Encuentro Redes&Telecom

Foro Ransomware

Hay que integrar la seguridad en nuestro modo de vivir y de operar

Foro 'Ransomware: Alerta Máxima'

Redacción Computing y Redes&Telecom

Si 2016 ya fue señalado como 'el año del ransomware', ha sido en mayo de este año cuando esta modalidad del cibercrimen ha saltado a los medios generales con WannaCry como gran protagonista. Este malware, que por suerte no resultó tan dañino pese a su resonancia mundial, ha servido al menos para que muchas empresas se conciencien y que instituciones como Incibe, Guardia Civil y el CCN extremen sus campañas informativas y formativas para ayudar a prevenir un tipo de ataque que secuestra la información corporativa y exige dinero virtual a cambio, sin ningún tipo de garantías para la víctima que lo sufre. El 'Foro Ransomware: Alerta Máxima' organizado por Computing y Redes&Telecom ha querido poner de relieve todos los aspectos que rodean al mundo de la ciberseguridad contando con la participación de expertos institucionales y CISO de grandes compañías (Vodafone, Mediaset, RSI e Iberdrola), y de proveedores del ecosistema como Check Point, Commvault, GMV, Sophos, Informática El Corte Inglés y OVH.

"Welcome to the Digital Jungle"

Las ciberamenazas persisten y son cada vez más sofisticadas y numerosas, y las empresas –y usuarios– deben estar prevenidos. Gianluca D'Antonio, Master en Cibersecurity del IE y CIO de FCC, dio inicio al Foro Ransomware refiriéndose a la "necesidad de aprender a vivir en la jungla digital que nosotros mismos hemos creado", y para ello debemos tomarnos "muy en serio la seguridad" porque "es un negocio que mueve cantidades ingentes de dinero en todo el mundo". La mejor prueba de ello es que "la cotización de los bitcoins subió 600 dólares tan solo una semana después del ataque de WannaCry". También hizo hincapié en el imperativo de hacer de la ciberseguridad un terreno atractivo para los jóvenes. No es suficiente con tener conocimientos y experiencia, hay que fomentar aptitudes. Pero esta falta de formación afecta a los directivos de las empresas. Por un lado se van anunciando nuevas alertas y por otro existe una inercia en el

mundo empresarial hacia la desidia. "Menos de 200 empresas en España tienen un responsable de seguridad", argumentó. Estamos viviendo en la jungla digital, un entorno en el que existe muy poca legislación pero en el que tenemos una dependencia creciente de los entornos TI y en el que vivimos una inmadurez en ciberseguridad y privacidad. Gianluca D'Antonio menciona buenas prácticas para sobrevivir en esta selva, todo ello siendo conscientes de que nuevas variantes de ransomware aparecerán con regularidad. En definitiva, la seguridad ha de tenerse en cuenta, hemos de acostumbrarnos a que somos vulnerables a un ataque y afrontarlos de otra manera, al igual que cuando cruzamos una calle y miramos hacia los lados.

El cibercrimen, un negocio en auge

La Administración juega un papel decisivo en la lucha contra el cibercrimen, no en vano, son muchas las voces que se alzan señalando a algunos gobiernos como la mano negra que está detrás de la creación de estos softwares maliciosos. La ciberguerra es una realidad, "solo en 2016 aparecieron 200 nuevas familias de malware relacionado con el ransomware, el tipo de cibercrimen con mayor auge", señaló en el Foro Alejandro López Parra, responsable de los Servicios Avanzados en el CERT del Instituto Nacional de Ciberseguridad de España (Incibe).

Mucho se ha hablado de WannaCry y Petya, sin embargo, estos virus no son, "ni de lejos", los más dañinos ni los más sofisticados; pero sí son los que han tenido más eco en los medios por los actores a los que ha afectado a nivel global. No obstante, Parra celebró la existencia de ambos por servir para concienciar a la sociedad.

En 2016, Incibe gestionó 115.257 incidencias, de las que casi el 70% fueron malware, y se prevé que este año la cifra aumente un 25%. Bajar la guardia se convierte en la peor de las opciones. Las entidades de ciberseguridad ya tienen puestos los ojos en la última vulnerabilidad detectada, BlueBorne, que accede a los datos de los usuarios a través de bluetooth.

Desde Incibe animaron a las empresas a perder el miedo a reportar los ciberataques porque ninguna compañía está exenta de padecerlos, de hecho, "su grado de preparación no se mide por si sufre o no ataques, sino por cómo reaccionan cuando los sufren", aclaró. Potenciar la colaboración público-privada, tener una institución que filtre la cantidad de información que se genera cuando se produce un ciberataque, y la monitorización y concienciación de la plantilla, son los frenos más importantes; "el eslabón más débil de la cadena es el usuario, al que hay que dotar de formación y herramientas".

"Todas las empresas sufren ciberataques, se sabe si están preparadas por cómo reaccionan al sufrirlo"

NoMoreCry

WannaCry, el software malicioso de tipo ransomware que salió a la luz el pasado 12 de mayo, "podía haber sido diseñado por un estudiante de primero de Informática", confesó Luis Jiménez Muñoz, subdirector del Centro Criptológico Nacional (CCN). Sin embargo, él solo bastó para poner en jaque a empresas e instituciones de todo el mundo. El repunte de los ataques de malware que vivimos desde 2016 se debe a un cambio en la forma de negocio de los ciberdelincuentes, como los ya célebres Shadow Brokers.

Hacen falta cuatro ingredientes para cocinar un ciberataque efectivo: una vulnerabilidad en el sistema, un programa que explote esa vulnerabilidad (exploit), un vector de infección por el que introducir el exploit en un equipo ajeno (mail, bluetooth, o el protocolo SMB de Windows, entre otros); y una infraestructura que permita pagar el dinero a los ciberdelincuentes a cambio de recuperar la información robada.

La implicación de la alta dirección en la seguridad de la empresa evita que se creen situaciones de pánico en caso de ser víctima de malware. Asimismo, Muñoz se sumó a la petición de mejorar los canales de comunicación público-privada para contar con datos exactos: "se desconoce el impacto real que tuvo WannaCry en el sector privado, solo sabemos que la vacuna contra el ransomware que desarrollamos, NoMoreCry, tuvo una descarga masiva por parte de este sector, cosa que no ocurrió con la Administración".

"Hay un problema de talento"

Vivimos en un mundo híper complejo que nosotros mismos hemos creado. Un mundo en el que la tecnología forma parte de nuestras vidas y los procesos se automatizan. Un mundo cíber con nuevas coordenadas al que nos tenemos que adaptar. Para afrontar esa complejidad es necesario talento, un talento que debemos buscar. "Y no hablo de ingenieros de telecomunicaciones o informáticos, hablo de juristas, de científicos de datos, de psicólogos…", indicó Enrique Ávila Gómez, jefe del área de Seguridad de la Información, Servicio de Innovación Tecnológica y Seguridad de la Información de la Dirección General de la Guardia Civil. El reclutamiento de este talento es el principal problema al que nos enfrentamos hoy ya que lo necesitamos para combatir la ciberguerra. A tal fin es imprescindible "la generación de inteligencia colectiva, pues las capacidades individuales no sirven para nada en la ciberguerra. Esta se combate con talento físico, personal y automatizado. Hay que eliminar esas dependencias individuales si son incapaces de generar sinergias y buscar equipos pluridisciplinares y con pensamientos laterales".

La voz del CISO se alza frente al malware

La experiencia del CISO fue narrada por los responsables de Seguridad de Mediaset, Vodafone, Iberdrola y Rural Servicios Informáticos. Los participantes advirtieron que un ciberataque ya "no sólo afecta a un cliente en particular, sino a la reputación de la compañía", aún así, resaltaron la importancia de informar de las infecciones nada más ser conscientes de ellas como "la única manera de combatir el cibercrimen eficientemente". Lo preparada que está una organización no se mide por "si sufre ciberataques o no, sino por cómo reacciona ante estos ataques".

La idea de que la responsabilidad única de la seguridad de una empresa recae sobre el CISO es una creencia aún arraigada en muchas compañías, y que los mismos CISO llevan tiempo tratando de erradicar, porque "luchar contra las ciberamenazas sin la colaboración activa de todos los empleados es nadar contracorriente".

GDPR: no todo son escepticismos

Varios CISO consideran que "GDPR va a jugar un papel fundamental, ya que tiene aplicaciones en el terreno de los procesos de negocio", y se perfila como un "dinamizador de la protección empresarial". Otros se muestran más escépticos, señalando que su implementación corrobora que se están llevando a cabo las tareas pertinentes para cumplir con la normativa. Algo muy subjetivo, la solución es "establecer estándares en las empresas". Sobre este asunto, no hay que perder de vista el intrincado mundo del sector de las telecomunicaciones. Determinar la figura del DPO para que "sea un miembro proveniente de dentro de la compañía que conozca los pormenores de la misma", se antoja primordial.

"WannaCry fue una prueba de que no estamos libres de amenazas y de que debemos estar alerta"

Estrategia de seguridad, clave en la empresa

También se reconoció la importancia de configurar una estrategia de seguridad integral –desde el proceso de diseño de software–, y dirigida tanto a trabajadores como a clientes finales, además de contar con un departamento específico para coordinar la seguridad entre el resto de unidades.

Coincidieron en que el sentimiento de desafección por parte de los CEO hacia la seguridad de la empresa ya no es tal. Nuevas herramientas a su disposición han aumentado significativamente la implicación del consejo administrativo.

Colaboración público-privada

La escasa atención que se le presta a la propiciación de un canal de comunicación continuo entre el sector privado y el público fue uno de los mayores lamentos expresados. La existencia de una organización, incluso a nivel supranacional como sugirió el presidente de la Comisión Europea Jean-Claude Juncker, que impulse la colaboración entre los países de Europa, y de otros continentes, puede suponer un revulsivo.

WannaCry, ¿piedra de toque?

Los medios fueron el altavoz que difundió el ataque perpetrado por WannaCry y que elevó el ransomware a estatus de peligro inminente global. Esta repercusión fue, en cierto modo, celebrada por los expertos por constituir una campaña agresiva de 'awareness' y mostrar a la sociedad un escenario que es más una realidad que una amenaza lejana. Pese al revuelo mediático, las empresas españolas vivieron el ataque con cierta tranquilidad gracias a una reacción por su parte que los CISO calificaron como "muy satisfactoria".

"Lo peor está por llegar"

Libramos una batalla permanente frente al cibercrimen. Estamos expuestos a los ciberataques y sólo nos queda asumir que somos vulnerables y concienciarnos de que el riesgo está ahí. Aunque "lo peor está por llegar", no está todo perdido. Este mensaje fue una de las principales conclusiones de la segunda mesa celebrada en el Foro y en la que participaron Check Point, Commvault, GMV, Sophos, IECISA y OVH.

El futuro que dibujaron resultó desalentador: "Soy pesimista. La tecnología está en todas partes y las amenazas también. Podemos protegernos, pero el gasto en protección no será infinito. Lo importante es gestionar el riesgo". Esa gestión pasa por la innovación permanente, por invertir en personal y en soluciones tecnológicas. "Una parte del presupuesto de las empresas tiene que ir a las inversiones en seguridad". Potenciando la prevención e identificando cuál es el escenario en el que trabajar (cloud, movilidad o redes).

Estamos en una carrera: "los cibercriminales persiguen a los clientes y los fabricantes tenemos que correr para darles la mayor seguridad". Pero para los usuarios la seguridad debe ser un habilitador de negocio. Fabricantes, proveedores de servicios e integradores tienen que evangelizar sobre su importancia y coordinarse y trabajar en conjunto para solventar las amenazas.

"La clave no es si me va a tocar a mí o no, sino cuándo". En este entorno, "hay que darse cuenta de la importancia del dato y protegerlo garantizando unos niveles de servicio adecuados". Porque, eso sí, "lo que no he protegido previamente no lo voy a recuperar".

Sea como fuera, "lo peor está por llegar". Habrá que prepararse para plantarle cara pero con un punto a nuestro favor: la digitalización. Las empresas están inmersas en un proceso de transformación digital en el que se están redefiniendo los procesos y las operaciones; es el momento en el que hay que involucrar a todos los departamentos desde el inicio.

"GDPR sería un gran dinamizador de la seguridad en las empresas, pero pocas compañías en España se han adaptado a ella"

Estrategia a medida del cliente

En el debate salió a relucir el 11S, que demostró que el análisis de riesgos no funcionó y marcó un antes y un después configurando la táctica actual de "prepararse para todo". Sin embargo, el peligro máximo no sabemos cuál es. Te preparas para lo que conoces invirtiendo en los recursos razonables. La clave es valorar el peso de cada aplicativo y empresa. Hoy se plantean soluciones ad hoc a las necesidades del cliente.

Plan de contingencia

WannaCry fue una prueba de que no estamos libres de amenazas globales y de que debemos estar alerta. Cuando llega un ataque de este tipo el mínimo impacto es económico, es más de operaciones, de sistemas. La mejor estrategia es tener un plan de continuidad de negocio, algo que ya está en la agenda de las empresas.

Como Europa

España no está peor que otros países de nuestro entorno. Quizás sea a consecuencia de la globalización, que hace que el gap sea menor, pues no sólo llega tecnología, también procedimientos o políticas. El nivel de seguridad que hay en España es bastante nuevo y alto, pero no se valora. De ahí la fuga de talentos. Hay muchos profesionales y clientes versados en la materia. No obstante, faltan emprendedores, una estrategia general de seguridad y una concienciación del usuario. "La seguridad no ha arraigado suficiente así que nos queda mucho camino por recorrer". Sobre todo en cloud.