ENTREVISTA

Juanjo Fuster: "Hoy cualquiera puede meterte pornografía infantil en el ordenador"

ENRIQUE FUERIS | Palma 14 ENE. 2018 | 10:29

El fundador de Intec y experto en ciberseguridad, Juanjo Fuster. / JORDI AVELLÀ

Le pregunto si él también es de los que recomiendan tapar la cámara del portátil con esparadrapo. «Espera un segundo». Vuelve con su móvil en la mano, totalmente parapetado. Toda precaución es poca en un mundo en el que hemos pactado compartir un espacio común en el que depositamos nuestras vidas, desde la cuenta bancaria a las citas por WhatsApp. Juan José Fuster, bunyolí de 41 años, es socio fundador de Intec, la única empresa en Baleares con certificación CERT (Equipo de Respuesta ante Emergencias Informáticas). Probablemente la primera de las muchas que llegarán mientras nos acostumbramos a teclear bitcoin y *spear fishing* en Wikipedia.

P. Si un gigante como HBO no puede evitar que le roben Juego de Tronos, ¿qué posibilidades tengo yo

R . Creo que esa ha sido la serie más saqueada de la historia (risas). Pero fue gente de dentro: siempre hay amenazas internas y externas y hay que saber protegerse. La gente de a pie también debe saber cómo tomar precauciones.

P . ¿Cuánto tiempo dedican en su empresa a estar simplemente al día?

R . Invertimos entre un 25% y un 35% de nuestro tiempo sólo en estar al día y actualizar conocimientos. La seguridad es algo muy dinámico, la disciplina informática con más movimiento. Hay que estar en constante formación, si no en un mes te quedas obsoleto. Cada día salen miles de amenazas nuevas porque detrás hay mafias que se dedican profesionalmente a esto. Avanza a una velocidad impresionante y la ciberdelincuencia ya es a día de hoy el negocio ilegal que más volumen de dinero genera en todo el mundo.

P . ¿Cree que no se presta suficiente atención a estos riesgos?

R . Sí, sobre todo en las empresas. Lo ven como algo lejano y lo entienden como un gasto, no como una inversión. Hay algo muy peligroso en este desconocimiento porque implica que las empresas creen estar seguras si tienen un informático que les lleva la web y el mantenimiento de los ordenadores. Es un error capital. Nosotros colaboramos con empresas informáticas con las que nos complementamos porque entienden que ese no es su núcleo de negocio. Y luego te encuentras con empresas que te dicen «yo es que ya tengo un informático que es muy bueno y ya se encarga de todo esto». Están equivocadísimos. Yo he presentado informes periciales forenses de más de 100 páginas que ya le costaba entender al propio informático porque es algo muy específico.

P . Usted asegura que es precisamente la pequeña y mediana empresa la más expuesta.

R . Son el objetivo principal de los delincuentes a día de hoy porque al no estar protegidas es más fácil robar mil veces 3.000 euros que tres millones a una gran empresa de una vez. Se acaban dando cuenta cuando ven que no les cuadran las cuentas. No tienen medidas de seguridad, solo el antivirus que les instala el informático. No quieren invertir.

P . ¿Los ataques a pymes provienen de competidores directos?

R . De competidores, de trabajadores descontentos, de mafias que intentan sacar dinero…

P . ¿Cuesta encontrar a gente que esté realmente preparada para desarrollar este trabajo?

R . Los fichajes que espero hacer próximamente vendrán de fuera. En Baleares no hay nadie y en España sí hay gente pero están colocados o trabajan para empresas de fuera. Yo me he cansado de buscar. Encuentras a gente que te dice que sabe de redes o de Linux o de configuraciones de red, pero de seguridad no saben. La seguridad informática es una disciplina en sí que necesita de un background extenso y específico.

P . ¿Una titulación prepara a alguien para entrar en el mundo de la ciberseguridad?

R . Es el sector donde menos se valora la titulación: existe pero no sirve para medir la habilidad real. Conozco a gente que no ha estudiado informática pero son máquinas. Y gente con una carrera de informática que no sabe ni cómo se ataca ni cómo se defiende. Hacen falta buenos formadores pero la gente que sabe prefiere trabajar en algo que se le pague bien y no formando. Eso sí: la formación debe ser con buenos profesionales, no con tutoriales de Internet. Sobre todo porque a veces esos mismos tutoriales son subidos por los propios ciberdelicuentes.

P . Explíqueme qué es un hacker.

R . Normalmente la gente asocia el nombre con el hacker malo, el pirata informático. Hay una definición que

P . ¿Cuáles son los países que llevan más ventaja en este terreno?

R . En congresos internacionales ves que los más avanzados son Estados Unidos, China, Rusia e Israel. A nivel de concienciación, Europa va detrás, España va a la cola de Europa y Baleares a la cola de España. En términos de ciberseguridad, Baleares está en niveles tercermundistas. Si a eso le añades que aquí hay bastante riqueza pues esto se convierte en Disneylandia para la ciberdelicuencia. Es contradictorio porque uno se protege en el mundo físico con cerrojos, alarmas, seguros, cajas fuertes... Pero en el mundo virtual la gente no se protege.

P . ¿Qúe experiencias ha tenido en Baleares en este sentido?

R . He tenido clientes que han tenido un incidente serio y después han seguido con sus proveedores de siempre. La gente no está concienciada. Nosotros llevamos el caso de una importante constructora de Mallorca que hacía un año que no estaba ganando contratos y no sabía por qué. Había dejado de facturar cinco o seis millones de euros. Alguien había entrado en el servidor donde preparaban las ofertas y estaba sacando toda la información para dársela a otras empresas que eran las que ganaban los contratos. En esta empresa tenían un informático pero nunca pensaron que debían invertir en ciberseguridad.

P . ¿Es tan habitual el hackeo a nivel balear?

R . Sí, lo que pasa es que la gente no lo dice, no se hace público. Son daños para la imagen y para los clientes. Normativas como la nueva Ley de Protección de Datos Europea van a hacer que cuando haya un incidente de seguridad alguien se tenga que responsabilizar de ello. El empresario no quiere hacer ese gasto porque no es consciente del peligro en el que a día de hoy ya está inmerso y los informáticos dicen que están preparados para proteger a la empresa cuando no lo están porque tienen miedo a perder su trabajo. Eso es una negligencia. La gente va a ir cobrando conciencia con el tiempo pero me temo que va a ser a base de palos. De cada diez nuevos clientes que cogemos en España a nueve ya les ha pasado algo.

P . ¿Reciben también encargos de particulares?

R . El grueso de nuestro trabajo es con empresas pero también ha acudido gente a la que le vigilan el móvil, la ex pareja que ha contratado a alguien para hackearle el ordenador, etc. En Mallorca también pasa bastante. Sólo a nosotros nos llegan dos casos al mes. Un conocido recibió un mensaje de extorsión por unas imagenes extraídas de la cámara de su portátil en las que se le veía entrando en su cuarto con una chica que no era su pareja.

P . ¿Cómo lo hacen?

R . A través de emails, cosas de internet que no deberías bajarte, etc.

P . ¿También hay ciberguerrilla en el mundo de la política?

R . Desde luego. A nosotros han acudido políticos de Baleares y de ámbito estatal a los que habían hackeado para obtener información. Con ellos y con todos nuestros clientes establecemos canales de comunicación totalmente seguros para que nadie sepa de qué hablamos.

P . ¿El aparato judicial está preparado para los ciberdelitos?

R . Al ser algo tan nuevo está todo muy verde: ni los jueces ni los abogados están al día. El problema es que casi no hay legislación ni jurisprudencia. Explícale tú a un juez que resulta que un señor que está en Ucrania ha conseguido entrar en tu ordenador por email con un ataque de spear phishing y te ha metido un troyano que te ha instalado un software capaz de mostrarle tus conversaciones con un cliente y ha vendido esas informaciones

a tu competencia. El juez te va a decir «conozco películas de Spielberg que no tienen tanto argumento. No

P. ¿Puede la policía con sus medios hacerse cargo de un mundo tan vasto como el del cibercrimen?

R. Están muy preparados pero saturados de trabajo. Nosotros les llamamos si encontramos cosas que pueden ser delitos como pornografía infantil y ellos nos piden sobre todo asesoramiento técnico cuando tienen mucha carga de trabajo. No pueden estar al día como estamos nosotros ni tienen nuestras herramientas. La ciberseguridad será cosa del sector privado. Ya es así.

P. ¿Hay también motivos para preocuparse por la cuenta bancaria?

R. Las entidades bancarias, por la cuenta que les trae y por la propia naturaleza de su negocio, tienen grandes medidas de seguridad, lo que pasa es que el delincuente prefiere no pegarse con el banco, sino con los clientes. Hackear a los bancos pasa en las películas; la forma realista es atacar al eslabón más débil, los clientes. Si consigues entrar en la cuenta de 1.000 personas puedes hacer muchas extracciones perqueñas en vez de una grande.

P. ¿Cómo operan estas mafias?

R. Funcionan como empresas, tienen un modelo de negocio con franquicias. Por ejemplo, crean un malware que es capaz de entrar en ordenadores y robar información, lo distribuyen para que otras mafias y otros delincuentes lo usen y después van a medias, como una franquicia.

P. ¿Cree que el precio por compartir este espacio común ha sido demasiado alto?¿Estamos vendidos?

R. La verdad es que ahora somos mucho más vulnerables. Es así: estamos vendidos. Pero el mayor peligro es la baja concienciación y el intrusismo que hay en la seguridad. Tenemos que utilizar las cosas con conocimiento pero tampoco hay que volverse locos. Es cierto que todas estas nuevas tecnologías son una mejora en nuestra calidad de vida pero llevan implícitos unos riesgos. Hay que saber qué riesgos son y controlarlos. El internet de las cosas, por ejemplo, es otro vector de ataque muy importante. Compras una smart TV que pones en el salón de casa, con una cámara y sin medidas de seguridad y desde ahí alguien se puede conectar y verte a ti con tu familia viendo la tele. Eso ya está pasando. Ya se hackean coches y ya se podía provocar un accidente así. La ropa inteligente, por ejemplo, se puede utilizar para espiar al usuario.

P. ¿El bitcoin es otra alfombra roja para el ciberdelincuente?

R. Totalmente. El problema más grande que le veo es que tú tengas bitcoins y alguien entre en tu wallet (cuenta bancaria) y te los robe.

P. Con los recursos de un hacker no hace falta ni guardar material comprometedor en el disco duro, se podría introducir...

R. Sí, si consigo entrar en tu ordenador y mi finalidad no es robarte al menos lo usaré para atacar a otro y que parezca que el ataque es tuyo. Hoy día cualquiera con conocimientos puede meterte pornografía infantil y si un día le pilla la policía, él no tendrá nada, lo tendrás tú. Y demuestra entonces que no has sido tú. Ya se han dado casos.

P. ¿Qué opina de la creencia de que quien crea el virus crea el antivirus?

R. De esto se lleva hablando desde los años 80. La primera vez que oí hablar de ello fue con MacAffee. Puede pasar, pero a día de hoy, habiendo ya tanta mafia y tanta gente ejerciendo «el rol de malo»... Si fuera cierto que las empresas de antivirus crearon los virus en algún momento ahora ya no tendría tanto sentido.

P. ¿A día de hoy ya somos analfabetos sin conocimientos informáticos avanzados?

COMENTARIO

coralisima
14/01/2018 21:14 horas

#1

Ante la imposibilidad de exponer mi punto de vista respecto al artículo de opinión firmado en EL Mundo (Baleares) firmado por LolaSampedro, titulado 'Yo tb soy puritana'(pues su autora no da la oportunidad de replicarla..), utlizo el foro abierto en esta información. Es vergonzoso e indign leer más

Ver 1 comentario →

Enlaces de interés