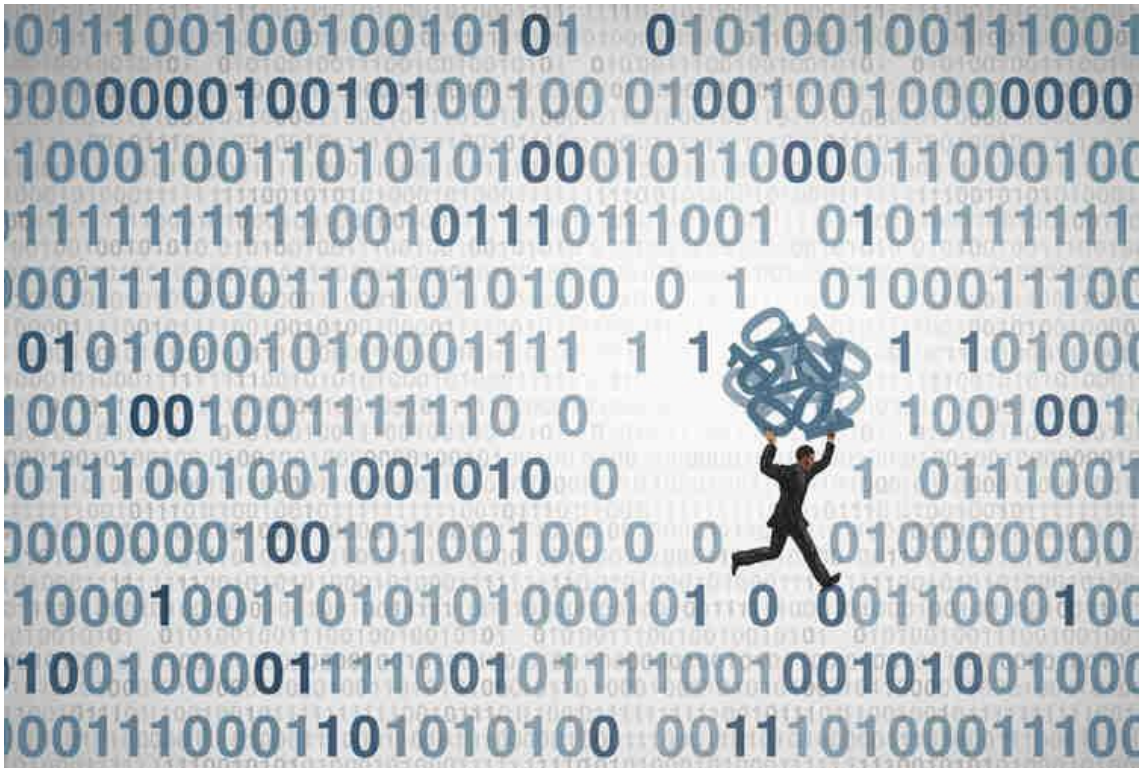
3. El coste real de la ciberdelincuencia y los ciberataques



La compañía de seguridad de EEUU ha estimado recientemente el coste anual de la ciberdelincuencia en compañías con más de mil empleados, siendo la media de 504.000$. Las compañías con menos de cincuenta empleados sufrieron pérdidas de 24.000$.

Para algunas organizaciones, el coste era mucho mayor que la media que se sugería. En su Evaluación de la Amenaza de la Delincuencia Organizada (EADO) del 2019, la Europol cita el ejemplo de un ataque de cibersecuestro de datos en Norsk Hydro AS que costó a la compañía 35 millones de euros (p.24). Varios costos individuales suman miles de millones de dólares o euros al año. En febrero del 2018, el Centro para Estudios Estratégicos e Internacionales (CSIS) y la firma de seguridad McAfee calcularon que el coste anual de la ciberdelincuencia rondaba en torno a los 600 mil millones de dólares por año.

Para poner esto en perspectiva, los economistas creen que Internet genera entre 2 y 3 billones de dólares al año del PIB mundial. Eso significa que quizás hasta una quinta

parte del valor total de Internet está desapareciendo debido al robo cibernético cada año, según el experto en seguridad estadounidense John P. Carlin. [1]

Esto fue en 2018.

Dos años después, la Comisión Europea dijo que el coste anual de la ciberdelincuencia en la economía global en el 2020 estaba cerca de los 5,5 billones de euros, el doble que en el 2015, lo que representa la mayor transferencia de riqueza económica de la historia. [2]

Aunque estos números sean extraordinarios, el verdadero coste de la ciberdelincuencia y de los ciberataques va más allá del coste a las agencias de limpieza o el reemplazo de los códigos infectado, de los equipos comprometidos, del tiempo de inactividad en la red y del daño a la reputación. El verdadero coste de la ciberdelincuencia y de los ciberataques debe tener en cuenta los costes individuales, los 19.000 pacientes que han perdido operaciones debido a que el servicio de sanidad fue víctima del ataque de cibersecuestro de datos de WannaCry, o a los clientes que sufrieron de ansiedad cuando encontraron muchos artículos que desconocían en sus tarjetas de créditos. El coste de la ciberdelincuencia debería tener en cuenta, no solo las veces que se ha tenido que lidiar contra ataques, también el daño moral y el estrés que causa, que se desconoce. También está el coste de la oportunidad, cuando el tiempo y el dinero que se ha gastado en los ciberdelitos se podría haber gastado en algo más importante.

Existen otros costes sociales que aumentan debido a la ciberdelincuencia y a los ciberataques, como la divergencia de la sociedad –ya lo vimos aumentar con la interferencia de Rusia en las elecciones en EE UU de 2016–, la pérdida de la confianza en nuestras instituciones y la ruptura de alianzas. Cuantificar todos estos costes es un desafío: puede que sean invisibles, pero son reales.

A pesar de estos costes reales, más de la mitad de las 1.500 empresas encuestadas por el CSIS para su informe en 2020 dijeron que no tienen planes para prevenir y responder a un incidente cibernético. [3] Debido a la información insuficiente, es difícil evaluar el impacto real y los costos del delito cibernético. Responder a ciberdelitos y prevenirlos obliga a todos –personas y empresas– a seguir buenas prácticas y a comprender que ser víctima de delitos cibernéticos no debe considerarse un fracaso individual o un motivo de vergüenza.

En el proyecto CC-DRIVER, estamos llevando a cabo una evaluación del impacto socioeconómico del delito cibernético, en la que tendremos en cuenta los costos visibles e invisibles, teniendo en cuenta la observación de Carlin de que «hoy en día es imposible capturar realmente el costo del delito cibernético.» Además, nuestro consorcio concluyó recientemente un informe en el que se analizan las divergencias entre las tipologías de delitos cibernéticos y se recomienda una mayor armonización en este ámbito. Ello facilitaría una evaluación más precisa de los costos del delito cibernético a escala mundial.

Independientemente del coste real, podemos comprobar sus alucinantes proporciones. Por desgracia, la carga de estos costes recaerá no sólo en el gobierno y las empresas, sino también en todos los demás. Además, por desgracia, los ciberdelincuentes pueden causar enormes daños sociales y económicos con poco retroceso - por lo que nos incumbe a todos –gobiernos, empresas, universidades, los medios de comunicación, los ciudadanos– estar constantemente alerta ante los ciberdelitos y los ciberataques y presionar para obtener opciones políticas disuasorias eficaces.

Póngase en contacto para más información sobre el proyecto y para más noticias, regístrese en nuestro boletín y síguenos en Twitter y LinkedIn.

Notas

[*] En su informe de diciembre del 2020, el coste que estimaron era mayor de 1 billón de dólares.

Bibliografía

[1] Carlin, John P., *Dawn of the Code War*, Public Affairs, New York, 2018, p. 88. [2] *EU Cybersecurity Strategy*, Brussels, Dec 2020, p. 3. [3] Zhanna Malekos Smith and Eugenia Lostri, *The Hidden Costs of Cybercrime*, CSIS and McAfee, 2020, p. 4.