ARTÍCULO

Amenazas cibernéticas y riesgo de proliferación en el área de logística: un resumen del problema

Cyber threats and risk of proliferation of threats in the area of logistics - an outline of the problem

Monika Szylkowska, Phd

Universidad Militar de Tecnología, Varsovia, Polonia. Facultad de Logística, Departamento de Seguridad y Defensa. monika.szylkowska@wat.edu.pl

Anales de la Real Academia de Doctores de España. Volumen 4, número 1 - 2019, pp. 5-15.

RESUMEN
El artículo presenta consideraciones seleccionadas en el área relacionada con las amenazas cibernéticas y el riesgo de proliferación de peligros en el área de logística. Indica ejemplos seleccionados, ilustrando la escala de los riesgos potenciales en esta esfera y las lagunas identificadas en esta área.

ABSTRACT
The article presents selected considerations in the area related to cyber threats, risk and risk of proliferation of threats in the area of logistics. Indicated selected examples, illustrating the scale of the potential risks in this sphere and identified loopholes in this area.

PALABRAS CLAVE: Comunicación audiovisual, prestadores de servicios audiovisuales, cine, inversión, directiva, derecho

KEYWORDS: cyberthreats, logistic, risk, proliferation of threats

El mundo global, dinámico y digital de hoy está generando nuevas oportunidades, desafíos, riesgos y amenazas en todos los aspectos. La revolución técnica y tecnológica se ha convertido en un determinante del nivel de desarrollo y crecimiento. Actualmente, no solo en todos los aspectos de la vida y el funcionamiento de individuos, empresas, organizaciones y estructuras de estados, sino también las alianzas internacionales son un aspecto inseparable del ciberespacio, por lo tanto están en un grado menor o mayor - dependiente e interrelacionado con él.

El sector de las Tecnologías de la Información y la Comunicación (TIC) es un Sistema que consiste en partes como hardware, software y servicios de TI. El uso de lo moderno. Los sistemas mejoran y soportan numerosas tareas y procesos complejos en el ámbito de logística (por ejemplo, gestión de inventario, planificación de suministros, servicio al cliente, etc.). El uso y la implementación de soluciones modernas es hoy en día una condición “sine qua non” para el funcionamiento, asegurando la competitividad de una empresa. En la era de la globalización, el mercado logístico también está sujeto a un desarrollo dinámico, por un lado, adaptándose a cambios que ocurren, por otro, sin embargo, con el objetivo de superar y luego responder a las necesidades y expectativas de los clientes. Competente y, lo más importante, eficiente y cooperación óptima de todas las cadenas de enlaces en el ámbito de la logística que es posible gracias a los modernos sistemas que procesan los datos y la información. El papel y la importancia de la información en el mundo moderno no requiere ninguna justificación, ya que es el recurso más valioso. En todas las áreas y campos, en términos de economía, *la gestión de la información y su calidad son factores clave para la competitividad*

Parece interesante que, como principio, **el concepto de información en** sí mismo no es **definible**[1], aunque "acompaña al hombre y su actividad desde los albores del tiempo". Sin embargo, independientemente de la definición elegida, la información tiene algunas características.

Entre las de mayor importancia se encuentran: relevancia, precisión, actualidad, integridad, coherencia, calidad, credibilidad y seguridad.

[1] Fuente: www.encyklopedia.pwn.pl. Acceso: 21.11.2018 r.

1. CLASIFICACIÓN GENERAL Y RETOS QUE SE IMPLICAN EN LA LOGÍSTICA

La importancia de la información y los riesgos potenciales a ella están determinados por el lugar de su funcionamiento, es decir, principalmente sistemas de telecomunicaciones, que implican diferentes tipos de amenazas digitales. El denominado *crime* de la "nueva generación" es el resultado del desarrollo de la civilización y la revolución informática, por lo tanto, es un tema extremadamente dinámico y, en consecuencia, sujeto a cambios constantes.

El ciberespacio suele definirse como el espacio de comunicación en el que se digitaliza la información que opera. Dicha información es generada, procesada, archivada y transmitida en tal espacio. El ciberespacio es un área que conduce, por una parte, al desarrollo, y por otro lado, genera amenazas como la ciberdelincuencia, **[1]**. Estas amenazas están estrechamente relacionadas al área económica, ya que son empresas las que a menudo son víctimas de ataques digitales (especialmente fraudes o demandas de rescate).

Teniendo en cuenta el hecho de que la información, la comunicación y la tecnología (TIC) es actualmente crucial en términos de logística ampliamente definidos, siendo un componente importante en el proceso de lograr una ventaja competitiva por parte de los individuos. Las entidades, siendo las empresas en el campo de la logística una de las partes más innovadoras. En el ámbito de las TIC, las posibles amenazas digitales no solo pueden ser cruciales para los conceptos básicos de su funcionamiento, sino también en los procesos económicos. Dentro de las soluciones existentes, uno puede encontrar tanto las típicas (utilizadas en diversas industrias) como las soluciones que están estrictamente especializadas, dedicada a sectores específicos. Los principales grupos de sistemas de apoyo logístico incluyen: los que apoyan la cooperación entre entidades, aquellos que apoyan el funcionamiento de una entidad, y soluciones que proporcionen los medios para rastrear y monitorear envíos y vehículos, iCargo, e-Fraght, etc.

Independientemente del área, dominio o nivel de avance de las herramientas y tecnologías utilizado, los peligros de la información digitalizada siguen siendo un problema común. En la comunicación para la Comisión al Parlamento Europeo, al Consejo y al Comité de los Estados miembros COM (2007) 267 **[2]** sobre la estrategia general para combatir el *crime* cibernético, coexisten tres aspectos básicos han sido clasificados en tipos de delitos informáticos: 1. Formas tradicionales; 2. Publicaciones ilegales de contenido en medios electrónicos y 3. Delitos "típicos" dentro de la red. Formas tradicionales que incluyen el fraude y la falsificación, pero con el uso de redes informáticas electrónicas y sistemas de información (un ejemplo

de los cuales son estafas masivas, robo de identidad y *phishing)*. El segundo grupo incluye en particular sitios web que contienen contenido ilegal (por ejemplo, odio, incitación a actos terroristas, etc.). Los delitos "típicos" incluyen la piratería, ataques, ciberataques, ataques DDoS.

La ciberdelincuencia en su amplio alcance se puede utilizar para definir una acción que tenga efectos negativos causados en el espacio de procesamiento e intercambio de información, creado por sistemas TIC. Por lo tanto, se consideraría un acto en un entorno digital que pretende o podría interrumpir, neutralizar o detener el funcionamiento de los sistemas de TIC, resultando tanto del acto y el abandono de lo humano (usuario).

Dado lo anterior, los principales grupos de amenazas cibernéticas incluyen:

a) Los resultantes de actividades humanas:

- intencional (ciberdelincuentes virtuales y reales, un ejemplo de los cuales es el robo o el daño causado al equipo).

- no intencional [personal no capacitado, inconsciente o despreocupado].

b) Los que resultan del entorno natural [como un desastre natural que resulta en la falta de poder].

c) Los no relacionados con actividades humanas intencionales [errores de sistemas, errores de software, fallas en la fuente de alimentación].

d) Mixto / híbrido.

Las principales amenazas a la emisión de noticias para cada entidad incluyen en particular:

- Falta de información.
- Falta de información adecuada (en el momento, lugar y destinatario correctos).
- Información incorrecta, imprecisa o falsa (costos exagerados, costos subestimados, etc.).

Pero también:

- Robo de información (sobre competencia en el mercado: particularmente producto nuevo, nueva estrategia, etc.)
- Destruyendo o modificando la información.

Se debe enfatizar en los sistemas desprotegidos o vulnerables que pueden desencadenar cualquier forma de los ejemplos de amenazas antes mencionados.

Pérdidas por la falta de posibilidad de tramitación de información o la falta de flujo de información aumenta los costos totales, incluyendo el tiempo de inactividad, reparaciones y restauraciones necesarias, pero también pérdidas futuras de beneficios debido, por ejemplo, a la falta de la base de clientes (y sus ventas en el mercado negro), así como también superan los costos de seguridad. Sin embargo, la pérdida mayor e incalculable para cualquier entidad es la pérdida de la reputación.

2. TIPOS DE AMENAZAS

La clasificación general de las amenazas está determinada principalmente por su identificación. Debido al criterio aceptado - una división se puede hacer en grupos individuales - el principal, que puede incluir: amenazas internas y externas. Entre ellas, se distinguen las siguientes: política, económica, social, natural (incluso ecológica). Por lo tanto, un criterio de amenazas puede ser adoptado para un tema dado, entonces la división en amenazas internas y externas pueden ser sometidas a una identificación más detenida, incluyendo el área de funcionamiento y condiciones ambientales específicas. Las amenazas internas (la fuente se encuentra en un tema dado) puede incluir, por ejemplo, errores de dispositivos, ataques deliberados por parte de empleados o personas no intencionadas. Errores debido al tipo de razón causada por las amenazas, se pueden distinguir:

a) No intencional - resultante de causas aleatorias o causada por errores del empleado.

b) Intencional: ser el resultado de una actividad humana consciente.

Debido al tipo de pérdidas incurridas, se pueden distinguir los siguientes riesgos: no causantes de pérdidas financieras y amenazas que las causan. El alcance y significado de las consecuencias de amenazas puede determinar una clasificación adicional, por ejemplo: significativas, o que causen interrupciones en el funcionamiento del sujeto, e incluso: amenazando con una mayor existencia.

3. EJEMPLOS SELECCIONADOS QUE ILUSTRAN LA ESCALA DE LOS RIESGOS POTENCIALES

Dada la variedad de tipos y naturalezas de amenazas, por razones objetivas, solo las seleccionadas se discutirán en el artículo.

Según el informe de Kaspersky Lab en 2016:

- El 49% de las empresas encuestadas había experimentado un ataque dirigido.
- El 50% experimentó un ataque de ransomware (un software que bloquea el acceso a datos y exige un rescate, en el 20% de los casos se bloquearon los datos).
- El 48% de los encuestados encontró un incidente de violación de seguridad debido al personal despreocupado.

Las falsificaciones digitales son un primer ejemplo de esto, se pueden dividir en las siguientes subcategorías **[3]**:

a. realizado con el uso de software malicioso,
b. realizado con mensajes falsos (correos electrónicos);
c. híbrido (correos electrónicos falsos que contienen software malicioso o enlaces a dichos programas).

La siguiente ilustración muestra un correo electrónico falso que contiene información sobre el supuesto envío:

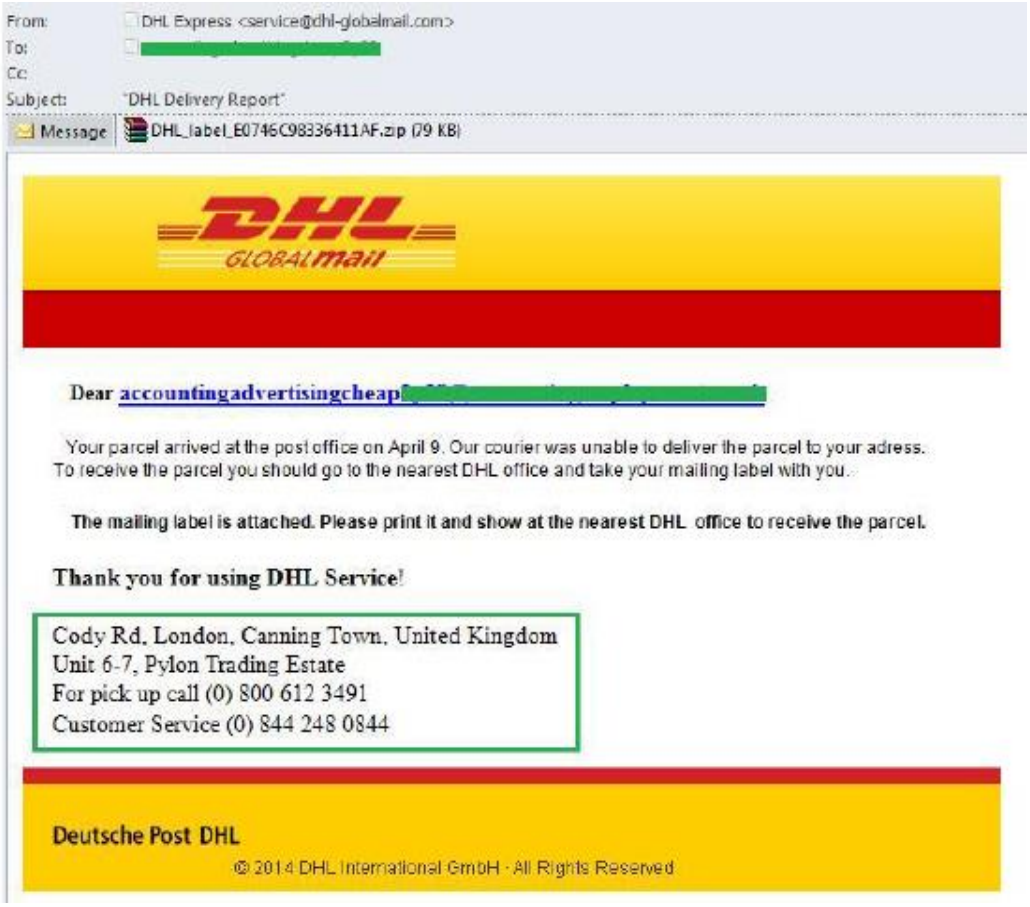


Fig. 1. El contenido del mensaje falso que contiene información sobre el supuesto envío
Fuente: https://securelist.com/scammers-delivery-service-exclusively-dangerous/66515/ Acceso: 8.12.2018

Además, el archivo adjunto al mensaje (llamada extensión de archivo, por ejemplo, .doc, .docx, .pdf) se supone que sugiere un documento de texto que, de hecho, contiene un programa *malicioso* y está destinado a engañar al usuario para abrir el archivo. *Crime* híbrido: fraude y engaño que puede ser clasificado como un ataque de phishing (debido a sus métodos de operación: engañar a un usuario y obligarle a realizar ciertas acciones) - es un tipo particular de actividad criminal que implica estafa, con el dinero que se envía a una cuenta bancaria falsa. El acto consiste en la falsificación de un mensaje que contiene información sobre el cambio de una cuenta de un negocio financiero existente a una nueva, que debe utilizarse para transferir las finanzas. Comúnmente, la información está contenida en un archivo que presenta todos los datos personales de la entidad, incluida la firma de la persona autorizada (ej. el presidente). También llama la atención por la facilidad con la que las entidades comparten libremente archivos y documentos legales en sus sitios web, por ejemplo, referencias sin ninguna medida de seguridad (por ejemplo, marcas de agua), o incluso sin borrar los sellos. Recientemente, las víctimas de este tipo de delito fueron una de las ramas de Autoridad de Carreteras de la Provincia, donde un empleado del departamento financiero transfirió 3.7 millones pln a una cuenta bancaria falsa. En este caso, el *malware* no se utilizó para cometer el delito, el empleado pensó en un documento falso.

Un ejemplo de falsificación de *malware* es American Mega Metals Company: los delincuentes infectaron una computadora del agente que trabaja para la compañía y enviaron un mensaje a la entidad, en relación con el cambio en el número de cuenta del proveedor. La credibilidad de los mensajes recibido de la dirección de correo electrónico real relacionada con pedidos reales ha causado que el destinatario transfiera fondos a la cuenta bancaria designada. El fraude solo fue descubierto cuando un verdadero proveedor envió un aviso de facturas impagas por un total de 100,000 $.

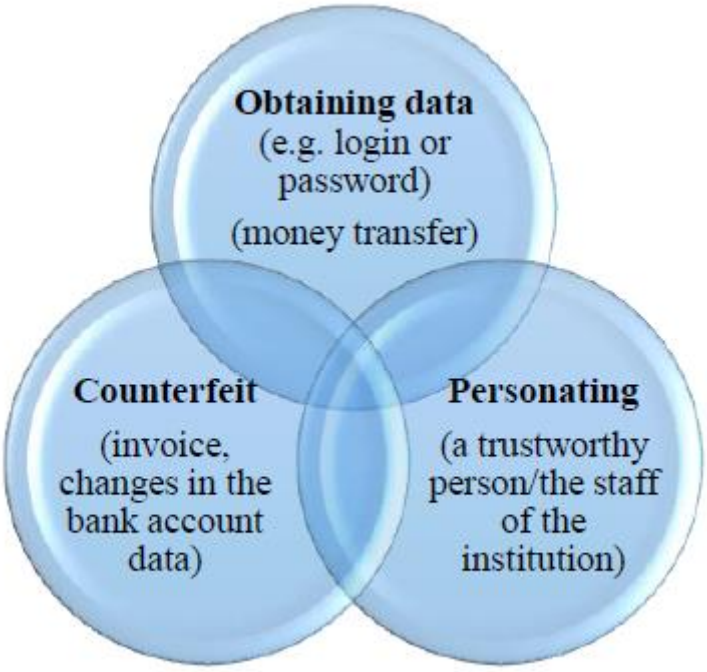
Otro ejemplo son los ataques de *ransomware* o susceptibles de rescate. *Ransomware* es un tipo de *malware* que cifra los datos en una computadora infectada o bloquea el acceso a ella, incluido el mensaje con instrucciones que se muestran en la pantalla: el rescate se debe pagar para recuperar datos o un acceso a ellos. Según una investigación realizada por Kaspersky Lab en 2016, la frecuencia de ataques a entidades que utilizan este tipo de software ha aumentado tres veces, es decir, uno cada 40 segundos (1 de cada 5 empresas) **[4]**.

La siguiente ilustración presenta un ejemplo de un resultado de un ataque de ransomware:

Fuente: https://www.enigmasoftware.com/prismyourcomputerhasbeenlockedransomware- Eliminación / Acceso: 8.12.2018.

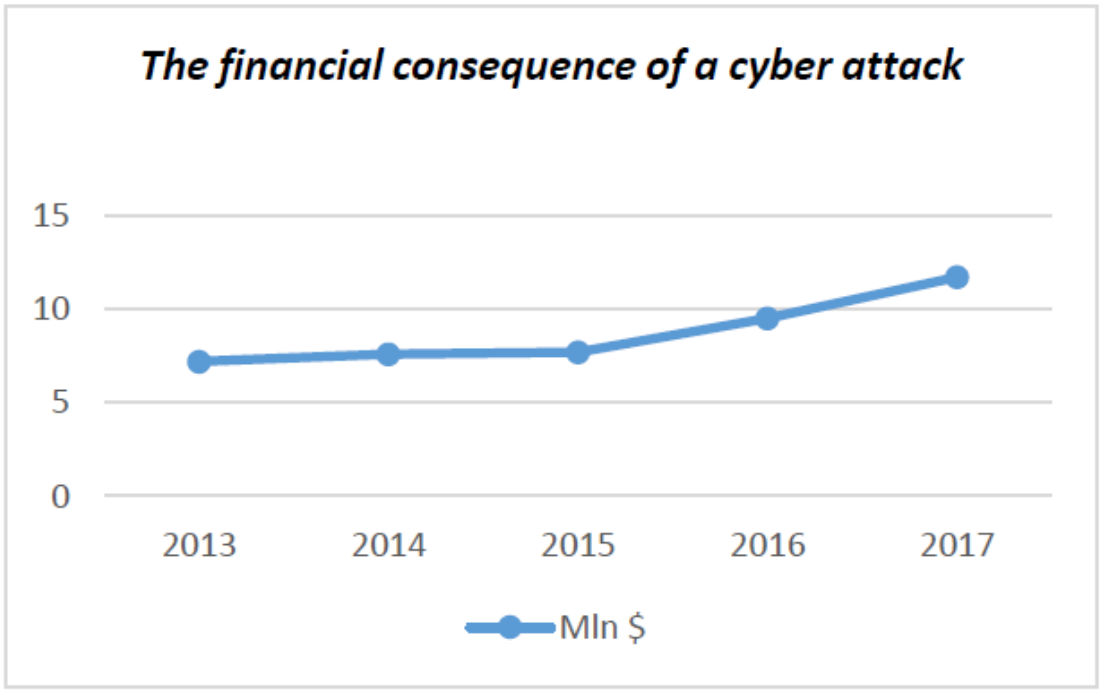
Para resumir los ejemplos mencionados anteriormente, se puede observar que su denominador común es el hecho de que los ciberdelincuentes utilizan tanto la ignorancia como el desconocimiento de los usuarios de TI. Dado que, es la razón más común de superar la protección contra todas las formas de un ataque técnico mientras buscan el punto más débil del sistema de seguridad, ese es el humano **[5]**.

Métodos indicados:



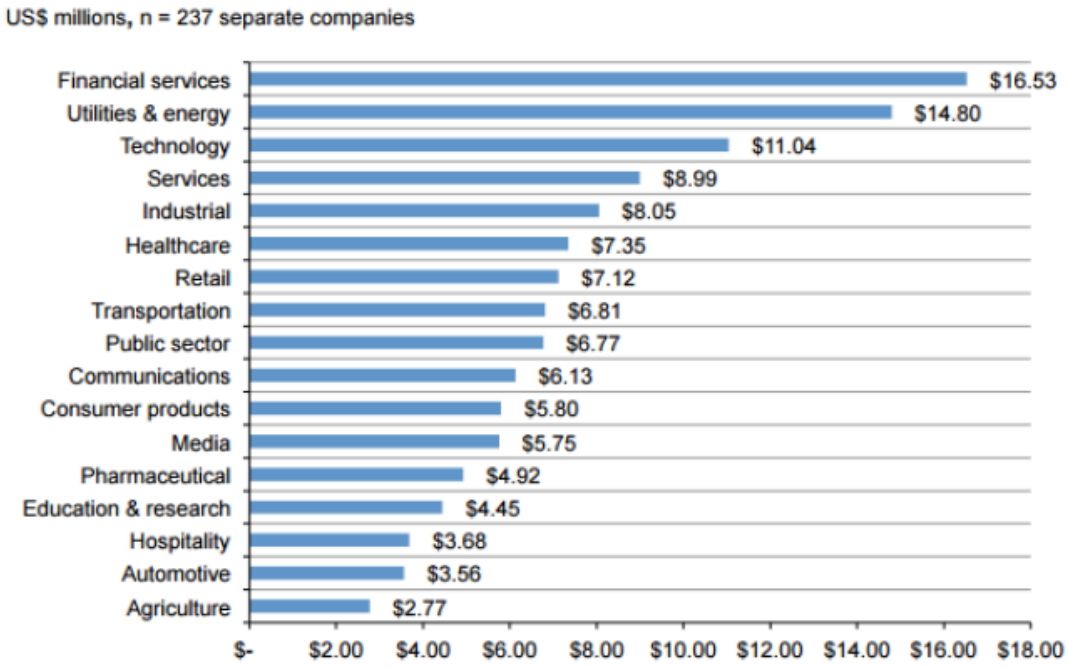
La compañía HP ha presentado los resultados de su encuesta anual, que indica que, a lo largo de los últimos tres años, la frecuencia de los ataques cibernéticos se ha más que duplicado y, como consecuencia de ellos las pérdidas financieras han aumentado en casi un 40 por ciento.

En una logística ampliamente definida, una parte primaria y fundamental son las entidades comerciales que constituyen enlaces individuales en la cadena. Esta es la causa de que cada entidad hasta cierto punto depende de otra (cliente del proveedor, etc.), por lo tanto cada materialización de las amenazas cibernéticas afectará a las demás. Según lo indicado por la investigación realizada por el Instituto Ponemon por encargo de Hewlett Packard Enterprise, actualmente la información del robo sigue siendo la causa de las mayores pérdidas (44% del costo externo total incurrido) como resultado de los delitos cibernéticos); interrupciones del funcionamiento de una entidad, o reducción de la productividad representa hasta el 30 por ciento de los costos externos.



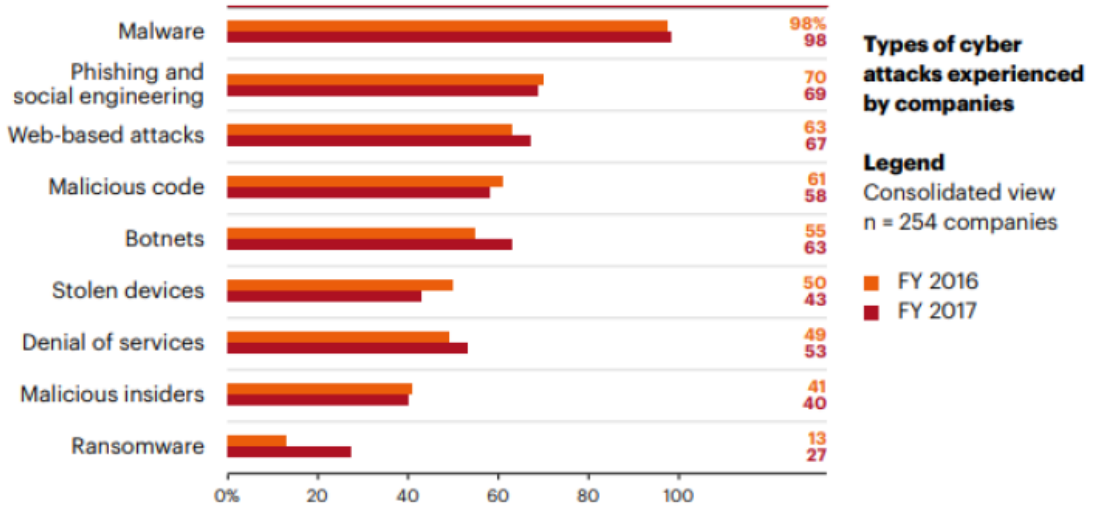
Basado en la fuente: https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61 / Accenture-2017-CostCyberCrimeStudy.pdf. Acceso: 8.12.2018 **[6]**

Se ha indicado que los costos del delito cibernético afectan a todos los sectores de la economía, como se ilustra en la siguiente tabla:



Fuente: http: //www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT% 20FINAL% 203.pdf Acceso: 7.12.2018.

Dentro de la misma investigación, los tipos más comunes de ataques cibernéticos incluyeron:



Fuente: Estudio del Costo del Delito Cibernético 2017, Ponemon Institute © Informe de investigación, https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf **[7]**

La proliferación de amenazas se puede hacer de forma dicotómica: indirecta o directa e intencional o no intencional. También puede tener lugar en combinaciones: intencional - directa, intencional - indirecto; no intencional - indirecto; no intencional - directo [por ejemplo, intencional o la apertura no intencional de un archivo adjunto que contiene códigos maliciosos, que en efecto infecta las redes corporativas completas.

BIBLIOGRAFÍA

[1] Sienkiewicz P. *Terroryzm w cybernetycznej przestrzeni*. W (eds.) Jemioła T., Kisielnicki J., Rajchel K.: Cyberterroryzm - nowe wyzwania XXI wieku. Wyższa Szkoła Informatyki, Zarządzania i Administracji, Warszawa 2009.

[2] Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Consejo. Comité de las Regiones - *Hacia una política general en la lucha contra el delito cibernético* {SEC (2007) 641} {SEC (2007) 642} Bruselas, 22 de mayo de 2007, http://eur.fm/legal-content/EN/TXT/?uri=CELEX:52007DC0267

[3] M. Szyłkowska, la *extorsión y falsificación* digital *como la principal amenaza para las empresas: la cadena de suministro,* GOSPODARKA MATERIAŁOWA i LOGISTYKA, 5/2016, PWE 2016, 716-727.

[4] Kaspersky Security Bulletin 2016, https://kas.pr/R3tY. Access: 21.03.2018.

[5] M. Szyłkowska, Ataques *socio-técnicos como una amenaza para el funcionamiento de las entidades públicas [en origen: Ataki socjotechniczne jako zagrożenie dla funkcjonowania jednostek publicznych*] [En proceso de publicación]

[6 y 7] https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

[8] Oleński J. *Ekonomika informacji. Podstawy*. PWE Warszawa, 2001.

[9] Hołubowicz W., Samp K., *Informacja i informatyka w logistyce*. www.logistyka.net.pl/.../Kongres2008-w3-ref-A-1.pdf.

[10] Susłow W., *Od organizacji do systemu informatycznego. Modelowanie i analiza systemów informatycznych.* http://moskit.weii.tu.koszalin.pl/~swalover/MiASI_w1.pdf.

[11] Graczyk M. *Projektowanie podsystemu wspomagania decyzji w systemie informacyjnym aglomeracji.* http://repozytorium.put.poznan.pl/Content/294223/Magdalena_Graczyk_(...).pdf.

[12] Gozdek J., *Hakerzy bez granic* , CHIP 11/2015.

[13] Portal internetowy Encyklopedii Polskich Wydawnictw Naukowych: encyklopedia.pwn.pl.

[14] Revista Niebezpiecznik.pl. http://niebezpiecznik.pl

[15] Revista CHIP 11 / 2015.http: //www.chip.pl