Ciber... riesgos, también para las aseguradoras

Mª Ángeles Navarro Bas // Actuario de Seguros y coordinadora de Estudios de INESE Data.

En estos tiempos de pandemia que estamos viviendo, en los que nos encontramos más que nunca ciberconectados y donde gran parte de los contactos con empresas, clientes, proveedores o usuarios se realizan a través de la red, la exposición al riesgo cibernético de las empresas se ve incrementada. La directora del Centro Nacional de Inteligencia (CNI), Paz Esteban, reconocía a finales de noviembre que los ciberataques durante la pandemia habían registrado un aumento "cualitativo y cuantitativo". La directiva precisó que, si bien no se aprecian nuevos riesgos, la crisis ha sido un "potenciador" de las tendencias.

No es de extrañar que la ciberseguridad y la protección de datos hayan escalado en las listas de potenciales riesgos y preocupaciones que afrontan las empresas. Buen ejemplo de esta situación la encontramos en el Barómetro de Riesgos de AGCS[1]. Este informe, que identifica los principales riesgos corporativos tras consultar a más de 2.700 expertos en gestión de riesgos de todo el mundo, sitúa los riesgos cibernéticos a la cabeza de la clasificación en España y en tercera posición en el ranking global, solamente por detrás de interrupción de negocio y de los derivados de una pandemia.

Foto: iStock.com/voyager624

El papel del Seguro

El sector asegurador, experto en el manejo de los riesgos y, entre ellos, el riesgo cibernético, permite su transferencia con la suscripción de ciberseguros. Pero las aseguradoras también son empresas que, al igual que ocurre en otros sectores, se encuentran expuestas. Para conocer con más detalle las vulnerabilidades que pueden presentar en su entorno digital, en INESE Data hemos realizado el estudio 'Análisis de la exposición de activos digitales de las aseguradoras a los ciberriesgos'[2], en colaboración con Lazarus. Nuestro *partner* es una compañía que tiene uno de los mayores laboratorios de Europa dedicados a seguridad, continuidad de negocio e informática forense. Con un equipo forense experto, tanto en incidentes de ciberriesgo como en investigación tradicional, Lazarus ha realizado un análisis no intrusivo a los *sites* corporativos de 178 compañías aseguradoras que operan en el mercado español que es la base de este estudio.

Este análisis se ha estructurado en los siguientes puntos:

- Mapa general de la infraestructura, donde se expone la relación entre la IP y el dominio; dominios alojados en el servidor; emails corporativos; subdominios asociados a dicho dominio.
- Listado de puertos abiertos en su servidor.
- Listado de vulnerabilidades asociadas a la página web y al lenguaje-tecnología/servidor/BBDD.

1 AGCS, 'Allianz Risk Barometer', enero 2021. https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html
2 INESE Data y Lazarus, 'Análisis de la exposición de activos digitales de las aseguradoras a los ciberriesgos'. https://www.inese.es/estudio /analisis-de-la-exposicion-de-activos-digitales-de-las-aseguradoras-a-los-ciberriesgos/

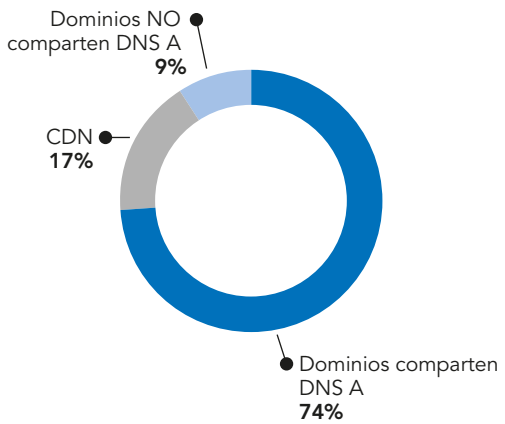
- Emails comprometidos por credenciales expuestas o comprometidas en fuentes conocidas.
- Emails identificados como sospechosos.
- Información relevante sobre el certificado SSL

Una vez obtenida la información de los quince parámetros que han sido evaluados, se han podido detectar las vulnerabilidades que se encuentran en el servidor y en la web; la reputación de los emails corporativos; las credenciales y/o cuentas asociadas al email que podrían haber sido robadas; la situación del certificado SSL; la reputación del dominio principal y la reputación de la IP asociada al dominio principal. Finalmente, en base a los problemas encontrados y mediante algoritmos, se ha elaborado una lista de recomendaciones y correcciones para efectuar en la compañía.

Tras el análisis particular de las 178 aseguradoras, de las que finalmente se han obtenido 187 dominios, ya que algunas compañías tenían asociado más de uno, se ha agregado la información de manera que nos ha permitido extraer conclusiones generales extrapolables al sector asegurador, de las que destacamos:

- El **74% de los dominios** analizados **comparte *hosting*** con otro u otros servidores, lo que supone un riesgo para las webs alojadas en ellos. Cuantos más dominios comparten hospedaje, más riesgo.

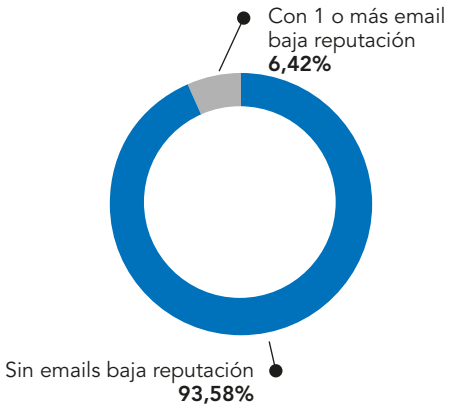
Figura 1: Dominios analizados



Fuente: *INESE Data.*

- **El 97,3% de los dominios tienen subdominios**. Cuantos más subdominios, más frentes abiertos a posibles ataques. Según se destaca desde Lazarus, si bien los dominios suelen estar bien securizados, no ocurre igual con los subdominios; es ahí donde suelen estar las vulnerabilidades.
- De todos los **emails** localizados, el **6,4% tiene baja reputación**, según los algoritmos de Lazarus. Esta situación puede indicar que algo no va bien para esas compañías.

Figura 2: Reputación emails compañías

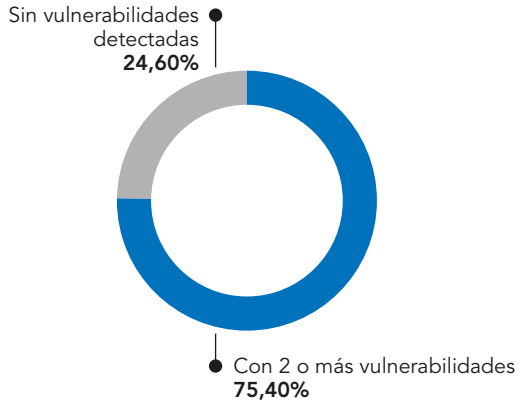


Fuente: *INESE Data.*

Pero más preocupante es que de la mitad de los dominios analizados, concretamente **el 52,4%, ha sufrido filtración en sus emails corporativos**. Se trata de credenciales robadas y/o cuentas en plataformas externas asociadas a dichos emails que han sido vulneradas y constituyen un riesgo para la empresa.

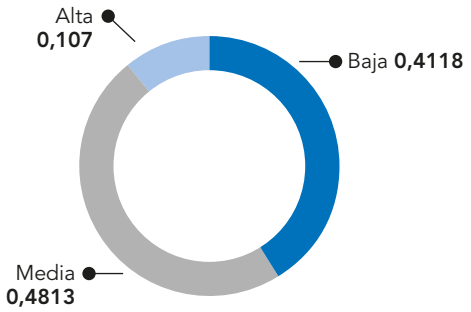
- En el **75% de los dominios** analizados se han hallado **vulnerabilidades en sus webs**. El número oscila entre 2 y más de 800. Y dos datos más para el desasosiego: las **vulnerabilidades son críticas** en el **8,5%** de los casos y algunas de ellas datan de 2007.
- Los algoritmos de Lazarus basados en diversos parámetros analizados han calificado con un **nivel de reputación general bajo** al 0,53% de los dominios de las aseguradoras, al 28,9% con un nivel medio, y al 68% con un nivel alto.
- El **nivel de seguridad global**, que permite obtener una visión general de la seguridad de los activos digitales, califica como **bajo al 41% de los dominios analizados**, que corresponde a

Figura 3: Vulnerabilidades en websites



Fuente: *INESE Data.*

Figura 4: Nivel de seguridad general aseguradoras



Fuente: *INESE Data.*

77 compañías del informe. Como reconoció Manuel Huerta, CEO de Lazarus, en la presentación del informe[3], "es un dato muy llamativo. Un 10% sería lo esperado. Pensábamos que este tipo de compañías tendría esto mejor resuelto, pero nos ha sorprendido hasta a nosotros", argumenta.

Como se puede ver, las aseguradoras adolecen de los mismos problemas que cualquier otra empresa y deben estar atentas a estos riesgos, que pueden ocasionar un daño reputacional y económico considerable, además de dejar a la entidad afectada operativamente fuera de juego durante muchos días o semanas, algo que difícilmente se pueden permitir.

Tienen más información sobre el estudio 'Análisis de la exposición de activos digitales de las aseguradoras a los ciberriesgos' en el área de estudios de inese.es. ●

3 Cristina García, responsable de INESE Data, y Manuel Huerta, CEO de Lazarus. Webinar 'Vulnerabilidades de las aseguradoras en materia de ciberriesgos'. https://youtu.be/hO03ca1FEuc

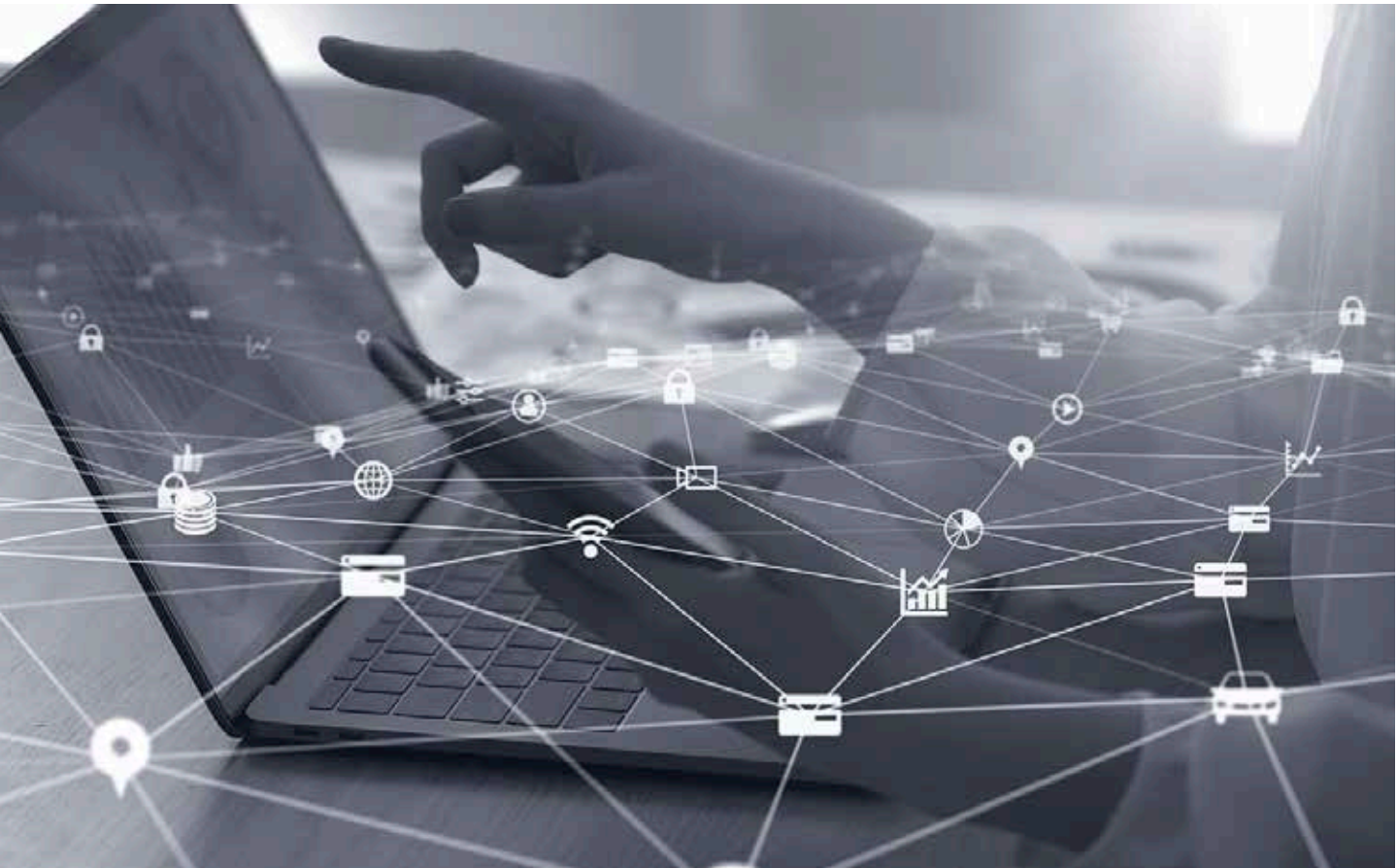


Foto: iStock.com/metamorworks