red, que desemboca en el colapso de servidores.

Faltan perfiles específicos

Para evitar todos estos ciberataques, además de invertir en entornos IT preparados para ello también es muy importante que las empresas contraten al talento necesario para blindar su ciberseguridad.

> Hoy en día hay más de 120.000 puestos sin cubrir en áreas de ciberseguridad

Así pues, los cuatro perfiles de ciberseguridad específicos que ya están empezando a demandarse en nuestro país son, principalmente, estos: los denominados como *pentesters* o *hackers éticos*, técnicos capaces de atacar los entornos y sistemas de la empresa con el objetivo de detectar y prevenir fallos; especialistas en *cloud computing*, la tendencia prioritaria de digitalización; expertos en Tecnología EDR (*Endpoint Detection and Response*), en pro de resolver los conflictos derivados del uso de dispositivos IoT y detectar y prevenir amenazas avanzadas (ATP); y arquitectos de ciberseguridad, profundos conocedores de las tendencias del mercado capaces de delimitar las directrices de la estrategia concreta de cada cliente.

El grave problema es que el capital humano especializado en estas áreas de la ciberseguridad tan específicas escasea en España, pues somos uno de los pocos países de la Unión Europea que más a la cola está en talento del sector tecnológico. Y los datos así lo avalan, según un reciente análisis llevado a cabo por Factum, una reconocida compañía proveedora de soluciones de ciberseguridad y digitalización. En este riguroso informe se calcula que a día de hoy existen más de 120.000 puestos sin cubrir en las áreas de ciberseguridad y digitalización de las empresas.

Inversión económica, tecnología y capital humano son las tres claves que tanto a autónomos, pymes como grandes compañías les pueden salvar de estos piratas propios del siglo XXI y que tantos perjuicios pueden ocasionar en el funcionamiento y a la reputación de las empresas.

La ciberseguridad ha llegado para quedarse. Estos ciberdelincuentes no tienen ninguna intención de irse y además cada minuto que pasa están más preparados para el futuro ataque. Las empresas españolas no deben dejar al descubierto su frente tecnológico. *Craso error.*