Debates en directorTIC

Información de valor para la toma de decisiones

Ransomware: el terror de las empresas

Aunque el *ransomware* lleva presente en nuestras vidas desde el año 1989, muchas empresas no han sido muy conscientes de su existencia hasta que el mismo no ha dado un salto a los medios de comunicación. En 2016 se dio un repunte importante y los pronósticos ya alertaban que este iba a ser una de las tendencias en el mundo tecnológico en 2017. Pronósticos certeros, que vieron su punto álgido, al menos mediáticamente, con la aparición de WannaCry, uno de los "ataques de moda" que, si bien ha tenido una gran repercusión, no ha sido el que más daño ha causado, según los expertos.

Check Point SOFTWARE TECHNOLOGIES LTD | KASPERSKY lab | panda | S21SEC | SOPHOS

¿Cuál es la lección que se puede extraer? La necesidad de parchear las aplicaciones, "algo que hasta ahora las compañías no se tomaban muy en serio, a lo que hay que unir que no eran lo suficientemente ágiles a la hora de llevarlo a cabo. No hay que olvidar que algunas no tenían parches disponibles en el momento en el que se produjo el ataque", recuerdan los representantes de Sophos, Check Point, Panda Security, S21sec y Kaspersky Lab, que acudieron al debate que Director TIC realizó en torno al mismo y las consecuencias que ha ocasionado al mundo empresarial español.

Otro de los aprendizajes gira en torno a que cualquier empresa, independientemente de su tamaño, puede ser atacada ya que, si antes el objetivo eran las pequeñas y medianas, los ciberdelincuentes han evolucionado y han puesto sus miras también en las grandes, dejando en evidencia la vulnerabilidad de sus sistemas de protección.

> "Muchas compañías no se atreven a decir que han sido asaltadas, por lo que esto implica"

Evolución

Los atacantes no son como hace años, recuerdan los asistentes al debate. Ya no son recién licenciados que buscan notoriedad. Ahora estamos ante auténticas corporaciones delictivas que se organizan, con el fin de ser lo más competitivas posible. En su opinión, van a estar en constante evolución, con el fin de alcanzar el máximo rendimiento.

De momento es importante el salto cualitativo que han dado, apuntan, atacando una vulnerabilidad del sistema operativo, lo que ha provocado que se expanda de una manera mucho más rápida, causando un mayor daño del que estábamos acostumbrados.

Aunque las cifras proporcionadas por el Centro Criptológico Nacional, indican que en España fueron 239 las direcciones IP afectadas y 1.200 máquinas, lo cierto es que los expertos creen que el número de afectados ha sido mucho mayor. Es más, apuntan a que, como la unidad monetaria que mueve el mundo es el dato, el elemento que nos hace ser competitivos frente a otras empresas, muchas compañías no se atreven a decir que han sido "asaltadas", por lo que esto implica. Por ello, consideran que posiblemente hay un gran número de damnificados anónimos, desde el usuario final hasta pequeñas empresas.

De todas maneras, resaltan que cada día hay ataques de *ransomware* que no son mediáticos, que afectan a cientos de empresas que se ven obligadas a pagar un rescate para recuperar sus datos.

Si no hay pago, no hay *ransomware*

Los fabricantes de seguridad recomiendan a los afectados que no abonen el importe exigido porque el *modus operandi* ha cambiado. Ya no podemos fiarnos de que el ciberdelincuente vaya a devolvernos nuestra información, afirman. "Se ha perdido la lealtad del atacante. El modelo está cambiando y, a pesar del pago, los datos seguirán codificados". Y todo ello sin olvidar que el pago fomenta la existencia del *ransomware* y de su crecimiento, advierten.

Bitcoin

¿Si no existiera el *bitcoin* no existiría el *ransomware*? No tiene por qué responden, porque esta no es la única manera de rescate solicitada. En algunos casos demandan una transferencia en una cuenta que no se puede localizar y, si no, inventarían otra cosa, aseguran. Es más, creen que en este momento habrá otras monedas que estarán luchando por ganar terreno al *bitcoin*, porque esto no puede ser un monopolio.

Perfiles de los ciberdelincuentes

Los perfiles de los maleantes son varios. Por un lado, están los ciberterroristas, con motivaciones terroristas y políticas. Motivaciones que, si bien han existido desde siempre, la tecnología ha servido para cambiar la política o la guerra sucia entre estados.

Por otro lado, debemos tener en cuenta el cibernegocio como servicio: el *malware as a service*, el *ransomware as a service*… Una industria muy potente, muy competitiva, que está generando decenas de miles de millones de dólares, con clientes a los que les exigen dinero por utilizar esas herramientas, y pagan por su utilización. Un negocio muy lucrativo y difícil de parar, amparado en el anonimato. Su funcionamiento es sencillo, incluso para aquellos que no tienen ni idea de seguridad. "Cualquiera puede meterse en un navegador, comprar un *rasom*, alquilar una plataforma de *ransom as a service*, y lanzar su campaña. Es como un supermercado de servicios en el que solo hay que coger las herramientas que han desarrollado otros, juntarlas y lanzarlas. Dinero rápido, fácil, indetectable, de efecto inmediato…". Algo muy alejado del estricto mercado al que tienen que someterse los fabricantes de seguridad, repleto de normas y leyes.

Y es precisamente esa facilidad a la hora de "hacer dinero" la que ha marcado el crecimiento de este negocio ilícito.

El camino a seguir por los fabricantes de seguridad

El mecanismo del ciberterrorismo lleva a los fabricantes de seguridad a replantearse, una vez más, cómo hacer frente a la lucha continua que tienen que llevar a cabo frente a los generadores de *malware* en una carrera "que nunca van a dejar de correr y en la que van a ir apareciendo amenazas nuevas". Algo que les hace plantearse dónde tienen que poner sus esfuerzos a la hora de cubrir las necesidades de sus clientes.

> "La tecnología ha servido para cambiar la política o la guerra sucia entre estados"

En su opinión, "cuentan con la capacidad de protegerse, aunque no saben exactamente a qué se enfrentan", por lo que manifiestan que "hay que poner el foco en el impacto que WannaCry ha podido tener en las empresas, sobre todo focalizando en la criticidad de los servicios o en la capacidad de que estos grupos delictivos puedan paralizar una compañía, teniendo que cortar todos los sistemas y enviando a los empleados a casa". Y con los ojos puestos en los dispositivos móviles, uno de los grandes retos a cubrir, porque ya está empezando a haber secuestros de móviles, algo que va a ir evolucionando.

Recomendaciones

Una política de *backup* es importante para poder recuperar una información, pero no es suficiente porque este puede fallar. Podemos pensar que solo pueden cifrarnos la información y pedir un rescate, pero ¿y si estos atacantes han dejado algo dentro y están robándonos información? ¿Para qué sirve un *backup* si nos siguen robando? Esto es lo que va a venir. Los expertos consideran que esto sí que es grave. Y, advierten, las tecnologías tradicionales no pueden detectarlo, por lo que hay que ir hacia herramientas de nueva generación que nos den una visión proactiva y preventiva. Hay que invertir en las mismas y verlo como un valor y no como un coste, porque lo importante es que las empresas tengan su información controlada y vigilada.

> "Sobre el CIO recae la responsabilidad de implantar las tecnologías que den respuesta a esos planes de seguridad"

Se necesita anticiparse al ataque: extraer los códigos maliciosos antes de que entren y formación sobre la manera de trabajar a la hora de utilizar la información de la compañía. Incluso no estaría de más realizar un *disaster recovery* correcto o una replicación de datos. En este sentido, recomiendan llevar a cabo un *backup online* y lanzar esa replicación fuera de la oficina. Todo ello junto a la concienciación. "Las empresas tienen que concienciarse de que los fabricantes de seguridad cuentan con herramientas que les permiten no tener que recuperar los datos del *backup* ya que disponen de muros que van a impedir que la amenaza siga expandiéndose y de herramientas que previenen de ese ataque", dicen.

La importancia del GDPR

El nuevo reglamento europeo también es importante a la hora de implantar medidas apropiadas de seguridad, con la consiguiente protección de la información. En este sentido, la nueva regulación obliga a las empresas a informar cuando hay datos se ha producido una sustracción de datos. Algo fundamental si tenemos en cuenta que, aproximadamente el 60 % de las brechas de seguridad, a nivel mundial, es consecuencia de un *malware* que extrae información crítica de las empresas.

El papel del CIO

Y, aunque normalmente el CISO lleva el papel de la planificación, definición de los planes de seguridad, tomar las medidas preventivas correctivas… sobre el CIO recae la responsabilidad de implantar las tecnologías que den respuesta a esos planes de seguridad, por lo que tienen que estar plenamente sincronizados y trabajar en perfecta armonía, aconsejan los fabricantes de seguridad. Y más teniendo en cuenta que ahora se les une la figura del *data protection officer* como consecuencia de la nueva regulación. Consideran que hay que "hacer un barrido" y seguir bajando en el organigrama empresarial, porque es un tema de concienciación de toda la organización, sobre todo pensando en que hay empresas que no cuentan con ninguna de estas figuras directivas. En este sentido comentan la necesidad de contar en el sector con profesionales que tengan conocimientos de seguridad, algo que escasea.

Objetivo: competitividad

Sin embargo, quieren lanzar un mensaje positivo porque, a pesar de que las amenazas existen, el negocio del cibercrimen está en expansión y va a seguir y si se toman las medidas adecuadas, el impacto se minimizará en gran medida. Las empresa tienen una gran oportunidad, dicen, "si lo ven como parte del *core* de su negocio y cumplen las medidas de seguridad, van a ser mucho más competitivas".

Cómo combatir el *ransomware* minuto a minuto

Desde nuestra redacción queremos ayudarle y para ello hemos desglosado el debate en varios apartados, con el fin de que elija el que más le interese, haciendo clic para dirigirle al contenido relacionado, aunque puede ver el vídeo completo e ir avanzando o retrocediendo gracias a la barra de tiempo situada en la parte inferior.

0 m 59 seg ¿Qué ha representado WannaCry para el mundo empresarial?

12 m 23 seg ¿Cómo ha afectado a España?

16 m 33 seg Más allá del *backup*. Medidas a tomar.

22 m 16 seg ¿Están las herramientas informáticas preparadas para conocer si más allá del ataque nos siguen extrayendo información?

35 m 02 seg Perfiles de los ciberdelincuentes.

42 m 28 seg Razones del crecimiento del *ransomware*.

46 m 06 seg La importancia del *bitcoin*.

46 m 50 seg La responsabilidad del CIO.

52 m 33 seg ¿Motivos para el optimismo o para el pesimismo?

57 m 18 seg Herramientas disponibles para luchar contra el *ransomware*.

1 h 07 m 28 seg Protección de los sistemas de la industria.

Recomendaciones de Check Point para luchar con el *ransomware*

El *ransomware* ha venido para quedarse, mutará y seguirá afectando a nuestros sistemas. Así lo afirma Antonio Abellán, director comercial de Check Point España, quien nos da, en este vídeo, una serie de recomendaciones para combatirlo. Pero más allá de estos consejos también se necesitan soluciones que se anticipen a los posibles ataques o que anulen los que ya se han instalado en los equipos.

VER VÍDEO

Antonio Abellán,
director comercial de Check Point España

Check Point®
SOFTWARE TECHNOLOGIES LTD

Kaspersky Lab: Ciberjuegos para concienciar

Una de las lecciones que deberíamos haber aprendido de WannaCry es que hay que proteger el entorno operativo y las aplicaciones instaladas. Diego Quintana, *head of technical support* de Kaspersky Lab Iberia, explica la importancia de ello, así como de la concienciación. En este sentido, Kaspersky Lab cuenta con una serie de ciberjuegos que permiten concienciar a diferentes capas de la empresa, junto a herramientas para detectar y acabar con el *ransomware*.

VER VÍDEO

Diego Quintana,
***head of technical support* de Kaspersky Lab Iberia**

Panda Security: Fortificando el puesto de trabajo

En su compromiso por hacer más fácil la vida a sus clientes en el ámbito de la seguridad, Panda Security cuenta con herramientas como Adaptive Defense, un arma muy eficiente contra peligros como WannaCry, admite Rosa Díaz, directora general de la compañía en España. Aunque sus soluciones también son capaces de conocer por dónde puede entrar el virus, estableciendo medidas de remediación que fortifiquen el puesto de trabajo.

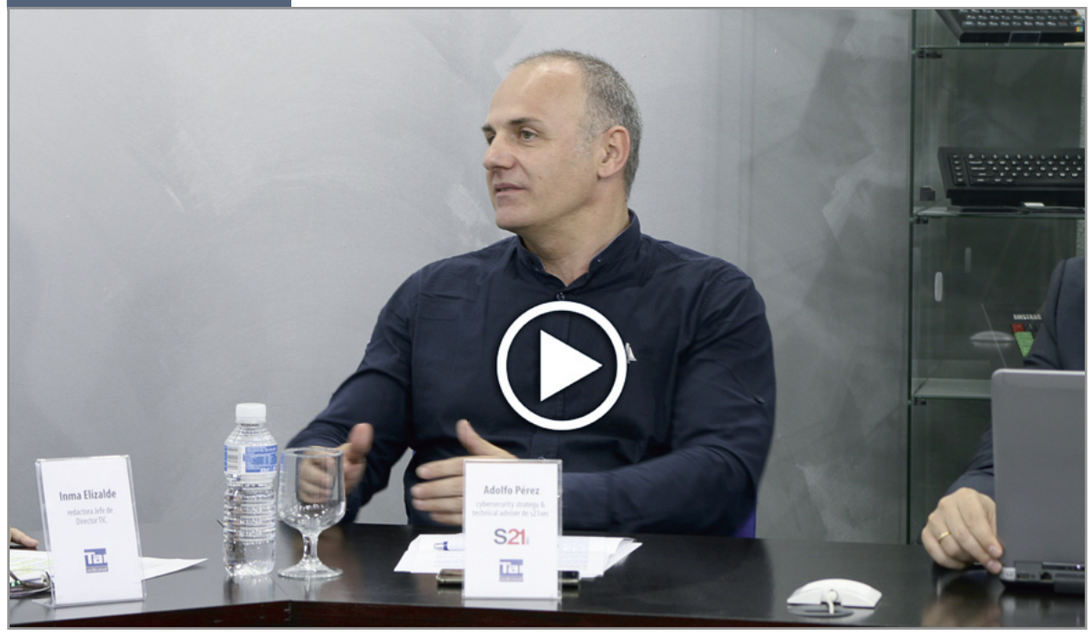
VER VÍDEO

Rosa Díaz,
directora general de Panda Security en España

S21sec: investigando las infraestructuras criminales

Contar con un valor diferencial es fundamental en el mercado y si es en el de la seguridad, más. Por ello desde S21sec, Adolfo Pérez, *cybersecurity strategy & technical adviser* de la compañía, asegura que esta diferencia, en su caso, estriba en ir más allá, contando con equipos de investigación que analizan e investigan las infraestructuras criminales. No en vano colaboran con las fuerzas de seguridad del Estado.

VER VÍDEO



Adolfo Pérez,
***cybersecurity strategy & technical adviser* de S21sec**

Sophos: la seguridad como un todo

Desde Sophos entienden la seguridad como un todo con Sophos Central, una única consola con la que pueden realizar una seguridad gestionada, incluso por capas o máxima protección para las empresas, detectando posibles amenazas o paralizando las que ya existen con herramientas como Sophos Intercept X, enfocada a la extinción del *ransomware*, por poner algunos ejemplos. Ricardo Maté, director general de Sophos Iberia, lo explica en este vídeo.

VER VÍDEO

**Ricardo Maté,
director general de Sophos Iberia**

SOPHOS