Masterhacks – “Israel es probablemente el país mejor protegido del mundo contra el fenómeno hacker hoy”, dijo el CEO de Kaspersky Lab. «Pero dadas las amenazas que enfrenta, no puede ser autocomplaciente».

Eugene Kaspersky afirma que los ciberataques van a empeorar y se verán afectadas las infraestructuras civiles vitales como la electricidad, telecomunicaciones y transporte, ya que serán blancos para las batallas cibenéticas globales.

“Antes de arreglar el ciberespacio, para hacerlo intrínsecamente seguro e inmune a los ataques, es probable que la situación de seguridad empeore con todos los miles de dispositivos y sistemas vulnerables que se desarrollan y producen todos los días”, afirmó Eugene, de 51 años y CEO de Kaspersky Lab en una entrevista por correo electrónico antes de la apertura de las nuevas oficinas de su empresa y centro de I + D en Jerusalem el miércoles.

“El peor de los casos es que un ataque a la infraestructura crítica tenga éxito. Me temo que el riesgo de un ataque así sigue siendo alto”, agregó.

Estas advertencias se dan entre la aparición de informes que afirman que el software malicioso llamado Crash Override o Industroyer, fue responsable del apagón en 2016 en Uncrania. Las dos compañías que descubrieron el software malicioso fueron ESET y Dragos Inc, y ambas advirtieron que el malware se podría modificar fácilmente para dañar operaciones de infraestructura crítica en todo el mundo.

“Alcanzar un nivel muy alto de seguridad es posible, pero requiere esfuerzos serios”, dijo Kaspersky en una sere de comentarios enviados por correo electrónico. “Los operadores de infraestructura crítica deben actualizar constantemente sus sistemas de seguridad utilizando inteligencia y tecnologías de amenaza de vanguardia. Yo recomendaría tener auditorías periódicas de seguridad”.

Afirmó también que la seguridad de estos sistemas debería ser «una cuestión de prioridad nacional, porque su protección es una cuestión de seguridad nacional».

Por otro lado, respecto a las sospechas de Estados Unidos sobre actividades en la empresa, Kaspersky aseguró que las preocupaciones «simplemente no están basadas en hechos. Hemos estado en este negocio durante 20 años, y siempre hemos sido un jugador responsable. Estamos listos para ofrecer nuestro código fuente para su revisión en los EE.UU. Es algo que ya hemos hecho con grandes contratos gubernamentales en otras partes del mundo; no es un problema para nosotros".

"Estamos trabajando muy duro para asegurar que nuestros productos y servicios hagan la vida de los hackers mucho más difícil, no más fácil", agregó.

Cabe mencionar que una ciberguerra es de mucho interés para las empresas de seguridad cibernética, y como prueba se tiene que las acciones de todas las grandes empresas de seguridad informática comercializadas en Estados Unidos, aumentaron de valor en mayo, debido al ataque del ransomware WannaCry que afectó a más de 150 países.

"Los cuentos sobre las compañías antivirus que escriben virus son tan antiguos como la propia industria", dijo el experto.

"Es cierto que la gente no nos necesitaría si no hubiera malware o cibercrimen. Pero, por desgracia, sí existen. Y hay tantos problemas de seguridad en los sistemas de Tecnología de la Información que el mercado seguirá creciendo de todos modos", añadió.

Agregó que es imposible atacar al cibercrimen sin cooperación. El problema se agrava por la falta de confianza entre las naciones.

"No vemos mucha confianza en las relaciones internacionales hoy, y me temo que como resultado hay una clara falta de cooperación entre los países", aseguró Kaspersky.