Artículo

Ciberseguridad y crímenes informáticos: el lado oscuro de la red

Carlos Miguel Arce Sáenz
Máster en Gerencia de Proyectos
Experto en Ciberseguridad
Docente del Programa
Técnico Superior en Dirección de Proyectos
Sede Central, Alajuela
Universidad Técnica Nacional
carcesa@utn.ac.cr

1. Resumen

El presente artículo reflexiona acerca de la ciberseguridad o la seguridad de la información, un tema que cobra gran relevancia en la actualidad, ya que para el año 2015, los ciberataques reportaron más ganancias que el tráfico de drogas. Sólo en el 2018 las ganancias del cibercrimen alcanzaron los $1.5 trillones. El enfoque principal del artículo se centra en la necesidad de capacitar a las personas y empresas, para que puedan proteger su información, ya que han aumentado los incidentes y robo de la información, por lo que se han vuelto muy vulnerables los sistemas informáticos, tanto a nivel personal como a nivel empresarial.

La mejor línea de defensa para individuos y para las organizaciones es capacitarse y conocer ¿cuáles son los motivos que impulsan a los delincuentes a robar información?, ¿posibles víctimas?, ¿vectores de ataques?, ¿técnicas de propagación?, ¿información buscada? Es importante determinar que los crímenes cibernéticos ocurren en el mundo del ciberespacio, pero sus víctimas y su impacto pertenecen mundo real.

2. Palabras claves: Ciberseguridad, integridad, disponibilidad, confidencialidad, riesgo de la información, explosión de datos.

3. Abstract

The abstract gives some insights about the cybersecurity and information security, a current and a relevant topic, since in Y2015, all reported cyber-attack were profitable than drug deal. Y2018 reported cyber-crimes profits represented $1.5 trillions. This abstract basis idea resides on training basics to people and enterprises, to protect own data, incidents and information theft are raising and impact to organizations escalated to critical, our information system's vulnerability is being exposed, personal or business levels.

The best defense line for individuals and organizations is to get trained to identify, identify the reasons why criminals steal information? possible victims? attack vectors? propagation techniques? Favorite information types? The article emphasizes on cyber-crimes happen within the cyber-space but victims and impact belong to our real world.

4. Keywords: Cybersecurity, integrity, availability, confidentiality, information risk, data explotion.

5. Introducción

El viejo paradigma de las empresas ensambladoras, donde en sus líneas de producción se generan grandes volúmenes de información y, al final del día, sus trabajadores se iban todos a dormir, sin ninguna preocupación hasta el otro día, se ha ido y nunca más volverá. En el escenario actual, el

mundo de los datos en línea está siempre encendido, grabando, monitoreando y trabajando, con el objetivo de proteger la información.

En las corporaciones y, a nivel personal, la divulgación de información confidencial, robo de secretos industriales (procesos internos, planes a futuro, futuros productos), hurto de información personal (PII) de los empleados (salarios, enfermedades, información financiera, etc.) representan preocupaciones válidas para los gerentes de Tecnologías de información (TI) y gerentes de Seguridad de Información (CISO).

Para mitigar posibles ataques, es necesario que las organizaciones inviertan en seguridad informática, de igual forma que lo hacen a nivel físico mediante perros guardianes, cercas y hasta personal de seguridad.

En el Reporte Global de Riesgos del año 2019 (World Economic Forum Global Risks Perception Survey 2018–2019, 2019), siendo parte del Foro Mundial Económico, se evalúan los riesgos económicos, ambientales, sociales y geopolíticos. Asimismo, existe una categoría para los riesgos de tipo tecnológico, la cual, se concentra exclusivamente en Ciberseguridad.

5. Desarrollo

5.1 La explosión de datos

La llegada de tecnologías disruptivas, como la Inteligencia artificial (IA), Blockchain, Internet de las cosas (IoT), Machine learning (ML) y la Transformación digital (PowerData, 2018) han posibilitado un enorme crecimiento y una estrategia diferente (computación en la nube y redes sociales) de lo que antes se conocía en la administración y almacenamiento de la información. La generación de información en línea y en todo momento, se relaciona con productos, tales como, los vehículos autónomos que, con la ayuda de sensores, se desplazan de acuerdo con las condiciones encontradas y toman decisiones usando la información que procesan. O bien, los conocidos wearables – un reloj, en este caso - que permite a un corredor, en tiempo real, tomar decisiones mientras se evalúan métricas de rendimiento (distancia, ritmo cardiaco, peso, velocidad, etc.) mediante un programa de entrenamiento a la medida almacenado en la nube.

Esta explosión de datos, estimada para el año 2025, se verá incrementada con la llegada de la red móvil de quinta generación (5G) _entendida como una nueva autopista de información_ así como, con otras tecnologías como la Nube, la velocidad de transmisión de los datos y la expansión de conocimiento, lo que potenciará un mayor uso de datos (ver figura 1).

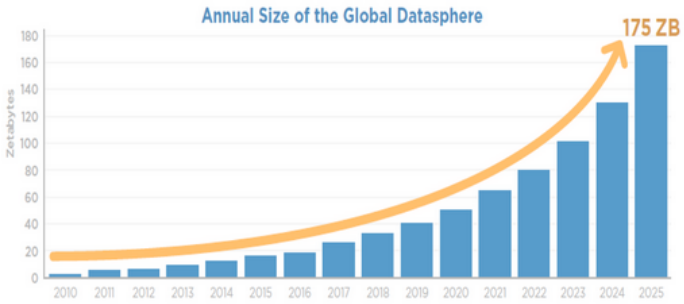

Figura 1. Crecimiento anual datos en la Nube. Fuente: Coughlin (2018).

Por encima de todas las tecnologías descritas, se encuentra la seguridad de la información, que consiste en asegurar y determinar los riesgos de la información en cualquiera de los estados, durante su ciclo de vida, a saber, ingreso, almacenamiento, transferencia, respaldo y borrado de la información.

5.2 Mundo Real vs. Mundo Cibernético: crímenes

Una de las mayores preocupaciones de los profesionales en seguridad de la información, es; ¿qué se puede hacer para mantener segura la información y los activos, de los engaños y ataques a las organizaciones y a las personas? Las estadísticas indican que, para el año 2018, los ciberataques más comúnmente usados y con una efectividad

del 78% fueron ransomware (secuestro de datos), la ingeniería social (social engineering) y la suplantación de identidad (phishing) (ver figura 2).

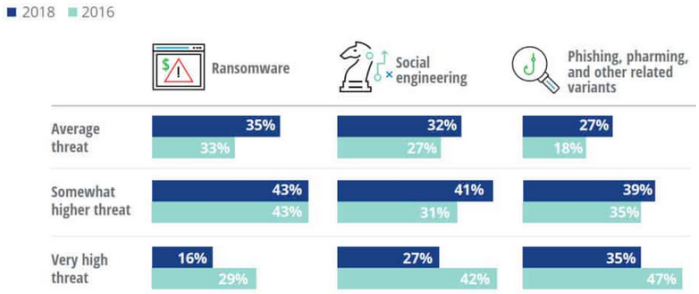

Figura 2. Comparativo años 2016 y 2018, tres primeros tipos de ciberataques. Fuente: Zaharia (2019).

Estos tres ciberataques tienen su contraparte criminal en el mundo real, como lo son la extorsión, el robo y el engaño, respectivamente.

Asimismo, el ransomware es un programa malicioso que, una vez instalado en un dispositivo (computadora, teléfono, servidor) encripta (PowerData, 2018), la información y pide a la víctima un depósito a cambio de volver a restablecerla. Una vez hecho el pago, se envía una llave para desencriptar la información. Como en la vida real, el pago no siempre garantiza la recuperación de la información (ver tabla 1).

Tabla 1

Resultados finales del pago del rescate

	2018	2019
Percentage of organizations victimized by ransomware	55.1%	56.1% ↑
Percentage of victimized organizations that paid ransom(s)	38.7%	45.0% ↑
Percentage of victimized organizations that refused ransom(s) and lost their data	13.1%	19.2% ↑
Percentage of victimized organizations that paid ransom(s) but lost their data	50.6%	38.8% ↓

Fuente: Imperva (2019).

Además, como vectores de infección, se tienen identificados los archivos de Microsoft (Excel, Word, Power Point) vía email, archivos comprimidos (.zip o .rar) y, en tercer lugar, archivos de Acrobat Reader (.pdf).

A su vez, la Ingeniería Social es un término general que se usa para engañar a través de actividades humanas. Usa la piscología humana para manipular al usuario, para que realice errores en seguridad o brinde información sensitiva. El perpetrador, primero investiga a su víctima: sus gustos, historia personal, carrera, amigos, entre otros aspectos. Con la confianza ganada, comienza a indagar sobre debilidades en sistemas de seguridad de la empresa, protocolos de seguridad, tipos de control, plataformas, aplicaciones, bases de datos, hasta llegar a darle información sensitiva, como nombres de colegas, jefes, roles y responsabilidades, contactos, proveedores, etc., con el fin de obtener o ir escalando en privilegios, para ganar acceso a recursos críticos en la organización.

De acuerdo con un estudio de Gallup (2018), que se concentró en 13 crímenes, desde robo en casa, asaltos bancarios, delitos sexuales, robo y asaltos en carro, terrorismo, entre otros, arrojó que un 71% de los norteamericanos participantes en el estudio, están preocupados por el hacking de sus cuentas bancarias o tarjetas de crédito. En un segundo lugar, un 67% expresa preocupación por el robo de identidad.

Asimismo, el phishing o suplantación de identidad, es el más conocido de los crímenes de ingeniería social. Un ejemplo de este es la suplantación de identidad, la cual puede darse a través de un correo electrónico con un link y un mensaje que indica que debe cambiar su contraseña. La víctima accede al sitio web solicitado, que luce idéntico a su contraparte original. Cuando le solicitan las credenciales, la víctima no sabe que está exponiéndose a una suplantación de su identidad y que sus datos pueden ser usadas en bancos, sitios de gobierno, redes sociales, etc.

Algunas estadísticas (Brenan, 2019) de este crimen en Norteamérica son las siguientes:

- Perpetradores enviaron 6,4 millones de correos falsos diariamente (EY – Encuesta Global de Seguridad de la Información 2018-2019).
- Casi el 87% de las firmas listadas en la revista Fortune 500 son vulnerables a phishing.

- Sólo el 5% de las compañías han implementado el uso de la cuarentena, para enviar los correos falsos al folder de correo no deseado (Spam).
- El 41% de las direcciones de los sitios web afectadas por el phishing se incluye un cambio de un sólo carácter, 32% tienen un carácter adicional y un 13% han añadido o borrado un carácter al principio o al final con el objetivo de confundir y engañar a las víctimas. Ejemplo: Dirección Correcta – https://www.google.com, dirección falsa - https://www.gogle.com (falta un carácter en el nombre de la dirección).
- El 30% de los sitios en la web usados para phishing sites usaron HTTPS en el 2017, comparado con 5% durante el 2016, un crecimiento que los expertos creen que va en aumento.

5.3 Costa Rica: escenario local

Existe un llamado con carácter de urgencia, a nivel nacional, en cuanto al papel que juegan las tecnologías en la agilización de trámites y transferencia de información ciudadana, a pesar del riesgo que esto implica. Sumado a ello, existe un rezago en tecnología estimado en 30 años en infraestructura tecnológica, hardware y software. Para analizar esta situación, se puede utilizar el siguiente ejemplo: el ingreso del cobro del impuesto de valor agregado (IVA). Es un proyecto que involucra a todos los costarricenses, con una dependencia tecnológica alta y, a nivel de seguridad de la información, es altamente crítico, ya que es información que debe ser clasificada como confidencial, debido a que es el pago de impuestos, muy asociados a los ingresos de las entidades físicas o jurídicas. Ante este panorama, el abordaje de esta necesidad debe planearse tomando en cuenta la seguridad de la información (confidencialidad, disponibilidad e integridad) desde un punto de vista individual – ciudadanos - como también de las organizaciones que van a captar y almacenar información pública.

En Costa Rica, en los últimos 2 años, se han reportado desfalcos de cuentas bancarias por medio de llamadas telefónicas. Es un ejemplo del uso de ingeniería social, donde el perpetrador se hace pasar como un funcionario de la institución (una suplantación de identidad), con el objetivo de asistir a la víctima en la implementación de la cuenta International Bank Account Number (IBAN) – para este caso, como un funcionario del Banco Central de Costa Rica (BCCR) - o bien, para colaborar en la actualización de datos personales bancarios, siendo el Banco Nacional (BNCR) y el Bac Credomatic (BAC) los casos más sonados. Más recientemente, debido a la aprobación del impuesto de valor agregado (IVA), dichos engaños se extienden hacia el Ministerio de Hacienda, buscando claves personales o la tarjeta inteligente virtual (TIV) de las víctimas.

Otro engaño común reportado y, con un impacto mayor, se encuentra en la venta de artículos desde sitios de ventas en línea, donde por medio de ingeniería social, el supuesto comprador, para realizar la transferencia de dinero - sin solicitar asistencia - se le obliga la supuesta intercesión de call-center bancario, para completar la transferencia.

5.4 Datos relevantes de los ataques

Existen algunos rasgos por destacar que son comunes en este tipo de ataques o crímenes:

- La llamada es iniciada por la entidad, en vez de ser generada por el cliente.
- Parte de un servicio bancario no solicitado por la víctima.
- Existe un carácter de urgencia y debe ser finalizado durante la misma llamada.
- Solicitud expresa del perpetrador a solicitar datos personales al cliente, datos como, el usuario de cuenta internet, la clave personal, los códigos de transferencia, etc.

- En algunas llamadas se ha reportado el uso de conferencia tripartita (tres personas durante la llamada telefónica).
- Palabras más frecuentemente usadas durante las llamadas: urgencia, respuesta inmediata, actualización inmediata, Call Center o centro de asistencia, acceso remoto a la computadora del cliente, asistencia, transferencia y número de cuenta.

Entidades mencionadas durante las llamadas:

- Banco Central de Costa Rica (BCCR).
- Banco Nacional de Costa Rica (BNCR).
- BAC San José.
- Ministerio de Hacienda.

Con la obtención de la información personal, el siguiente paso es el fraude o robo de fondos de las cuentas de banco, pero esta vez se hace una suplantación de identidad de la víctima. El valor de la información personal puede medirse, para estos casos, proporcionalmente al daño y los riesgos que puede causar.

6. Conclusiones

La transformación digital tiene su base en la información, su distribución y su uso eficiente, con el fin de mejorar procesos, generar valor a los clientes y usuarios finales. Está aquí y vino para quedarse. Por lo cual, es clave saber el valor de la información que se genera, como organización y como individuos.

Asimismo, la computación ubicua, mediante el uso de diferentes dispositivos, hace que se envíe y reciba información en todo momento y en cualquier lugar. Además, hay mayor cantidad de dispositivos, (IoT) y, en un futuro cercano, se incorporarán más, que necesitarán estar conectados intercambiando información para su correcto funcionamiento y funcionalidad esperada. Por ejemplo, datos de localización añadidos a las fotografías y su integración con las redes sociales, vislumbran un nuevo riesgo, ya que se revela la localización durante las vacaciones familiares.

Es necesaria la aplicación de buenas prácticas para la protección de la información personal, con el fin de minimizar el impacto y la ocurrencia de incidentes. A continuación, se ofrecen algunas recomendaciones:

- Denunciar los incidentes, por parte de las víctimas, es de suma importancia, debido a las lecciones que se pueden aprender de las experiencias, con ello, se evita la propagación.
- Educación básica en ciberseguridad, incluyendo la integridad, la confidencialidad y la disponibilidad de la información.
- Animar a las personas a discutir las quejas y dudas en el tema de seguridad de la información, con una autoridad en el tema.
- Definir las diferentes categorías o niveles de confidencialidad de la información.
- Determinar qué es contenido ilegal y definir listas de bloqueo.
- Educar a los usuarios en las consecuencias de visitar redes sociales y compartir información.

La seguridad de la información es vital y es el conector entre los mundos real y cibernético, ya que protege los intereses de personas y organizaciones en un mundo muy amplio y, que cada vez, somos – como sociedad – más dependientes a esta. Por lo tanto, debemos conocer las reglas del juego en materia de seguridad de información. Los alcances, roles y responsabilidades en ambos mundos, para evitar malas experiencias, que tienen su repercusión y penalización – muy duras por cierto -en el mundo real.

"Si usted conoce a su enemigo y se conoce a sí mismo, no tiene por qué temer el resultado de 100 batallas" (Sun Tzu, 2010).

7. Referencias

Coughlin, T. (Nov, 2018). 175 Zettabytes by 2025. Forbes [https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/#3ad581754597].

Imperva. (2019). Phishing Attacks. Imperva [https://www.imperva.com/learn/application-security/phishing-attack-scam/].

Brenan, M. (May, 2019). Cybercrimes Remain Most Worrisome to Americans. Gallup [https://news.gallup.com/poll/244676/cybercrimes-remain-worrisome-americans.aspx]

Power Data. (Julio 2019). Transformación digital. Qué es y su importancia y relación con los datos. Power Data [https://www.powerdata.es/transformacion-digital].

Sun Tzu. (2010). El arte de la guerra. China: EDAF.

World Economic Forum Global Risks Perception Survey 2018–2019. (2019). The Global Risks Report 2019. 14th Edition. [http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf]. Zurich, Ginebra.

Zaharia, A. (Mayo, 2019). Comparitec, 300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends. Comparitech [https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/ - Top_cybersecurity_threats_2019].

Figura 3. Imagen ilustrativa. Fuente: Pete Linforth en Pixabay en https://pixabay.com/es/illustrations/hacker-ciberdelincuencia-1952027/