

“Hay que invertir en inteligencia de amenazas y tecnología robusta para fortalecer la seguridad”

Asusta pensar que los ataques de *adware* a los dispositivos móviles se han multiplicado por dos, así como el *spyware* comercial o los abusos del servicio de accesibilidad.

En esta entrevista, Daniel Creus, *security researcher*, *GReAT* de Kaspersky hace un repaso por el panorama de la seguridad empresarial y da algunos consejos a tener en cuenta para reforzar la seguridad de nuestras compañías.

Inma Elizalde



Daniel Creus, *security researcher*, *GReAT* de Kaspersky



El año pasado Kaspersky sorprendía presentando un nuevo enfoque en su negocio, pasando desde la ciberseguridad hacia el concepto de “ciberinmunidad”, por el que la seguridad no debe limitarse a proteger dispositivos sino al desarrollo de un ecosistema en el que todo lo que esté conectado, esté protegido. ¿Es este un reto asumible para las empresas?

Es la filosofía que tendrían que adoptar incluso las empresas que no tienen ese nivel de madurez en ciberseguridad, porque con los tipos de ataques que vemos, incluso utilizando *exploits* para los parches, tenemos que buscar alguna manera de hacer el camino del atacante mucho más difícil.

El mundo del cibercrimen es como una empresa. Lo cibercriminales van a ir a por lo más rentable y si conseguimos que valoren el esfuerzo, y que no vale la pena atacarnos, irán a por otra víctima.

En este mundo en el que los fabricantes van por un lado y los ciberatacantes por otro, si tuviera que hacerme una valoración DAFO del CISO español, ¿cuál sería?

No sé si soy la persona adecuada para hablar de CISO. Lo que sí sé es que en España tenemos una cultura de seguridad muy buena. Tenemos una cantera de seguridad de gente joven, incluso de CISO y otros ejecutivos que son realmente buenos. Si puedo decir, a nivel general, que debemos dejar de ver la seguridad como un gasto y verlo como una inversión, porque la historia nos ha demostrado que cuando no inviertes en seguridad, la inversión que vas a tener que hacer después del incidente va a ser mucho mayor. Tiene sentido tener cierta prevención.

Hablando de inversión, un estudio presentado por Kaspersky decía que, para este año, del total de la inversión prevista en TI, el 21 % iba a ir destinada a la seguridad.

Dentro de ese 21 % ¿dónde recomendaría invertir?

Simplificándolo, en dos vertientes. La primera, en una solución de seguridad robusta. Es decir, que una empresa tenga en cuenta la seguridad en sus diferentes capas. Ya no es suficiente proteger solo un dispositivo, tienes que proteger el perímetro de la red, la privacidad, etc. La tecnología tiene que ser multicapa.

La concienciación de los usuarios es fundamental. La tecnología es un aspecto importante, pero si tienes la mejor solución de seguridad del mundo, no haces caso a lo que tienes monitorizando y aceptas mensajes que te aconsejan instalar algo, eso no va a servir de mucho.

La segunda vertiente sería la inteligencia. Hay



“En Kaspersky ya no queremos decir tanto que protegemos un dispositivo, como que protegemos al usuario”

que invertir en inteligencia porque de esta manera podemos tener conocimientos de los adversarios y esto, muchas veces, nos puede ayudar a minimizar el tiempo de reacción

cuando ocurre un incidente.

Es decir, es una mezcla entre inteligencia de amenazas y tecnología robusta.

Con respecto a la inteligencia, la inteligencia artificial va a dominar el mundo, pero ¿cómo luchar contra una IA al servicio de los ciberdelincuentes? ¿Cuáles son los mayores peligros que nos amenazan?

Es un poco el juego del ratón y el gato. Siempre tenemos que adoptar soluciones, en parte, en base a los ataques que hacen “los malos” pero nosotros, como compañía de se-

guridad, tenemos que seguir innovando en todas aquellas áreas que nos pueda suponer minimizar ese tiempo de reacción del que hablábamos. Y en ese sentido, la inteligencia

artificial, la búsqueda de patrones, la heurística avanzada... es algo que ayuda a minimizar este riesgo.

Este es el año del 5G. ¿Cuáles son los mayores problemas de seguridad que se pueden desencadenar?

Yo creo que se producirá otro punto de inflexión similar a cuando teníamos la red de telefónica básica para conectarnos a Internet y un ordenador conectado, una hora o dos al día, con el que transferíamos un determinado número de datos.

Tal vez no sea un punto de inflexión tan agresivo, pero el hecho de que tengamos cada vez más poder de conexión y los dispositivos cada vez más tiempo conectados, y más capacidad de canal para mover información, tiene sus peligros. Uno de ellos es filtrar información.

De alguna manera la superficie de amenazas se amplía, por lo que los ciberatacantes tienen más donde jugar y donde atacar.



¿Cuáles van a ser los sectores más amenazados este año? Imagino que todos los relacionados con los datos.

Por un lado, los cibercriminales van a ir donde puedan ganar dinero, atacando a un usuario,

una empresa o un banco. Esto es algo reiterativo que venimos viendo.

Por otro lado, veremos ataques más dirigidos a empresas especializadas, e incluso empresas que trabajan con finanzas, con criptomonedas...

Cuando hablamos de seguridad, ¿tenemos que implementar las mismas medidas? ¿Sirven las mismas soluciones para un sector u otro?

La base puede ser la misma. Aquí entraríamos en el tema de hablar de modelado de riesgos, es decir, intentar saber qué es lo que yo tengo, qué quiero proteger y qué es lo que me va a atacar. En ese sentido no son las mismas medidas de seguridad, pero para eso es necesario saber el patrón de riesgo.

Imagino que las grandes empresas tienen estos modelos de riesgos porque necesitan priorizar en qué invertir en seguridad y una manera de hacerlo es llevar a cabo un modelo de riesgos.

¿Cuáles son los mayores riesgos de pasar la infraestructura de una empresa a la nube?

Básicamente dejar nuestros datos en una infraestructura en la que no tenemos control. Dicho esto, las empresas que actualmente se mueven en el *cloud* son muy conscientes de esto y toman todas las medidas que pueden para proteger nuestros datos. Es una cuestión de control. De alguna manera tienes los datos en tu perímetro, sabes lo que tienes que hacer, cómo hacerlo. En otro caso, tienes todos tus datos en un proveedor ajeno a ti, que muchas veces te ofrece capacidades de control como si estuvieras en tu casa, pero es una diferencia en cuanto a dónde guardar los datos. Riesgos también tiene guardar los datos en tu casa y no tener una buena seguridad.

En cuanto a la seguridad de las APIs, ¿cuáles son las mayores amenazas que están por llegar?

Ya hemos visto el abuso de APIs o incluso APIs no documentadas de redes sociales, por la cual

es posible extraer información, que en teoría debería ser privada. Eso ya recae, de alguna manera en el proveedor de redes sociales. Hay que tener mucho cuidado en qué se expone. Esto se ha demostrado en grandes redes sociales en las que alguien podía pedir información que, en teoría, estaba marcada como privada por los propios usuarios de la red. Es una cuestión pura y dura de seguridad, de qué datos quieres hacer accesibles.

¿Cuáles son los mayores *stoppers* en el mundo de la seguridad, aparte de que los responsables de seguridad no cuentan con el dinero que necesitan?

Un poco la concienciación. Puedes no tener un gran presupuesto en seguridad, pero puedes hacer una campaña de concienciación que pueda ayudarte a minimizar mucho los riesgos.



Es una pata clave de la seguridad y privacidad.

¿Dónde va a poner el foco Kaspersky este año?

Ha cambiado un poco el paradigma y ya no queremos decir tanto que protegemos un dispositivo, como que protegemos al usuario. Queremos no dar por hecho que un dispositivo es un usuario, sino no vamos a proteger al usuario como tal. Esto implica nuevas coaliciones, nuevas asociaciones. Implica cambiar nuestros productos para adaptarlos.