ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

45/2013 6 agosto de 2013

Mª José Caro Bejarano

MÁS SOBRE LA AMENAZA CIBERNÉTICA

MÁS SOBRE LA AMENAZA CIBERNÉTICA

Resumen:

La evolución tecnológica en el ámbito de las tecnologías de la información y la comunicación, las denominadas TIC o CIS en su acepción inglesa, han cambiado y continúan cambiando nuestra sociedad en la llamada aldea global.

Esta actividad tecnológica plantea múltiples dilemas, fruto de las distintas facetas que ofrece. Así, además del notable progreso para la humanidad, nos enfrentamos a las consecuencias de un mal uso, intencionado o no, de estas tecnologías, a todos los niveles, gubernamental, empresarial, de la ciudadanía, etc.

En este documento se estudian varios ámbitos que se ven afectados por el uso de estas tecnologías, así como su respuesta y concienciación ante las mismas.

Abstract:

The technological development in the field of Information and Communication Technology, ICT and CIS in Spanish, have changed and continue changing our society in the so-called global world. This technological activity raises many dilemmas, as the result of the different sides. Thus, besides the remarkable progress for the humanity, we face the consequences of misuse of these technologies, intentional or not, at all levels, government, business, citizenship, etc

Palabras clave:

Tecnologías de la Información y Comunicación, TIC, ciberamenaza, ciberataque, ciberseguridad, infraestructuras críticas.

Keywords:

Information and Communication Technology, ICT, cyber threat, cyber-attack, cyber security, critical infrastructures

MÁS SOBRE LA AMENAZA CIBERNÉTICA

Como refleja la sexta edición del Informe Anual "La Sociedad en red 2012 (edición 2013)" elaborado por el Observatorio Nacional de las Telecomunicaciones y la Sociedad de la Información (ONTSI)[1] de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información presentado a principios de julio de 2013:

- la cifra de internautas mundiales en 2012 se estima en 2.493 millones, con un crecimiento interanual del 10,7 %.
- crece la banda ancha móvil como tecnología de acceso a Internet, con 1.529 millones de líneas que suponen un crecimiento del 33,5 % en 2012.
- la banda ancha fija en el hogar está presente en el 72% de los hogares europeos.
- el gasto registrado en los hogares españoles en telefonía fija, telefonía móvil, Internet y televisión de pago en el cuarto trimestre de 2012 alcanzó los 3.155 millones de euros, lo que acumula un total de 13.308 millones durante todo el año.
- en 2011 en España, el sector TIC y de los Contenidos alcanzó una cifra de negocio de más de 100 mil millones de euros.

Estos datos de este informe a nivel europeo, que están contrastados y armonizados en un contexto internacional, permiten disponer de métricas comparativas con los países de nuestro entorno. Estos datos nos proporcionan una medida del grado de implantación y difusión de las TIC en el ámbito europeo y español, como ejemplo de lo que sucede en el resto del mundo.

LA PREOCUPACIÓN CIBERNÉTICA EN LAS EMPRESAS

Según un Informe de Lloyd's e Ipsos, Risk Index 2013[2], elaborado de forma conjunta con varios institutos internacionales, los ciberataques se han convertido en una de las cinco principales preocupaciones de las grandes empresas de todo el mundo, cuando hace dos años se subestimaba su impacto. En la clasificación general que ofrece este informe los cinco mayores riesgos señalados por las compañías son:

- la alta fiscalidad, que del puesto 13 en 2011 sube al número uno
- la pérdida de clientes y cancelación de pedidos, principal riesgo en 2011 y ahora en la segunda posición

[1] Véase el informe en: http://www.ontsi.red.es/ontsi/
[2] Véase el informe en:http://www.lloyds.com/news-and-insight/risk-insight/lloyds-risk-index

- los posibles ciberataques, que del puesto 12 en 2011 escala al tercero en 2013
- los costes de materiales, y
- el exceso de una legislación muy estricta

En concreto para Estados Unidos, los ciberataques son la segunda preocupación de las empresas, justo por detrás de la fiscalidad, mientras que en Europa se situaron en el sexto puesto.

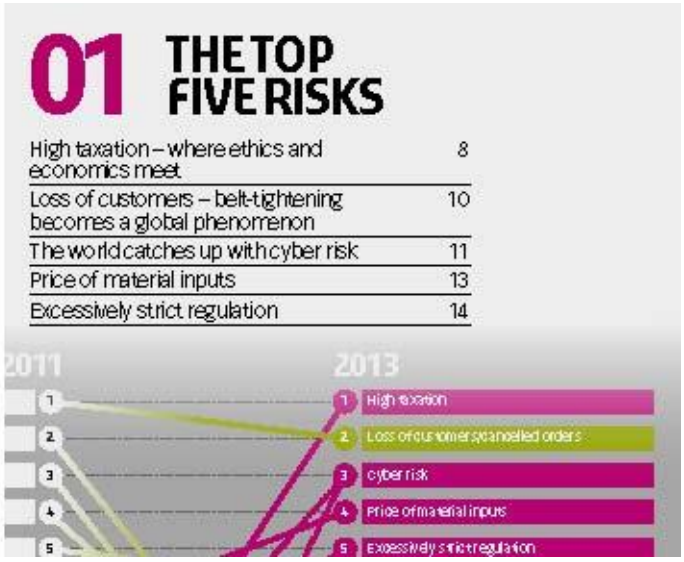

Figura1. Los cinco riesgos principales. Lloyd's Risk Index 2013.

El cambio en la valoración de los ciberataques puede deberse a que ha evolucionado la percepción de la motivación de los ciberataques, desde la delincuencia financiera a los ataques políticos e ideológicos. 2012 ha presenciado ataques a los sitios web de la Interpol, la CIA, empresas como Boeing, el robo masivo de contraseñas de la red profesional LinkedIn, la interrupción de los sitios web de los seis principales bancos de Estados Unidos y muchos más.

Además, crece el número de incidentes atribuidos a actos de piratería patrocinados por Estados y los ataques de venganza por redes de hacktivistas. De igual modo crece el coste de las infracciones cibernéticas. Un estudio de 2012 el Ponemon Institute[3] encontró que el coste promedio anual de 56 organizaciones de EE.UU. tomadas como punto de referencia era de 8,9 millones de dólares al año, en 2011 el coste fue de 8,4 millones de dólares, con un rango que osciló entre 1,4 millones hasta la asombrosa cifra de 46 millones de dólares por año y por empresa. Los ciberdelitos más costosos El

[3] Véase el informe en Ponemon Institute: 2012 Cost of Cyber Crime Study. www.ponemon.org/library/2012-cost-of-cyber-crime-study

más costoso ciberdelitos fueron los que involucran códigos dañinos, denegación de servicio y ataques a las bases de datos web.

La propia comisaria europea de Agenda Digital de la UE, Neelie Kroes apunta que "La ciberseguridad es demasiado importante para dejarla al azar, a la buena voluntad de las empresas", y "muchos gobiernos han avanzado en esta cuestión en los últimos dos años".

En mayo 2013, senadores republicanos y demócratas se reunieron para frenar con una ley[4] el robo de datos comerciales valiosos de empresas estadounidenses por parte de empresas y gobiernos extranjeros. La Comisión Europea, por su parte, se está planteando. La Comisión Europea, por su parte, está considerando imponer sanciones para garantizar que las empresas que almacenan datos en internet informan de la pérdida o robo de los datos personales información.

De acuerdo con un informe publicado en abril de 2013 por el Insurance Information Institute[5], el 39% de las brechas de datos se debe a la negligencia de empleados, el 24% a fallos del sistema y el 37% a ataques delictivos. Esto deja casi dos tercios de los incidentes a causas que tienen que ver con el control del negocio.

Al igual que en 2011, habría que preguntase si, a pesar de la escalada del gasto en ciberseguridad, las empresas están realmente invirtiendo dinero correctamente. Los especialistas en seguros cibernéticos están ofreciendo ciber-productos cada vez más integrados, incluidos los que proporcionan cobertura para los gastos de brechas de datos, análisis forense y crisis de los servicios de relaciones públicas en un solo paquete. Si bien estos productos son altamente eficaces en caso de emergencia, la inversión previa en la gestión del riesgo – junto con la garantía de se aplican las recomendaciones en toda la empresa – tiene un largo camino hasta prevenir un desastre cibernético antes de que comience.

LOS CIBERATAQUES APUNTAN A LAS BOLSAS DE VALORES

Las bolsas de valores del mundo también hacen uso de las TIC y por tanto, no se libran de ser objetivo de ciberataques. Cerca de la mitad de las Bolsas de valores del mundo fueron blanco de ciberataques el año pasado, según un sondeo a 46 de ellas, de acuerdo con un artículo de la agencia Reuters.

La frecuencia de los ataques y la naturaleza interconectada de los mercados crea el potencial de un enorme impacto, según recoge el documento del departamento de investigación de la Organización

[4] Véase H.R. 2281: Cyber Economic Espionage Accountability Act y S. 1111: Cyber Economic Espionage Accountability Act de 6 de junio de 2013.
[5] Véase el informe Insurance Information Institute: Cyber Risks: The Growing Threat, 8 April 2013. www.iii.org/assets/docs/pdf/paper_CyberRisk_2013.pdf

Internacional de Comisiones de Valores (IOSCO, por sus siglas en inglés[6]) y una oficina de la Federación Mundial de Bolsas de Valores (WFE, por sus siglas en inglés[7]).

Según el autor del informe: "Podría haber impactos sistémicos (...) desde ciberataques en los mercados de valores, considerando especialmente que nuestro sistema financiero depende cada vez más de la infraestructura tecnológica".

Entre las bolsas sondeadas, el 53% dijo haber experimentado un ciberataque el año pasado. Las formas más comunes fueron ataques de Denegación de Servicio (DDoS), que buscan cerrar sitios web y otros sistemas informáticos sobrecargando las redes de la organización atacada con un tráfico excesivo e incluso virus. Otras formas de ciberdelitos incluían el robo de ordenadores portátiles, modificación de sitios de Internet, robo de datos y robo de información privilegiada. Ninguna de las bolsas informó de robo financiero como parte de los ataques.

"El cibercrimen también parece ir en aumento en términos de sofisticación y complejidad, ampliando el potencial de infiltración y daños a gran escala", recoge el informe, agregando que un gran ataque podría crear desconfianza pública y una retirada de los mercados. En Reino Unido, los temores sobre ciberataques superaron a la crisis de la zona euro como el principal riesgo para los bancos del país, según un alto funcionario del Banco de Inglaterra. En Estados Unidos, los operadores de Bolsas Nasdaq OMX Group y BATS Global Markets dijeron en febrero del año pasado que recibieron ataques de denegación de servicio DDoS.

En octubre del 2011, el sitio web de la bolsa de Nueva York de NYSE Euronext estuvo inaccesible durante 30 minutos, según una compañía de vigilancia de Internet, aunque la bolsa no informó de interrupciones en su servicio. En 2010, piratas informáticos que se infiltraron en los sistemas informáticos de Nasdaq instalaron programas maliciosos que les permitían espiar a los directores de compañías que cotizaban en la bolsa, según reportó Reuters.

Existen datos limitados respecto a los costes que implica el cibercrimen para las Bolsas de valores, pero el informe asegura que varios estudios han estimado el coste para la sociedad en general entre los 388.000 millones y el billón de dólares. Las plazas que participaron en el sondeo dijeron que los costes directos e indirectos de los ciberataques les supusieron menos de 1 millón de dólares el año pasado.

LOS SISTEMAS DE CONTROL DE INFRAESTRUCTURAS CRÍTICAS EN EL PUNTO DE MIRA

El último documento del el CERT industrial de EE.UU. (Industrial Control Systems Cyber Emergency Response Team, ICS-CERT[8]), informa de más de 200 incidentes de seguridad en todos los sectores de

[6] Véase http://www.iosco.org/
[7] Véase http://www.world-exchanges.org/.
[8] Véase https://ics-cert.us-cert.gov/

infraestructuras críticas en la primera mitad del año 2013. El 53% de estos ataques ha tenido como objetivo el sector de la energía.

Como ejemplo, ICS-CERT pone de relieve un ataque realizado en febrero contra una estación de compresión de gas. Los agresores habrían intentado acceder a la red de control de procesos de la empresa con el lanzamiento de ataques de fuerza bruta. Después de recibir la notificación del ataque, ICS-CERT publicó 10 direcciones IP en el portal del US-CERT para advertir a otros gestores de recursos de infraestructuras críticas. Poco después, otros gestores de infraestructuras críticas empezaron a informar de incidentes similares y se identificaron un total de 39 nuevas direcciones IP maliciosas.

Ninguno de los intentos tuvo éxito, pero los incidentes pusieron de relieve la necesidad de una vigilancia constante, advertía el ICS-CERT.

La ciberseguridad de las infraestructuras críticas es un tema muy debatido en la actualidad, las ciberamenazas podrían alcanzar a países extranjeros y causar la pérdida de vidas humanas de forma idéntica a un ataque convencional, los gobiernos se enfrentan a una amenaza silenciosa e impredecible que podría ser llevada a cabo por hackers patrocinados por Estados o ciberdelincuentes con diferentes propósitos como sabotaje o ciberespionaje.

Los Equipos de Respuesta ante Emergencias (CERT) de todos los países se están aproximando al problema, se está trabajando para completar un censo de las infraestructuras que examina su nivel de seguridad, estos grupos también están trabajando en programas de sensibilización y el intercambio de información, actividades claves para mitigar los riesgos.

Recientemente el ICS-CERT publicó un informe que alerta sobre el creciente número de ataques contra las infraestructuras críticas de EE.UU. entre 2009 y 2011, que registra un crecimiento impresionante del número de incidentes. Este informe también proporciona una guía con las siguientes recomendaciones:

- Realizar censos detallados de las estructuras y las evaluaciones de clasificación del riesgo para identificar las principales vulnerabilidades y las ciberamenazas que puedan explotarlos.
- Definir, divulgar y adoptar las mejores prácticas para defender las infraestructuras críticas.
- Para hacer frente a las empresas de phishing se debe desarrollar un programa de capacitación en seguridad que preparará a los empleados frente a los ataques de posibles vectores y frente a las principales técnicas de ingeniería social.

En este escenario, se espera que el número de ataques se incremente también en los próximos años, sin embargo, el aumento del nivel de conciencia y el mayor interés en el asunto podría evitar graves consecuencias.

UNIRSE CONTRA EL CIBERENEMIGO COMÚN

Teniendo en cuenta en cuenta que tanto Estados, empresas, administración, ciudadanos somos objetivo de los ciberataques, diferentes propuestas abogan por compartir la información relativa a las características de los ataques con el fin de protegerse ante ellos. Los diferentes CERTs o Centro de Respuesta ante Emergencias Informáticas intercambian información en este sentido.

En otros casos se establecen alianzas gobierno-empresas para mejorar la ciberseguridad, es el caso de EE.UU. y últimamente del Reino Unido. Este país ha establecido una alianza con firmas de defensa y telecomunicaciones para mejora su ciberseguridad.

En concreto, nueve de los mayores fabricantes de armas del mundo y algunos proveedores de telecomunicaciones están asociándose con Gran Bretaña para mejorar la ciberseguridad del país, con el objetivo de abordar la creciente amenaza que representan los piratas informáticos y otros atacantes de ese estilo.

Gran Bretaña convirtió la ciberseguridad en una de sus prioridades de defensa nacional en 2010, citando la creciente amenaza de ciberataques por parte de delincuentes y grupos extranjeros con apoyo estatal. Compañías como BAE Systems, Rolls-Royce, Lockheed Martin y Hewlett Packard están entre las empresas que se asociarán para compartir información y abordar ciberamenazas, según el Ministerio de Defensa británico.

Las redes del gobierno y de la industria sufren unos 70 ciberataques sofisticados al mes, y el 15% son contra el sector de defensa, según el GCHQ[9], el centro de inteligencia del Gobierno que también participa en el plan.

La asociación se produce mientras contratistas como BAE aumentan sus negocios cibernéticos anticipándose a la creciente demanda de gobiernos y empresas, en un momento en que la demanda de equipos sufre por los recortes presupuestarios en defensa. La denominada Asociación de Protección de la Defensa Cibernética también tratará de aplicar controles y compartir la inteligencia sobre amenazas para mejorar la seguridad de la cadena de suministros de defensa. "Es una demostración clara de que el gobierno y la industria pueden trabajar juntos: compartir información, experiencias y conocimientos", dijo el ministro para el Equipamiento Apoyo y Tecnología de Defensa, Philip Dunne.

Otras compañías implicadas son Selex, unidad de Finmeccanica; Cassidian, división de EADS, Thales, CGI Group y BT Group[10].

[9] Véase http://www.gchq.gov.uk/Pages/homepage.aspx
[10] Véase noticia de Europa Press 8/7/2013.

CONCLUSION

Como se visto con esta serie de ejemplos que afectan a empresas, al mundo financiero, las infraestructuras críticas, todas ellas pero también los gobiernos y los ciudadanos están en el punto de mira de los ciberataques. Las empresas estratégicas que son objeto de ataque y las de ciberseguridad con el conocimiento y capacidad de prevenir y mitigarlos empiezan a colaborar con los gobiernos para intercambiar información relativa a los ciberataques que permita ejercer una defensa común y compacta ante una amenaza que ha llegado para quedarse y evoluciona a ritmo exponencial en complejidad y número de objetivos, así como en el impacto de los ataques.

Mª José Caro Bejarano
Analista Principal IEEE