Javier Puyol es el socio director de Puyol Abogados, una nueva boutique legal especializada en el mundo de las nuevas tecnologías y el cumplimiento normativo y las nuevas tecnologías. Confilegal.

Todos podemos ser objetivos de ciberataques: es la “democratización” del peligro.

Javier Puyol - 31 Agosto, 2017 https://confilegal.com/20170831-todos-podemos-objetivos-ciberataques-la-democratizacion-del-peligro/#_edn5

Entre el 12 y el 16 de mayo de 2017 tuvo lugar un ataque sin precedentes en el mundo: un ciberataque que afectó a más de 360.000 dispositivos electrónicos de más de 180 países, por medio del ramsonware WannaCry.

El **Centro Criptológico Nacional (CCN)**, adscrito al Centro Nacional de Inteligencia (CNI), ha explicado que se trata de **un ‘malware’, denominado WannaCry**, que ha afectado a sistemas Windows cifrando todos sus archivos y los de las unidades de red a

las que estén conectadas, e infectando al resto de sistemas Windows que haya en esa misma red.

Tal y como publica Reuters, WannaCry, el "ransomware" que ha atacado a compañías como Telefónica o Renault o al sistema de salud británico, ha logrado bloquear más de 200.000 ordenadores en más de 150 países, y no solo consiguió paralizar a miles de empresas en todo el mundo, sino que también demostró lo frágiles que podemos llegar a ser y constató un hecho: estamos inmersos en una época en que las mayores guerras se libran tras la pantalla de un ordenador.

Aunque su actividad se ha ralentizado, se espera que en cualquier momento se puedan reproducir dichos ataques, incluso con la misma o mayor virulencia, siendo potenciales víctimas de ello, no solo las Administradores Públicas, o las grandes corporaciones económicas o financieras, sino que el efectos de estos ciber ataques tienen la virtualidad, por primera vez, de su democratización, en el sentido de que cualquier persona puede verse afectado, siendo, evidentemente dicha repercusión cuantitativamente mayor en las Pymes y en los consumidores, por la falta de información, pero sobre todo por la carencia de medios que estos tienen frente a las Administraciones Públicas o las grandes Corporaciones o Multinacionales.

La democratización de la ciberdelincuencia, consecuentemente con ello, implica su generalización, y la no exclusión de potenciales víctimas, con independencia de su importancia, volumen económico o la capacidad de su gestión.

En este sentido, debe tenerse presente que un ataque como estos paraliza la normal actividad de cualquier empresa, y en muchas ocasiones, el bloqueo de los ficheros, o la encriptación forzada de los datos y la información en ella contenidos, determina que se pierdan años completos de trabajo, y que afecte a todos los ámbitos y sectores de la empresa, tales como las ventas, la producción, la contabilidad y cualesquiera otros de dicho ámbito empresarial ciber atacado.

La consecuencia de todo ello, es que además de los perjuicios ocasionados, el paso siguiente consiste en contratar los correspondientes servicios externos para poder recuperar en la medida en que ello sea posible la información y recuperar tiempo perdido.

Así, c*ualquier información de valor que guardemos en nuestros ordenadores, en la nube o en nuestros móviles, ya sea personal o para una compañía, puede resultar interesante para los cibercriminales. Por ello, hay que extremar todas las medidas de seguridad. Ello afecta no sólo los datos de nuestras cuentas en el banco, también todo aquello que alguien podría robarnos y pedir un rescate a cambio.*

*Del mismo modo, c*ada persona cuenta con más dispositivos conectados a la red con los que manejar objetos cotidianos de nuestras vidas, (smartphones, tablets, ordenadores personales y demás dispositivos móviles, dentro de una variedad enorme de los mismos).

Además, debe tenerse en cuenta que, por ejemplo, que en nuestras casas, contamos con nuevos dispositivos conectados a la red, y que también pueden ser víctimas potenciales de los ciber delincuentes, como las persianas, la calefacción o la iluminación. Toda esta amalgama de mini-ordenadores conectados, conocida como el Internet de las Cosas (por sus siglas en inglés IoT), es como una puerta abierta de par en par en casa para los hackers o los cibercriminales, lo que aumenta las posibilidades colectivas e individuales de ser víctimas de esta nueva forma de delincuencia

Un factor que sin duda está colaborando poderosamente para la expansión de este tipo de ciber delincuencia, esto se debe a que la mayoría de estos dispositivos se han diseñado sin tener en cuenta los factores de ciberseguridad para ahorrar costes de producción y costes de mantenimiento. Los hackers saben bien, que con un pequeño esfuerzo pueden controlar casi cualquier dispositivo electrónico que haya en cada casa, en la empresa, o incluso en las Administraciones Públicas.

En cualquier caso, ¿cómo se llega a los cálculos totales?

Para El Confidencial, esta cuestión depende fundamentalmente de tres factores bien diferenciados, que son los siguientes:

1) Impacto directo

Por los costes atribuibles de modo inmediato y fácil: la pérdida del propio dispositivo afectado, los costes de remediación y recuperación de equipos de las empresas afectadas, la pérdida de las horas de trabajo asociadas a dichos dispositivos, etc.

2) Impacto indirecto

Que viene dado tanto por el sobreesfuerzo y horas extra derivados de la revisión y chequeos de seguridad y la inversión en la implantación de medidas adicionales de seguridad, así como por los costes reputacionales, legales y financieros derivados de haber sido víctima de este ataque.

3) Impacto diferido

Quizás el menos evidente, pero probablemente el más relevante a medio plazo. Incluiría los costes generados por la alteración del comportamiento del consumidor, de la inversión y de la productividad generada por la inactividad de los negocios

Según un Informe de la Consultora Deloitte[iii] los costes directos generados por dicho Ramsonware han sido muy cuantiosos, y se puede establecer las siguientes pautas para proceder a su evaluación, aunque probablemente, por diferentes razones, entre ellas las de naturaleza reputacional, nunca se conocerá a ciencia cierta, los daños producidos, o las cantidades percibidas por los ciber delincuentes, a consecuencia de la ejecución de dicho malware. En dicho Informe, se establecen las siguientes pautas para su cuantificación, que son las que se indican a continuación:

a). Impacto generado por el rescate

Solo entre un 5 y un 10% de los afectados están dispuestos a pagar por el rescate. En este caso en concreto los ciber delincuentes además solicitaban el pago en bitcoins. Según la empresa Elliptic, especializada en actividades de forensics realizadas sobre operaciones en bitcoins, se identificaron 3 direcciones diferentes asociadas a WannaCry a las que hicieron seguimiento, comprobando los pagos que se iban realizando a las mismas e identificando más de 300 transacciones y más de 100.000 dólares acumulados en total.

b). Impacto como consecuencia de la recuperación

Otro coste importante es recuperar la operatividad de los ordenadores afectados. En general, se estima que el coste de recuperación de los dispositivos afectados por un ransomware puede situarse entre los 300 y 500 euros.

Suponiendo una estimación conservadora de 300 euros por dispositivo afectado, estaríamos hablando de más de 100 millones de euros de pérdida global por el ataque del 12 de mayo.

Relacionado con este coste en necesario recalcar la necesidad de disponer de una cultura, hábito y medios para realizar copias de seguridad periódicas de la información mantenida en los ordenadores.

c). Impacto por la inactividad del personal y del propio negocio

Se trata de un coste más relevante que los anteriores y probablemente uno de los más complicados de estimar. Es el coste que supone para una empresa la imposibilidad por parte de su personal para realizar sus tareas asignadas, debido al bloqueo de su ordenador como herramienta de trabajo y/o de la información mantenida en el mismo, o de la caída en los sistemas.

Más aún, incluso sin estar afectados, el ataque global vivido el día 12 de mayo motivó que varias empresas solicitasen a sus empleados apagar sus dispositivos y abandonar sus puestos de trabajo como medida de contención contra el malware, ya que tiene la capacidad de infectar, a partir de un ordenador, a otros conectados a la misma red.

A partir de una estimación del salario de un empleado medio y de al menos 2 días de inoperatividad podríamos cifrar el coste por inactividad a nivel mundial por encima de los 100 millones de dólares.

El efecto negativo del ciberataque puede ir más allá del meramente funcional, generando pérdidas económicas relacionadas con aspectos financieros, legales, contractuales y reputacionales.

Por ello, la Consultora Deloitte, considerando los diferentes aspectos mencionados, estima que el impacto económico podría superar los 200 millones de dólares, incluso con el matiz de que tanto el efecto del viernes como la propia naturaleza del malware utilizado han suavizado el impacto sobre particulares y empresas. No obstante, ello, por ejemplo, en una primera estimación, West Coast cree que el coste de este ciberataque podría alcanzar los 4.000 millones de dólares a nivel global.

Por su parte, la Unidad de Consecuencias Cibernéticas de Estados Unidos (un instituto sin ánimo de lucro que avisa a gobiernos y negocios sobre los costes de los ciberataques) ha hecho una previsión más modesta al cifrar, el coste del ciberataque, en unos 1.000 millones de dólares.

Todo ello, no hace sino evidenciar el desconocimiento existente sobre el alcance real del impacto y los daños producidos que dicho ramsonware ha tenido sobre los sistemas de las diversas Administraciones, de las empresas, y de los particulares.

Desde la perspectiva de España, ISMS Forum calcula que en nuestro país ha habido entre 5.000 y 10.000 dispositivos afectados, muchos más que los 1.200 confirmados por Incibe, y con unas pérdidas aproximadamente de 5 millones de euros.

El coste por equipo afectado, según esta asociación, ascendería a 500 euros (una infección habitual ronda los 200 por equipo).

Tal como se puso anteriormente de manifiesto, a estas cifras habría que sumar los costes indirectos (tiempos de inactividad, revisión de equipos, reputación, etcétera).

Las 4 consecuencias de un ciberataque

Las consecuencias de un ciberataque para una empresa se distribuyen, en términos de coste, en cuatro aspectos principales:

a). La pérdida de información (39%);

b). La interrupción de actividades (36%);

c). La pérdida de ingresos (20%); y,

d). El daño a los equipos (4%).

Estas y otras consideraciones son las que nos deben llevar a la convicción de que la ciberdelincuencia ha llegado para quedarse, y que constituye un nuevo problema colectivo que necesariamente ha de ser afrontado por todos, pues el precio de vivir cada día más en el uso de las tecnologías basadas en la informática y en internet nos van a obligar a pagar el precio de liberarnos de esta nueva lacra social.