***CIBERDELITOS –Estado de situación y tendencias***

Una estudiante de psicología española es obligada a transferir tres Bitcoins a un beneficiario en Polonia para evitar la divulgación de sus videos íntimos. A un diputado de Paysandú le vaciaron su MasterCard. La empresa más grande del mundo es multada a escala millonaria, luego de haber pagado cientos de miles de euros a una organización chechena para recuperar la base de datos de sus clientes y, por si fuera poco, su director debe comparecer ante las cámaras del mundo a soportar la humillación. En Lima, un renombrado jurista pierde la vida en circunstancias extrañas: su marcapasos dejó de funcionar. Hoy es 31 de julio de 2019 y esta caído el sistema. Los ciberdelitos son el *trending topic* criminal.

Aprovechando esta era de hiperconectividad, los tentáculos de la delincuencia se han extendido hasta los botones de nuestros dispositivos, desde donde amenazan incluso hasta la propia noción de intimidad. ¿Cuál es la solución? ¿En quién confiar? Como desde hace siglos, la industria del seguro debe reinventarse para seguir brindando soluciones a la sociedad y dar cobertura a los riesgos asociados con el avance de la tecnología.

Recientes estudios han revelado la enorme dificultad que padecen las organizaciones que registran incidentes de seguridad para llevar datos y estadísticas fiables sobre la cantidad de incidentes ocurridos y registros afectados. La falta de un criterio unificado y de un mecanismo de consolidación de la información, sumado a que únicamente contamos con la versión del damnificado y al hecho indudable de que gran parte de los incidentes aún no se reportan, dan como resultado un cóctel letal que conspira contra la fiabilidad de la información. Sin embargo, el Reporte Anual 2018 elaborado por Internet Society (ISOC – www.internetsociety.org) revela datos preocupantes que anuncian una tendencia creciente hacia nuevas modalidades delictivas, al tiempo que socavan peligrosamente la privacidad, seguridad e intimidad personal.

Se estima que durante el año 2018 se reportaron aproximadamente 6.500 incidentes de seguridad con acceso no autorizado a datos privados, que afectaron un total de 5.000 millones de registros en todo el mundo. Si bien estos indicadores han bajado ligeramente respecto de 2017, el surgimiento de nuevas e ingeniosas modalidades delictivas hacen encender las alarmas de toda la comunidad. Los invitamos a conocer un poco más profundamente de qué se trata esto.

**RANSOMWARE** – Es un término que surge de la abreviación de “*Ransom* (rescate) *software*” y, como su nombre lo indica, se trata de un programa que bloquea el acceso a la información o al sistema operativo infectado y luego “pide un rescate” al legítimo propietario para liberar esa restricción. Mediante esta modalidad, el delincuente (llamado *cracker* o *hacker*) extorsiona a una persona u organización exigiéndole el pago de una cantidad determinada de dinero –en general electrónico- a cambio de devolverle el acceso a su base de datos.

La organización *Cybersecurity Ventures* (www.cybersecurityventures.com) estima en 8.000 millones de dólares las pérdidas materiales a causa de este delito durante el año 2018 en todo el mundo. Solo en 2018 se denunciaron más de una docena de incidentes que superaban los 100 millones de registros afectados, cada una. El más grande de estos episodios involucró a la base de datos nacional de la agencia de identificación de la India (“Aadhaars”) en un incidente que afectó a más de 1.100 millones de registros públicos. Los incidentes de *Marriot/Starwood* (383 millones de registros), *UnderArmour* (150 millones de registros) y el sonado caso de *Facebook/Cambridge Analytica* (87 millones) sean tal vez los casos con mayor exposición pública que han tenido lugar durante 2018.

**DENIAL OF SERVICE** (DoS = denegación de servicio) – Mediante esta modalidad delictiva el atacante impide que los legítimos usuarios de una aplicación o servicio Web de una empresa puedan acceder a ella, generalmente a través de la saturación del ancho de banda del proveedor del sistema atacado, provocando pérdidas económicas en función del tiempo de inactividad de sus plataformas on-line. Hace 10 años, un tráfico de 10GB/seg ya era capaz de saturar cualquier servidor o red privada, mientras que en 2018 se llegó a medir la cifra récord de 1,7 TB/seg en solicitudes ficticias, un guarismo 170 veces mayor, lo que demuestra el crecimiento que año a año tiene el pico de ancho de banda (”*peak*”) utilizado en los ataques y la facilidad y rapidez con que se aumenta el alcance de los mismos.

*Kaspersky Labs* y *NetScout* han reportado aproximadamente 6 millones de intentos de ataques de denegación de servicio durante 2018, de los cuales se estima que resultaron exitosos unos 150.000. Estos ataques, si bien no implican el acceso a información confidencial o privada, afectan a empresas de todos los rubros en cifras millonarias. En 2018 se han destacado por su notoriedad los ataques a ABN AMRO Bank, Twitter, Amazon, Spotify, Netflix, GitHub y la versión digital de The New York Times. Sin perjuicio de las dificultades ya aludidas en cuanto a la fiabililidad de las estadísticas ya mencionadas, se calcula un costo promedio de US$ 220.000 por cada ataque en términos de pérdidas por tiempo de inactividad relacionado con la oferta de servicios en internet.

**PHISHING** (Suplantación de Identidad) – Como su nombre lo indica, mediante esta modalidad delictiva el atacante se hace pasar por alguien de confianza de la víctima (un familiar, un cliente, un amigo, un socio comercial, un empleado, un jefe) con el objetivo de acceder a su información confidencial, exigir el pago de dádivas, favores y regalos o realizar amenazas bajo la apariencia de una identidad falsa con el objetivo de extorsionar a sus víctimas. El arte del engaño, como sabemos, no es algo nuevo; lo novedoso son las vías –cada vez más variadas y populares- de canalización de estos engaños.

El Reporte Anual 2018 publicado por Internet Society destaca como tendencia novedosa la utilización de tres modalidades de ingreso indebido: 1) Ataques a la cadena de suministro de la víctima; 2) A través del proceso conocido como “*Credential stuffing*” (derrame de credenciales) y 3) Dispositivos IoT (*Internet of things*).

El primero de ellos consiste en el ingreso indebido al sistema de la “empresa objetivo” a través de empresas tercerizadas con menor grado de seguridad informática a quienes se les permite, por razones operativas, el acceso a los datos privados de los clientes. Dicho con otras palabras, se ataca el eslabón más débil de la cadena de suministro para afectar a un objetivo más robusto en materia de ciberseguridad. Esto, además, le permite al atacante afectar una gran cantidad de empresas simultáneamente sin necesidad de atacar directamente sus propios servidores o sistemas, sino logrando acceder a los datos de sus clientes mediante la violación de seguridad de un componente secundario que no pertenece a la empresa principal sino a una tercerizada, en general, de menor tamaño y capacidad (en general formularios de pago o de registro de datos falsos o infectados).

El llamado “derrame de credenciales” es simplemente la utilización de datos previamente obtenidos para replicarlos en múltiples plataformas y servicios on-line con el fin de acceder a una mayor cantidad de datos con las mismas credenciales ya obtenidas. Así, el *phisher* logra el acceso a varias funcionalidades on-line de una misma persona o empresa, utilizando el mismo nombre de usuario y contraseña ya obtenidos previamente. Esto es posible porque, según mediciones recientes (SecureAuth – Jul/2017) ***el 81% de las personas utilizan la misma contraseña en dos o más cuentas, mientras se estima que un 25% utiliza la misma contraseña para todas sus cuentas***.

En cuanto a IoT, no es ninguna novedad que la vida diaria depende cada vez más de la utilización de aparatos electrónicos conectados a internet. Ya no hablamos de ordenadores personales, televisores o teléfonos celulares. La domótica vino para quedarse y el grado de automatismo y conectividad alcanza prácticamente a todos los electrodomésticos del hogar. Del mismo modo, los sistemas de vigilancia, calefacción, ahorro energético y comunicación de un hogar están siendo controlados por dispositivos con acceso a Internet. Así, el universo de potenciales vías de ingreso a la privacidad personal se multiplica en igual relación. En un sonado caso ocurrido durante 2018 el FBI alertó a los usuarios de *routers* de la empresa “CISCO” que debían resetear o cambiar sus dispositivos ya que se había comprobado la infección con malware de más de medio millón de *routers.*

Como dijimos, la extorsión a personas físicas y empresas no es algo nuevo, lo novedoso son las impensables maniobras mediante las cuales los atacantes acceden a los datos. Luego, lo de siempre: extorsión en función de la cantidad y calidad de datos obtenidos; engaño para conseguir algún beneficio o pago indebido en función de la suplantación de identidad; amenazas en nombre de otra persona y directamente vaciamiento de cuentas o consumo de saldos de tarjetas de crédito. Tal vez el componente más novedoso en este sentido está dado por la propia legislación vigente, ya que prevé importantes multas a las empresas que reconozcan violaciones a sus sistemas de seguridad, lo que la convierte en un arma de doble filo: por un lado intenta obligar a las empresas a robustecer sus sistemas de seguridad por miedo a ser multados, pero por otro los incita a ocultar la ocurrencia de incidentes por miedo a las multas y a la pérdida reputacional, perjudicando así un mejor y más coordinado abordaje del incidente.

**CRIPTOJACKING** – Se denomina así al uso no autorizado, por parte del atacante, de los recursos informáticos de una persona para “minar” criptomonedas en su beneficio. Estamos seguramente frente al mayor desafío que existe actualmente en el ámbito de la ciberseguridad a nivel mundial y a un delito que, sin necesidad de vulnerar la privacidad de los datos, reporta enormes beneficios económicos al delincuente y, tal vez por ello, ha crecido en el entorno de un 80% respecto a la cantidad de ataques reportados en 2017. Pero…¿qué es y cómo funciona esto?

Como sabemos, las criptomonedas como medio de pago independiente están floreciendo a lo largo y ancho del mundo, basta con ver el alza en la cotización de las mismas desde su lanzamiento hasta hoy (valor Bitcoin actual aprox US$ 11.000). Ahora bien, uno puede comprarlas en el mercado o puede “fabricarlas”. O mejor dicho “minarlas”. Como si se tratara del mismísimo oro. Para entender cómo funciona es necesario conocer la tecnología detrás de los *Bitcoins*, los *Ethereum* o los *Litecoins*, para lo cual sería necesario otro artículo; pero, en síntesis, lo que da valor a las criptomonedas es la seguridad de que la transacción es real y que vincula a personas y servicios fiables y constatables. Para ello se basan en la tecnología “Blockchain”, que consiste en un sistema de autenticación de transacciones extremadamente complejo y seguro, basado en el registro temporal e invariable de una cadena de validaciones que aseguran la fiabilidad de las transacciones registradas, minimizando al máximo la posibilidad de fraude o violación del registro. Para ello, es necesaria la participación de muchas personas y/o recursos informáticos que resuelven problemas matemáticos sumamente complejos y que, una vez resueltos, se registran de forma tal que la solución quede enlazada con el registro inmediato anterior y con el siguiente, de manera que la existencia de ese nuevo eslabón valida la fiabilidad de toda la cadena de transacciones.

En este contexto, parece obvio que alguien tiene que hacer el engorroso trabajo de validar las transacciones de la Blockchain, lo cual, como dijimos, insume muchísimos recursos informáticos y, por ende, capacidad de procesamiento de los ordenadores y por ende también, una enorme cantidad de electricidad. Para compensar todo este esfuerzo es que se “premia” a los colaboradores de la red otorgándoles Bitcoins en forma de pago en relación a la cantidad de transacciones que logren validar. Aquí es donde se comienza a vislumbrar el lucrativo negocio de los delincuentes: roban los recursos eléctricos y de procesamiento de distintas personas y empresas para resolver más cantidad de transacciones, utilizando así recursos ajenos en beneficio propio. Como contrapartida, el afectado percibe lentitud en el funcionamiento de sus sistemas y un mayor gasto de energía eléctrica, sin entender a qué se debe. Paradójicamente, esto lleva muchas veces a aumentar la capacidad de procesamiento de los equipos infectados, aumentando así la capacidad de procesamiento del delincuente, convirtiendo a la víctima en un cómplice involuntario.

**CONCLUSIÓN**

Para que quede claro, ninguna persona u organización se encuentra libre de ser víctima de un ciberataque. Internet nos vuelve más vulnerables, nos vuelve más inseguros: internet nos hace iguales. Sin dudas, los seguros que actualmente cubren las eventuales pérdidas materiales del asegurado o su patrimonio frente a reclamos de terceros afectados o multas del regulador de turno, son instrumentos útiles. Pero no suficientes. Es necesario que haya una comprensión global del problema y educar en seguridad informática. Es necesario especializarnos en informática forense para una correcta comprensión del riesgo y una adecuada suscripción del mismo. Se estima que más de un 90% de los incidentes ocurridos en 2018 pudieron haberse evitado con controles rutinarios sencillos y una cultura de seguridad informática adecuada.

El control de empleados, socios comerciales y proveedores es esencial para reducir la creciente exposición asociada con el aumento de dispositivos y servicios on-line. Una lista de proveedores lo más acotada posible y controles periódicos sobre sus sistemas informáticos es el horizonte al que debemos apuntar. En EEUU se indemnizaron sólo en 2018 aproximadamente US$ 2.000 millones en siniestros de ciberseguridad, lo que significa una reducción del 37% respecto de 2017. Si bien esto es visto como una señal de maduración del sector, es necesario comprender hacia donde está yendo el mundo de los nuevos ciberdelitos y tratar de actuar en consecuencia. En próximas publicaciones podremos ahondar en las herramientas que ofrece el sector asegurador y analizar casos prácticos que servirán de base para generar conciencia colectiva sobre este tema. Ese es, sin dudas, el principal desafío.

**Dr. Rodrigo Penadés**

****

Fecha y lugar de nacimiento: 28/Jun/1986, Montevideo (Uruguay)

Doctor en Derecho y Ciencias Sociales - ***Universidad de la República***

Postgrado en Responsabilidad Civil Profundizada - ***Universidad Católica del Uruguay***

Docente de Marco Legal de la Actividad Aseguradora – ***Instituto BIOS Uruguay***

Especializado en responsabilidad civil contractual, extracontractual y derecho de daños.

Asesor corporativo en Compliance y Prevención de Lavado de Activos