Ocho de cada 10 profesionales de TI en España están bajo presión para incrementar y mejorar su ciberseguridad

En España, más del 80% de los profesionales de TI reciben peticiones de sus clientes, accionistas y empleados para aumentar las medidas y mejorar los procesos de seguridad informática debido al aumento de los riesgos y amenazas a la seguridad TI observados durante la pandemia

MADRID, España, 21 de septiembre de 2021. Según un nuevo estudio de Citrix, el 83% de las personas responsables de la toma de decisiones relacionadas con las TI en empresas e instituciones en España recibe presiones para incrementar y mejorar sus protocolos de seguridad. Esta tendencia se observa justo cuando el 78% considera que los riesgos y amenazas a la seguridad TI han aumentado desde el inicio de la pandemia del COVID-19. Los clientes son los que más presión ejercen sobre las empresas a las que contratan productos o servicios para que incrementen la seguridad, ya que el 47% de los profesionales de TI informa que recibe presiones de este grupo, seguidos por los accionistas (44%), y los empleados (38%).

Es posible que, como respuesta a estas demandas exigidas, el 38% de los encuestados afirme que la ciberseguridad se ha convertido en una prioridad máxima en sus organizaciones durante los últimos 18 meses, aunque debemos añadir que el 53% indica que este asunto ha tenido una prioridad máxima "durante años".

“No resulta sorprendente que la seguridad TI se haya convertido en una prioridad aún mayor desde el comienzo de la pandemia”, afirma Mario Derba, Vicepresidente para Sur y Oeste de Europa en Citrix. “Los ciberataques han aumentado en todo el mundo a medida que el teletrabajo se hizo omnipresente de la noche a la mañana y, con ello, los empleados han podido tener algún descuido, por motivos personales o profesionales. Además, debido al trabajo remoto y al traslado masivo de aplicaciones y servicios a la nube en tiempo récord, el perímetro de seguridad, como se concebía antes, prácticamente ha desaparecido. Este estudio pone de manifiesto el reconocimiento y la preocupación de los stakeholders internos y externos ante los desafíos a los que se enfrentan las organizaciones en España”.

La madurez tecnológica, incluyendo estrategias Zero Trust y el puesto de trabajo digital, está impulsando la confianza

Sin embargo, a pesar del aumento de los ciberataques, de las demandas cambiantes y las presiones que se ejercen sobre los decisores de las TI, el 87% de los encuestados afirma sentirse cómodo con las disposiciones adoptadas en materia de seguridad informática, y el 28% dice sentirse “muy cómodo”. El 79% también cree que el personal encargado de la seguridad informática en sus organizaciones cuenta con “todas las competencias necesarias” para ocuparse de los retos actuales.

Esta confianza puede provenir, al menos en parte, del hecho de que muchas organizaciones están sustituyendo sus soluciones tradicionales de VPN por servicios Zero Trust basados en la nube. El 40% de

los encuestados en España ya los han implementado, y otro 44% tiene previsto hacerlo en los próximos 12 meses. Otro 9% tiene previsto hacer una implementación con estas características a más largo plazo. Las principales razones que han impulsado esta la implementación de servicios Zero Trust son: contar con una estrategia para teletrabajo y acceso remoto que sea ágil y seguro (53%); la necesidad de incrementar la seguridad para el acceso a las redes corporativas mediante dispositivos personales, BYOD, (47%); y la mejora de la experiencia del usuario final (31%).

Asimismo, el 92% de las personas responsables de la toma de decisiones en TI afirma estar satisfecho con las soluciones de puesto de trabajo digital que sus organizaciones han implementado para hacer posible el teletrabajo en los últimos 18 meses. El 56% de los encuestados implementó estas soluciones de puesto de trabajo digital como respuesta a las restricciones de movilidad y confinamientos en España desde el pasado mes de marzo de 2020, mientras que el 39% ya las utilizaba antes de la pandemia. Otro 4% no cuenta actualmente con soluciones de puesto de trabajo remoto, pero tiene previsto implementarlas en el futuro.

Entre otras tecnologías que las organizaciones españolas ofrecen para hacer posible el teletrabajo, las más populares son sistemas de vídeoconferencia o streaming (74%) como Zoom o Teams, correo electrónico (65%) y herramientas de colaboración (64%) como Slack.

La falta de competencias y formación pueden convertirse en vulnerabilidades

Aunque la mayoría de los decisores en materia de TI considera que cuentan con el personal adecuado para cumplir con los planes de sus organizaciones en materia de ciberseguridad, hay algunos retos en el horizonte. El 74% de los encuestados admite que tendrá que contratar a personal externo para contar con las competencias adecuadas en el futuro, mientras que el 65% considera que, en algún momento, el personal que se ocupa de la seguridad informática en sus organizaciones “tendrá que volver a formarse por completo”.

Además, el estudio muestra algunas fisuras en la formación en ciberseguridad para los empleados en España. El 55% de los encuestados afirma que la formación en seguridad para todos los empleados de sus organizaciones se imparte una vez al año, y el 12% admite que se imparte cada 2-3 años.

“Los desafíos causados por la pandemia y las presiones que sufren las personas responsables de la toma de decisiones relacionadas con las TI por parte de los principales stakeholders, han hecho que la ciberseguridad se encuentre en un lugar destacado en la lista de prioridades de numerosas organizaciones en España”, comenta Mario Derba. “Hemos tenido que hacer frente a grandes cambios en los últimos 18 meses con la implantación de nuevas tecnologías a una velocidad nunca antes vista, por lo que es positivo ver que la mayoría de los decisiones de TI en España se están adaptando y aceleran sus planes para contar con un nivel de preparación adecuado en materia de ciberseguridad".

“Sin embargo, no es el momento de dormirse en los laureles y es evidente que las empresas tienen la oportunidad de incrementar su seguridad con la mejora de la capacitación de su personal informático y con la formación periódica de todos los trabajadores en general”, añade Derba. “Desde el inicio de la pandemia hemos observado un alarmante aumento de los ciberataques y muchos de ellos

son consecuencia de errores humanos. Por lo tanto, no debemos infravalorar la importancia de una formación anual específica".

# # #