Más de la mitad de los profesionales de seguridad e IT encuestados a nivel global admitió que sus empresas han sufrido ciberataques en el último año

Según un nuevo estudio de IBM Security, en 2021 el volumen y la gravedad de las amenazas siguen aumentando y solo el 21% de los expertos considera que sus compañías se encuentran en un estado de madurez en temas de ciberseguridad

ARMONK, Nueva York, 10 de diciembre de 2021 – IBM ha presentado el Cyber Resilient Organization Study 2021, el sexto estudio anual sobre ciberresilencia basado en la encuesta de Ponemon Institute, para el que se ha entrevistado a más de 3.600 profesionales del sector de la seguridad e IT en todo el mundo. El estudio analiza el nivel de preparación de las organizaciones para tener una posición de seguridad ciberresilente, entendiendo que lo son aquellas que pueden prevenir, detectar, contener y recuperarse de una gran cantidad de amenazas graves contra los datos, las aplicaciones y la infraestructura de TI.

A lo largo de 2021 se ha experimentado un crecimiento exponencial del *ransomware* que se traduce en pérdidas de millones de dólares para las empresas. Dichas pérdidas no se producen sólo por la falta de ingresos durante el periodo de inactividad provocada por el ataque sino que, además, se suma la inversión de dinero, tiempo y recursos que deben hacer para poder resolverlo y afrontar las multas regulatorias, la pérdida de clientes y el coste de adquirir nuevos.

Según el 67% de los encuestados, tanto el volumen como la gravedad de los incidentes de ciberseguridad aumentaron o lo hicieron significativamente en los últimos 12 meses. Por su parte, el 51% admitió haber sufrido un ataque contra sus datos durante los últimos 12 meses, mientras que el 46% experimentó al menos un ataque de *ransomware* en los últimos dos años.

De las empresas que sufrieron al menos uno de esos ataques, en el 45% de los casos el origen se encuentra en el *phishing* o ingeniería social, los sitios web inseguros o falsos en el 22%, las redes sociales en el 19% y la publicidad maliciosa en el 13%. A pesar de ello, tan sólo el 51% de los expertos preguntados afirmó que sus empresas tienen un plan de respuesta específico

contra posibles ataques de *ransomware*.

De ahí la conclusión del estudio, que informa de que el 61% de las empresas que han sufrido un ataque de *ransomware* en los últimos dos años ha pagado un rescate que oscila, en la mayoría de los casos, entre uno y 10 millones de dólares. La razón más común fue la amenaza de filtración de datos que podría desembocar en una pérdida económica superior al rescate.

En el lado contrario se encuentran las empresas que no hicieron frente al chantaje y que, según el estudio, pudieron enfrentarse porque disponían de un *back up* de la información robada (el 58% de los encuestados), su política de empresa no admitía el pago de rescates (46%) o no creían que los atacantes fueran a facilitar el código de cifrado una vez realizado el pago (43%).

Por último, resulta interesante destacar que solo el 21% de los encuestados considera que su compañía se encuentra en estado de madurez en cuestiones de ciberseguridad. Todo esto permite concluir que es bastante previsible que cualquier empresa, en algún momento de su vida e independientemente de su tamaño y volumen, va a sufrir un ataque, ya sea del tipo *ransomware*, *phishing* u otro tipo de *malware*. Frente a estas amenazas, el *enfoque de zero trust* dota de seguridad a todos los usuarios, dispositivos y conexiones en todo momento. Esta tendencia, que seguirá vigente los próximos años, permite proteger los activos y gestionar los ataques de forma proactiva.

**Metodología*
El estudio IBV de Ciberresiliencia en las organizaciones encuestó a 3.600 profesionales del sector de la seguridad e IT de 15 industrias distintas.
El estudio completo está disponible en https://www.ibm.com/resources/guides/cyber-resilient-organization-study/

Acerca de IBM Security
IBM Security ofrece una de las carteras más avanzadas e integradas de productos y servicios de seguridad empresarial. La cartera, respaldada por la investigación de renombre mundial de IBM Security X-Force®, permite a las organizaciones gestionar eficazmente los riesgos y defenderse de las amenazas emergentes. IBM cuenta con una de las organizaciones de investigación, desarrollo y suministro de seguridad más amplias del mundo, supervisa más de 150.000 millones de eventos de seguridad al día en más de 130 países y ha obtenido más de 10.000 patentes de seguridad en todo el mundo. Para más información, consulte https://www.ibm.com/security, siga a @IBMSecurity en Twitter o visite el blog IBM Security Intelligence.

For further information: Alfonso Mateos Cadenas. Dpto. Comunicación IBM España, Portugal, Grecia e Israel.
alfonso.mateos@ibm.com