La Razón (Cataluña)
Comunidad de Madrid
29/05/17
Prensa: Diaria
Tirada: 250 Ejemplares
Difusión: 250 Ejemplares
Cód: 110724651
Página: 6
Sección: CATALUÑA Valor: 19.384,00 € Área (cm2): 748,1 Ocupación: 91,75 % Documento: 1/1 Autor: Ángela LARA- Barcelona Núm. Lectores: 1000

Ángela LARA– Barcelona

**–¿Qué se entiende por un ciberataque? ¿Qué características ha de tener para ser considerado como tal?**

– Cualquier actuación ilegal sobre sistemas informáticos, mediante la cual se puede intentar conseguir un beneficio económico o un beneficio reputacional o sencillamente provocar pérdidas en la organización atacada. La Unión Europea, a través de la directiva comunitaria, lo que hace es establecer unos mínimos de impacto que ha de tener este ataque para que sea obligatorio informar del mismo a las autoridades competentes de cada país y compartir información con el resto de organizaciones similares. Este impacto se mide en función de la cobertura nacional de los usuarios afectados y el importe económico del daño que se puede causar. Pero un ataque puede ser sencillo, también.

**–¿Cuáles son los principales riesgos a los que estamos expuestos?**

– Los riesgos más importantes ante los que nos tenemos que defender probablemente sean los ataques a la identidad para las personas y los procesos de negocios para las empresas. En el caso de las personas, eso puede hacer que perdamos la identidad y afecte a nuestra vida personal y en el caso de las empresas quiere provocar que dejen de dar servicio a los clientes y, por lo tanto, pierdan la capacidad de negocio.

**-¿Qué se debe hacer a nivel gubernamental para prevenir un ciberataque?**

-Ya hace unos 5 años que la Agencia Europea de Seguridad estuvo ayudando a todos los países europeos a crear unas estrategias nacionales de ciberseguridad, que España adoptó en su momento, mediante las cuales se definen unas estrategias que deben hacer los gobiernos para defenderse y entre las cuales figura la creación del CERT del Centro Nacional de Inteligencia, así como la creación del INCIBE como una herramienta para ayudar a las administraciones locales y a las empresas, y además el CERTSI, que es el CERT para proteger a los provedores de servicios esenciales para la sociedad de los ataques que puedan sufrir.

**– Y a nivel de usuario, ¿qué podemos hacer?**

-A nivel de usuario, hay que seguir las instrucciones y recomendaciones que nos dan desde estos centros. La primera recomendación básica es tener los sistemas actualizados, que es justo lo que no han aplicado las empresas afectadas por el útlimo gran ciberataque mundial. Luego también se recomienda utilizar contraseñas que sean difíciles de reproducir de una forma más o menos automática por los atacantes. Otra recomendación importante es activar los sistemas de doble autentificación: hay gente reacia a dar el número de móvil para validar los accesos a sus cuentas de redes sociales, por ejemplo, por miedo a recibir publicidad en el móvil, pero la realidad es que es mucho peor que te puedan robar la identidad porque no haya la posibilidad de utilizar este doble factor a través de móvil que el daño que te puede causar el que te envíen un mensaje de publicidad al móvil.o año

«ES IMPOSIBLE ESTAR A RESGUARDO DE LOS CIBERATAQUES. LOS PRODUCTOS COMERCIALES TIENEN ERRORES»

«LOS DISPOSITIVOS TOTALMENTE SEGUROS SON LOS QUE NO ESTÁN CONECTADOS A INTERNET»

**-¿Estamos preparados para hacer frente a cualquier tipo de ciberataque?**

–No, realmente es prácticamente imposible estar a resguardo de cualquier ciberataque porque los programas informáticos se lanzan al mercado sin haber pasado unos controles de calidad y de seguridad exhaustivos. Eso solo sucede en aernaves comerciales, centrales nucleares...pero los productos comerciales normales tienen errores, los cuales cuesta descubrir porque supone invertir mucho dinero en ello y normalmente los descubren investigadores financiados por mafias o gobiernos que se dedican a encontrar la manera de explotar esos errores para conseguir el control de los ordenadores.

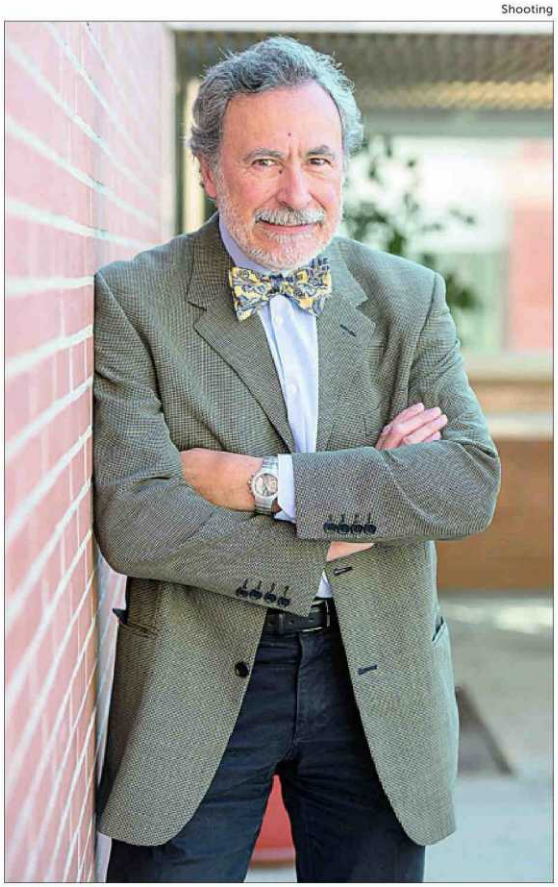
**– Detrás de un ciberataque que resulte existoso, ¿siempre hay un fallo del sistema?**

– No siempre. Hay veces que se utiliza lo que se llama ingeniería social, mediante la que se engaña a un usuario de la organización para que introduzca un programa en el ordenador y ese programa directamente se ejecuta sin explotar ninguna vulnerabilidad del sistema.

**–Parece que en la sociedad de la información y las tecnologías es cuando más desprotegida está nuestra información.**

– La diferencia fundamental es que con los sistemas de información actuales, nos pueden robar la información desde cualquier punto del planeta sin necesidad de desplazarse. Eso hace que los costes de acceso a la información de forma ilegal sean mucho más baratos y se puedan realizar de forma masiva.

Shooting



## MANEL MEDINA

DIRECTOR ACADÉMICO DEL MÁSTER EN CYBERSECURITY MANAGEMENT DE LA UPC Y DIRECTOR DEL ESCERT-UPC

# «Hay que cambiar la estrategia e introducir formación básica en ciberseguridad»

**– Hay quien habla incluso de la posibilidad de que se puedan generar desastres a nivel mundial mediante ciberataques. ¿Es eso posible?**

– Sí, de hecho hace más de medio año que el gobierno de Estados Unidos está alertando a sus centrales de producción de energía eléctrica de que extremen las precauciones y seguridad de sus sistemas para evitar sufrir un ataque. Llevar a cabo un ciberataque y provocar un apagón nacional es posible con la tecnología de hoy en día.

**– ¿Algún día tendremos algún dispositivo que sea totalmente seguro?**

– Los dispositivos totalmente seguros son los que no están conectados a internet y que no tienen conexiones.

**– ¿Hay un perfil de quien lleva a cabo un ciberataque?**

– Los más habituales son las mafias, que han pasado de utilizar pistolas a usar ciberarmas, y los gobiernos, que se están preparando para poder realizar ciberataques a otros países en caso de necesitarlo. También están los hactivistas, que realizan ataques para llamar la atención sobre actuaciones poco éticas de algunas organizaciones.

**– ¿Las personas mejor preparadas para combatir estos ciberataques son los propios hackers?**

– Hay quien piensa que los hackers son los malos, los que provocan los ataques, y hay gente que piensa que el hacker es el altruista que se dedica a buscar fallos en los sistemas para advertir a los fabricantes. En realidad, con independencia de la motivación, si entendemos por hacker un experto que es capaz de descubrir errores en los sietemas informáticos y modificarlos para que o bien se pueda explotar ese error o bien se pueda evitar que se pueda explotar, entonces efectivamente son los mayores expertos que hay. Así, estos hackers pueden ser cibercriminales, o hackers de sombreros blanco o éticos. En este sentido es importante el tema de formación. La mayoría de empresas no disponen de suficiente personal suficientemente cualificado para defenderse de los ataques y para prevenirlos y esto básicamente sucede porque se estima que solo en España se necesitan más de 20 mil técnicos en ciberseguridad y la capacidad de producción de técnicos es del orden de la décima parte de esta cifra. Hay que cambiar las estrategias de formación e introducir formación básica en ciberseguridad en las carreras universitarias.