Los ciberataques se han multiplicado desde el inicio de la pandemia. El phising ha crecido un 6.000% en el último año.

La pequeña y mediana empresa suspende en seguridad cibernética

Muchas empresas de la región han sufrido ataques informáticos pero sigue flaqueando la respuesta

El covid-19 ha disparado los ataques de los hackers, que actúan con armas cada vez más precisas y confusas para los ciudadanos. Por responder a esta oleada es necesario que tanto la Administración pública como las empresas cuenten con un buen plan de protección cibernético, pero la mayoría de compañías españolas se comportan con una enorme ingenuidad en este terreno.

El ciberataque que sufrió el Servicio Público de Empleo Estatal (Sepe) el pasado mes de marzo y que lo mantuvo paralizado durante días ha puesto de manifiesto los fallos en la prevención y la respuesta ante ataques informáticos en la Administración.

Que una organización como el Sepe haya sufrido este episodio debe servir para entender que cualquier organización está permanentemente expuesta a sufrir incidentes de seguridad. Y, en el caso de las empresas, un ataque puede conllevar pérdidas muy altas.

La seguridad informática en el entorno empresarial es un asunto de máxima importancia, aunque rara vez se le concede. Desde datos bancarios a información confidencial, pasando por sistemas internos o simples datos personales pueden ser los objetivos de los cibercriminales tanto en empresas grandes como en pequeñas. Solo el año pasado, el Instituto Nacional de Ciberseguridad (Incibe) gestionó 133.155 incidentes, un 24% más que en el anterior.

Desde que comenzó la crisis sanitaria, son muchas las empresas que han implantado el teletrabajo y otras tantas han creado o potenciado sus canales de venta *online*, dos factores que multiplican el riesgo de sufrir un ciberataque que ponga en peligro su viabilidad y su futuro.

Sin embargo, aun siendo conscientes de la importancia de una buena ciberseguridad, la mitad de las empresas españolas no le presta demasiada atención. Según el informe 'Madurez Digital en Ciberseguridad', elaborado por Minsait y SIA –Grupo Indra–, el 56% de las compañías no cuenta todavía con una estrategia de ciberseguridad bien definida y está lejos de cumplir el modelo de Organización Di-

gitalmente Protegida.

El informe también señala que el 90% de las compañías no tiene profesionales especializados en ciberseguridad y un 73% no ha establecido mecanismos para concienciar de este peligro a los empleados.

En líneas generales, banca, telecomunicaciones, seguros y energía destacan por su compromiso por la ciberseguridad. Sobresalen por su elevada inversión en nuevas tecnologías y por la búsqueda de respuestas innovadoras a los retos de la seguridad digital, en parte porque son los que más se juegan, especialmente el sector bancario, que nunca podría llegar a justificar la pérdida de datos de sus clientes.

En cambio, dos sectores básicos de la economía española –turismo y venta al detalle– destacan por su bajo desempeño en este terreno.

Las empresas españolas suspenden en seguridad cibernética. El 90% de las compañías no tiene personal especializado y el 74% no ha establecido mecanismos de concienciación entre su personal.

Ataques muy frecuentes para obtener datos

Todos los datos, por insignificantes que nos parezcan, tienen valor para los ciberdelincuentes. **"Este mercado gira en torno al dinero y sobre cuánto pueden obtener con la información que roban o secuestran"**, explica Roberto García, director general de Ámbar Telecomunicaciones y vicepresidente del Clúster TERA, que agrupa a 19 empresas de Tecnologías de la Información y Comunicación e instituciones de la comunidad autónoma, de las que más de la mitad trabajan en el ámbito de la ciberseguridad.

Por ello, la mayoría de ciberataques van dirigidos a los datos e información que se almacenan en bases de datos, robándolos o usándolos para espionaje.

"Para las grandes empresas se planean ataques extremadamente sofisticados, empleando modelos, herramientas y soluciones específicas, dado que el retorno es muy importante. Para las pymes, el enfoque es diferente. No se utilizan técnicas muy sofisticadas ni personalizadas sino que se lanzan ataques masivos a gran escala. El resultado es una recompensa menor, pero con un mayor número de víctimas, lo que lo hace muy rentable también", advierte García, que estima que, dependiendo del tipo de ataque, el impacto económico puede rondar entre los 15.000 y los 75.000 euros para una pyme, siendo muy superior para una gran empresa.

Engaños y secuestros

Uno de los ataques cibernéticos más comunes es el ***phishing*** *–que* se ha disparado un 6.000% durante la pandemia–, un método de engaño que los ciberdelincuentes utilizan para conseguir que su víctima revele información personal, como contraseñas o datos de tarjetas y de la seguridad social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica.

Estos correos electrónicos, que los ciberdelincuentes envían a cientos de destinatarios al azar, suelen tener nombres comunes como 'Envío de factura' y llegan con un documento adjunto. Un tipo de correo muy habitual para los dueños de pequeñas empresas, por lo que muchas veces descargan el fichero y lo abren.

Aunque aparentemente no ocurre nada, a excepción de que suele estar en blanco, al abrir el archivo se introduce en el ordenador un virus que le roba sus credenciales financieras, sus nombres de usuario y contraseñas, poniendo en riesgo su negocio.

Otro de los ciberataques más comunes es el ***ransomware,*** un *software* extorsivo cuya finalidad es impedir el uso del dispositivo que ataca hasta que se pague un rescate.

Al abrir un archivo infectado, se ejecuta el *script* escondido y va encriptando todo lo que se encuentra en su camino, además de ir corriendo por todos los dispositivos conectados a la red local, secuestrando su información y archivos. La única forma de evitar que siga causando daños es apagar el sistema.

Los archivos afectados por el virus quedan inhábiles y a la espera de que se haga un pago para desencriptar la información, que puede ir desde una pequeña cantidad a muchos miles de euros. Los delincuentes generalmente solicitan el pago en Bitcoins, para que no sea rastreable.

Este tipo de ataque suele llegar a las empresas a través de *spam* malicioso por correo electrónico. El mensaje puede incluir archivos adjuntos trampa, como PDF o documentos de Word, o enlaces a sitios web maliciosos.

En 2016, el centro de formación Decroly sufrió un ataque de *ransomware* por el que todas las carpetas con información de administración de la empresa (contratos, nóminas, facturación...) quedaron encriptadas a consecuencia de un virus llamado *Cryptolocker* que se ejecutó inadvertidamente desde uno de los ordenadores de la organización al abrir un correo.

Gracias a la preparación de este centro para un ataque, pudieron recuperar la información que se guarda diariamente en su nube, por lo que el perjuicio no fue demasiado grande.

Un proyecto pionero con sello cántabro para impulsar la investigación nacional en ciberseguridad

Cantabria es la principal promotora de una iniciativa pionera de ciberseguridad, la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC), que fortalecerá los puentes existentes entre el ámbito académico-investigador y la industria de ciberseguridad.

El proyecto contempla tres áreas de actividad principales, con varias acciones en cada una de ellas, con el objetivo de mejorar la transferencia de conocimiento hacia el tejido industrial e impulsar la excelencia en I+D+i en ciberseguridad.

En primer lugar, consistirá en promover comisiones industria-academia, y grupos de trabajo dedicados al estudio y resolución de problemas concretos de interés común para el ecosistema I+D+i español.

También se potenciará la colaboración con representantes de la industria para evaluar necesidades e incentivos para la generación de proyectos conjuntos de I+D+i en áreas prioritarias. Del mismo modo, se trabajará en la identificación de potenciales proyectos en convocatorias nacionales e internacionales.

Finalmente, se concretarán los mecanismos para retener, captar e intercambiar talento investigador nacional.

La cántabra Viesgo, del grupo EDP, es una de las organizaciones que han manifestado su respaldo a la propuesta de esta Red de Ciberseguridad. La compañía ha mostrado su interés en los resultados que surgirán de este proyecto.

La consejera de Economía y Hacienda, María Sánchez, durante la visita a las instalaciones de Viesgo, del Grupo EDP

La propuesta de RENIC es fruto del trabajo realizado conjuntamente desde la Dirección General de Universidades, la Dirección General de Fondos Europeos y la Oficina de Proyectos Europeos del Gobierno de Cantabria.

Veinte universidades y diez centros de investigación de todo el país colaborarán también en esta iniciativa.

Sergio Ibáñez, el coordinador TIC del centro formativo, recalca la importancia de estar preparado, especialmente porque la realización del pago para acabar con el secuestro de información representa dos problemas: **"Pagar para recuperar los datos secuestrados es ilegal, además de que no podemos fiarnos de que al ejecutar el pago cumplan lo prometido y no nos sigan reclamando nuevas cantidades"**. En ese sentido, el experto informático tiene claro que **"la única manera de volver a la normalidad y poder seguir trabajando consiste en mantener una adecuada política de mantenimiento preventivo y ser meticuloso en la realización de copias de seguridad, bien en dispositivos externos ajenos a la red o en espacios virtuales (la nube)"**.

Por entonces era poco habitual, pero en los últimos años ha habido muchos más casos similares en la región. Uno de los más llamativos fue el ocurrido en 2019 a la empresa pública Cantur, a la que otro de estos ataques le produjo el bloqueo de decenas de miles de documentos con información sensible (nóminas de sus trabajadores, convenios y contratos, concursos...). Toda esta información quedó comprometida, por lo que la empresa pública no pudo funcionar con normalidad durante una semana y el Gobierno regional solo pudo restablecer la normalidad tras ponerse en manos de una empresa especializada que recuperó la mayor parte de esa información.

Poco después, la fábrica de cocinas y estufas Hergom sufrió un episodio similar, que obstaculizó el trabajo de la empresa durante más de una semana y por el que le exigieron un rescate en bitcoins de unos 250.000 euros. A pesar de tener copia de seguridad, la empresa de Soto de la Marina se vio muy dañada por el incidente.

El grupo energético EDP, uno de los principales grupos eléctricos de toda Europa con presencia en Cantabria, también sufrió un ataque de este tipo el pasado año, solo que, en consonancia con su volumen de negocio, los *hackers* solicitaban 10 millones de euros en bitcoins para no hacer pública la información que le habrían robado (10 terabytes de datos).

Son solo algunos ejemplos de compañías de distinto tamaño y modelo de negocio que se han visto atacadas. Según valora el vicepresidente del clúster TERA, **"hay más de 1.000 ciberataques diarios dirigidos a empresas, organismos y particulares de nuestra región, y el grado de éxito está en torno al 10%"**.

Otro de los ataques más comunes es el ***spyware***, un *software* malicioso que infecta ordenadores y otros dispositivos conectados a internet, y graba secretamente sus datos de navegación, las páginas web que visita y sus compras *online*, así como sus contraseñas y los detalles de su tarjeta de crédito. El creador del *spyware* usa esta información en su beneficio o se la vende a un tercero.

Estos archivos van adjuntos al software legítimo que se descarga intencionadamente (como programas para compartir archivos y otras aplicaciones), o se descargan inconscientemente al visitar páginas web maliciosas o al hacer *clic* en enlaces y archivos adjuntos en *emails* infectados.

Se estima que la pérdida de datos causada por ataques informáticos causa daños que oscilan entre los 2.000 y 50.000 euros para las pequeñas y medianas empresas, según Incibe. Para las grandes, las pérdidas pueden ascender a los 3,6 millones de euros, según IBM.

El Incibe recomienda denunciar este tipo de incidentes y, si se ven comprometidos

Roberto García, director general de Ambar Telecomunicaciones.

datos de carácter personal, las empresas afectadas están obligadas a informar a sus clientes en el plazo de 72 horas.

Para evitar situaciones como estas, las organizaciones deben hacer un gran esfuerzo en la formación de los empleados. **"La mayoría de ocasiones se utiliza inadecuadamente la palabra *hackeo*, como si habláramos de un sofisticado sistema de ataque informático, cuando en realidad debiéramos de hablar de 'timo de la estampita' moderno, basado en el engaño por medio de envíos de *email* masivos que se aprovechan de la desinformación y la buena fe de los usuarios, que no son capaces de detectar qué correos son merecedores de atención y cuáles no"**, explica Ibáñez.

Por ello, recomienda contar con **"un buen antivirus actualizado en nuestros equipos Windows, MacOS o Linux; implantar un *firewall* o cortafuegos –un sistema cuya función es proteger una red privada de intrusiones o ataques de otras redes, bloqueándole el acceso–, y utilizar servicios en la nube"**, aunque recalca que una empresa siempre estará expuesta si un empleado no es capaz de detectar esos correos o páginas web con contenido dañino. **"Ante esto, formación y copias de seguridad"**, insiste.

Pequeña y mediana empresa

Independientemente del sector al que se dediquen, las pequeñas empresas y los autónomos son los más afectados por los ciberataques, puesto que suelen ser los menos preparados para defenderse. **"Soy una empresa pequeña, ¿cómo me va a atacar a mí? Eso solamente le pasa a las empresas importantes y a los gobiernos. Esta falsa idea genera que cada día un gran número de pequeñas empresas sean víctimas de un ciberataque"**, afirma Roberto García.

"La pyme es uno de los eslabones más vulnerables, por falta de medios, tiempo, e incluso concienciación", se lamenta el director general de Ámbar. Para blindarse ante amenazas que pueden costar miles de euros, un empresario deberá dedicar parte de su presupuesto a la gestión de estos servicios, algo que muchas pequeñas y medianas empresas no admiten o que, en muchos casos, desconocen.

"El hecho de digitalizarse sin ir de la mano de la ciberseguridad, no prestar la suficiente atención a los datos, una reducida inversión en tecnologías de seguridad y la falta de formación de los empleados en este ámbito, son algunos de los principales puntos vulnerables de las pequeñas y medianas empresas", asegura el responsable de Ambar.

"Para minimizar estas situaciones hay que aplicar un conjunto de soluciones de ciberseguridad. Si hiciéramos un símil con el mundo sanitario actual, estas soluciones constituyen la vacuna más eficaz frente a los ataques digitales externos", plantea García.

Consciente de la situación de las pymes de la región, Sodercan lanzó a finales de año una convocatoria de ayudas que contemplaba una línea de financiación específica para apoyar las inversiones en ciberseguridad. En concreto, se centraba en las inversiones relativas a la adaptación a estándares de ciberseguridad, la formación especializada y la concienciación de la plantilla.

Los 400.000 euros de la convocatoria se agotaron rápidamente, por lo que posiblemente la entidad pública la repita.

Ante la creciente magnitud de los ciberataques y la indefensión de muchas pymes, el Gobierno de España prepara, además, una batería de medidas para hacer frente a este problema. El proceso para hacer a las pymes más digitales y competitivas, a través del 'Plan de Digitalización de Pymes', contará con casi 5.000 millones de euros hasta 2023, procedentes del Fondo de Recuperación Europeo, también conocido como 'Next Generation EU'.

Con estos fondos, el Gobierno pretende alcanzar a 1,5 millones de pequeñas y medianas empresas –la mitad de las que existen en nuestro país–, de las cuales al menos 1,2 millones serán autónomos y microempresas.

El documento recoge un importante monto de 300 millones de euros para la contratación de "expertos en transformación digital". Las pequeñas y medianas empresas podrán acceder a una ayuda de hasta 20.000 euros anuales para hacer estas contrataciones.

María Quintana

Las pymes son las más vulnerables a los ciberataques, por falta de medios.