NOTAS OBSERVATORIO DE LA DIGITALIZACIÓN FINANCIERA

FUNCAS – 24 de junio de 2021 **ODF – Funcas 50 / 2021**

¿Cómo frenar el ransomware?

Los crecientes ataques de *ransomware* – por los que a través de un *software* malicioso se secuestran datos de una organización solicitando el pago de un rescate a cambio de devolver el acceso a los mismos– plantean el reto de cómo protegerse ante esta amenaza.

Algunas estimaciones apuntan a que en 2021 se podrían llegar a producir cerca de 100.000 ataques de *ransomware*. Se calcula que cada uno de estos ataques costará a las empresas afectadas unos 170.000 dólares en promedio[1]. En términos agregados, se espera que los daños por delitos cibernéticos alcancen los 6.000 millones de dólares este año. Recientemente viene observándose una tendencia creciente de ataques dirigidos a entidades financieras, bancos centrales e, incluso, bolsas de valores. En este sentido, el presidente de la Reserva Federal, Jerome Powell ha advertido que los ciberataques son el principal riesgo para el sistema financiero mundial y la necesidad de ser conscientes de esta amenaza para estar listos para afrontarla[2].

El reto reside en cómo estar suficientemente protegidos para prevenir este tipo de ataques. En este sentido, debe reconocerse que no

[1] Over 65,000 ransomware attacks expected in 2021: former Cisco CEO. Finance Yahoo. 14 junio 2021. https://finance.yahoo.com/news/over-65000-ransomware-attacks-expected-in-2021-former-cisco-ceo-125100793.html

[2] Cyberattacks are the number-one threat to the global financial system, Fed chair says. CNN. 12 abrill 2021. https://edition.cnn.com/2021/04/12/business/jerome-powell-cyberattacks-global-threat/index.html

existe una solución rápida y sencilla. Los analistas apuntan a que no se trata solo de una cuestión delictiva, sino también geopolítica y de seguridad nacional y global[3]. En este sentido, no parece adecuado argumentar que los gobiernos deberían dejar la responsabilidad a las empresas para que sean estas las que adopten medidas preventivas. En su lugar, parece más útil una acción colectiva coordinada internacionalmente, como se ha discutido en la reciente cumbre del G7.

A la espera de una posible actuación coordinada ante este riesgo global, las entidades financieras asumen que deben de estar preparadas para hacer frente a una escalada de ciberataques. Aunque el sector bancario siempre ha destacado por sus elevados estándares en ciberseguridad, parece que es necesario realizar un esfuerzo adicional. Algunos expertos sector señalan que el presente y el futuro debería pasar por invertir más en ciberdefensas impulsadas por inteligencia artificial. Esta tecnología puede servir como aliada para fortalecer la protección de las entidades financieras, lo que permitiría anticiparse en muchos casos a los posibles ataques de *ransomware.* Se habla también de la necesidad de incentivar el uso de estas tecnologías y de que los bancos centrales revisen el nivel de seguridad de las entidades financieras. De hecho, en la UE, son ya varios los bancos centrales nacionales (entre ellos el Banco de España) que han anunciado test de esfuerzo centrados en calibrar amenazas de ciberseguridad.

[3] Ransomware attacks must be stopped — here's how. Financial times. 11 junio 2021. https://www.ft.com/content/8a26196c-ee82-45ad-a138-16d0884f4f09