El Foro Económico Mundial dice que los países subestiman el riesgo de ciberataques

Los ciberataques son uno de los riesgos más graves a los que se enfrenta la economía global, según el informe del Foro Económico Mundial de 2016 sobre el riesgo

Bill Goodwin Computer Weekly 15 de Enero de 2016

Acceso a la noticia en:
http://www.computerweekly.com/news/4500270873/Countries-underestimate-risk-of-cyber-attack-says-WEF

El Foro Económico Mundial (WEF) advirtió que la mayor parte de las economías del mundo están subestimando el efecto potencial de los ciberataques a sus empresas y sus economías.

Un importante estudio realizado por el Foro Económico Mundial revela que, con la excepción de los EE.UU., la mayoría de los países han subestimado los riesgos de ciberataques en su bienestar económico.

Esta advertencia se hace a los líderes empresariales, políticos y organizaciones académicas y no gubernamentales que vienen a preparar la cumbre de Davos del 20 al23 de enero de 2016 **para discutir la "cuarta revolución industrial" y el impacto global de las nuevas tecnologías.**

La Tecnología tendrá un papel vital en el control de enfermedades, vigilancia del cambio climático y el crecimiento económico, pero también presenta nuevos retos.

El informe sobre Riesgos correspondiente a 2016 del WEF (*Global Risks Report 2016*) reveló que empresas de todos los tamaños se han visto afectados por ciberataques complejos, y han sufrido daños económicos, legales y reputacionales.

Costo del cibercrimen

Los estudios demuestran que el cibercrimen costó a la economía mundial **445bn £ en 2014.** Los costos serían mucho mayores si se tuviera en cuenta el espionaje económico y el hacking patrocinado por los Estados.

Sin embargo, sólo ocho economías han llegado a la conclusión de que los ciberataques son un riesgo que ha de tenerse en cuenta con la más alta preocupación: Estonia, Alemania, Japón, Malasia, Países Bajos, Singapur, Suiza y EE.UU..

Los resultados revelan una falta de apreciación por los efectos del cibercrimen en el resto del mundo, dijo John Drzik, presidente del Centro Global de Riesgos de Marsh & McLennan, y uno de los contribuyentes al informe de riesgo.

Según Drzik, las empresas estadounidenses son más conscientes de los riesgos informáticos porque los requisitos legales para reportar violaciones de seguridad han calado en las mentes

de los líderes de las compañías. Y como resultado, el 90% del seguro informático del mundo se toma en los EE.UU.

"Creo que va a haber una regulación parecida [fuera de los EE.UU.], y que va a desencadenar el crecimiento del mercado de seguros y traer más atención en el ámbito empresarial", dijo.

El informe advierte de que la amenaza del sofisticado espionaje, patrocinado por los gobiernos, excede la capacidad de las empresas para defenderse.

Crece el riesgo de ciberguerra[1] (Guerra informática)

Durante el último año, el número e impacto de los ciberataques se ha incrementado. Los hackers están volcando su atención en los sistemas de control industrial, en la situación de las plantas de energía, el transporte y otras infraestructuras en riesgo, dijo Drzik a Computer Weekly.

"Recientemente ha habido un ciberataque en Ucrania en una planta de energía y un sistema de control industrial. Hubo ataques anteriores en Alemania, en los sistemas de fabricación, y también hay ataques no denunciados", dijo.

Cada conflicto futuro tendrá un elemento-ciber y algunos pueden combatirse en su totalidad en el ciberespacio, dijo el WEF. Las infraestructuras físicas para el intercambio de datos, tales como cables submarinos, también podrían convertirse en blanco de los conflictos internacionales.

Aunque los grupos terroristas aún no han informado de realizar acciones de ciberguerra, esto puede cambiar en el futuro. "Por supuesto que veo al crimen organizado - una forma diferente de terrorismo - participando en este ámbito", dijo Drzik.

Riesgo reputacional

Los ataques de hackers, que han ocasionado pérdida de información confidencial, han tenido costes de millones de dólares para algunas empresas, - pero las empresas han perdido mucho más a través del daño a su reputación.

"Si su base de clientes comienza a preocuparse porque usted es poco fiable y no puede proteger los datos confidenciales, pueden irse a una empresa diferente - el amplificador de reputación puede ser enorme", dijo Drzik.

Algunas empresas han invertido en tecnología sofisticada para monitorizar y detectar violaciones de la seguridad. Sin embargo, dijo Drzik, las empresas se dan cuenta que no pueden prevenir todos los ataques y gastarán más recursos para mitigar y gestionar los efectos de un ataque.

[1] https://es.wikipedia.org/wiki/Guerra_inform%C3%A1tica

Carrera de armas informáticas

"No estamos sólo ante una carrera de armas informáticas entre países, sino que también entre la comunidad de seguridad y los hackers. Si usted está en el lado de la defensa, está tratando de prepararse para poder salir adelante ante un posible ataque, pero va a ir y venir, pues esta situación no va a desaparecer ", dijo Drzik.

El Foro Económico Mundial (WEF) advirtió que los riesgos políticos podrían afectar a la adopción de la tecnología digital, con cambios en la política y la inseguridad jurídica que dificulta la inversión en la última tecnología.

Aunque todos somos conscientes que los datos no conocen fronteras, sin embrago el régimen regulatorio está poco desarrollado, y carece de seguridad jurídica en áreas tales como la privacidad, la transparencia, el control de cifrado y las normas de propiedad intelectual.

Drzik dijo que las empresas necesitan un seguro más sofisticado contra los ciberataques y tendrán que ampliar las pólizas para cubrir la interrupción del negocio y los daños a la propiedad, ya que tales efectos podrán ser el resultado de los ataques contra los sistemas industriales.

"No hay más demanda que la que se oferta, porque actualmente las aseguradoras se están preparando para suscribir volúmenes más grandes de riesgo informático y están llegando a enfrentarse con el carácter de tales riesgos", dijo

Los cinco riesgos globales más importantes

1. Migración involuntaria a gran escala
2. Fenómenos meteorológicos extremos
3. Fallos para mitigar y adaptarnos al cambio climático
4. Conflictos entre Estados con consecuencias regionales
5. Las principales catástrofes naturales

Fuente: WEF: Most likely risks in 2016.

Read more on Hackers and cybercrime prevention

- Government drafts in civilians to fight cyber crime
- Only half of businesses ready to defend against cyber attack
- Automated bots drive cyber attack innovation
- Australian prime minister Malcolm Turnbull calls for free, open and secure internet