"La seguridad 100% no existe", pero el Centro Criptológico Nacional se encarga de detectar y gestionar los ciberataques y establecer las mejores medidas para mitigarlos. El segundo jefe del área de Ciberseguridad de este organismo, adscrito al Centro Nacional de Inteligencia (CNI), Pablo López, explicó ayer las potenciales amenazas en el curso 'Seguridad, Paz y Defensa en Canarias', organizado por la Universidad Nacional de Educación a Distancia (UNED) en la capital grancanaria.

Pablo López

Segundo jefe del Departamento de Ciberseguridad del Centro Criptológico Nacional del CNI

"Rusia y China son los estados que lanzan más ciberataques contra España"

Haridian Mederos
LAS PALMAS DE GRAN CANARIA

El segundo jefe de Ciberseguridad del CCN del CNI, Pablo López.| JOSÉ CARLOS GUERRA

¿Qué papel juega el CNI en las ciberamenazas?

Un papel muy importante. Cuando tienes que tratar la ciberamenaza hay que considerar tres pilares: uno es la defensa de las redes, que es a lo que nos dedicamos nosotros, el Centro Criptológico Nacional, encargado de gestionar incidentes, prevenirlos, detectarlos, determinar las mejores medidas para mitigarlos y evitar su propagación. La Inteligencia de Señales aborda el acceso a los datos. Y la Inteligencia va más allá, una vez que detectas un ataque no te puedes conformar con los detalles técnicos, sino determinar el *modus operandi* y el interés que hay detrás.

¿Cuáles son las potenciales amenazas?

Lo que más nos preocupa son las amenazas persistentes avanzadas, un tipo de ataque que suele estar dirigido y desarrollado con infraestructuras y recursos al alcance de muy pocos. De hecho, detrás de este tipo de ataques suelen estar los estados, capaces de introducirse en un sistema sin dejar rastro. Estas amenazas son muy difíciles de detectar, se mantienen durante mucho tiempo en el sistema de la víctima y, desgraciadamente, han venido para quedarse.

¿Sólo los estados?

Sí, porque son normalmente los únicos que se pueden permitir estos lujos. Aunque últimamente también ha cambiado este paradigma y con las publicaciones de WikiLeaks, por ejemplo, se han puesto al alcance de mucha gente herramientas que antes solo se podían permitir los estados. Esto aumenta la posibilidad de que haya otros actores, ajenos a los gobiernos, con estas capacidades de ataque o que incluso se contrate a alguien para que desarrolle estas capacidades, es lo que llamamos el cibercrimen como servicio.

¿Un ciberataque es la mayor amenaza que puede haber hoy?

Ahora mismo sí. Hay numerosas modalidades de ciberataques que pueden agruparse por las motivaciones de los atacantes, su repercusión o por los daños ocasionados. Los ciberataques pueden afectar a operadores de servicios esenciales para la sociedad y sus infraestructuras críticas. El ciberespionaje es una de nuestras principales amenazas.

¿Qué estados son los que ahora lanzan más ciberataques?

Rusia y China son los estados que más están atacando a España. Eso lo tenemos medido, pero ¿eso implica que tenemos la evidencia de que sean ambos países? No. Por el análisis técnico que hacemos y por el *modus operandi* llegamos a esa conclusión. Una evidencia para poder acusar a esos estados no tenemos, pero sí información que, analizada en base al interés geopolítico en un momento dado y el *modus operandi*, lleva a esa conclusión.

> "Desde enero hemos gestionado 11.500 incidentes, 47 de ellos críticos, relacionados con el ciberespionaje"

> "Usar redes sociales implica que mucha gente sepa mucha información de ti, hay que tener cuidado"

¿Por qué esos dos países están atacando a España?

Rusia por el interés geopolítico y China por el interés económico.

¿Qué 'armas' tiene el CNI contra los ciberataques?

Aparte de nuestra Capacidad de Respuesta a Incidentes (CCN-CERT), es fundamental el Esquema Nacional de Seguridad. Es una normativa, desarrollada a través de un Real Decreto que define las medidas de seguridad que se deben aplicar el sector público. Así conseguimos que todos los organismos públicos implementen las medidas de seguridad desde el primer momento para conseguir un entorno lo más seguro posible y estar menos expuestos a ciberataques.

¿Cuántos han logrado frenar?

No hablamos de frenar ciberataques, sino de gestionar incidentes. Tenemos desplegadas 150 sondas en organizaciones del sector público y en empresas de interés estratégico. Estas sondas son un sistema de alerta temprana que permite detectar los incidentes. En lo que va de año hemos gestionado alrededor de 11.500, mientras que el año pasado fueron 21.000. El dato importante es que desde enero hemos gestionado 47 incidentes críticos relacionados con ciberespionaje, con estados. En este caso hablamos de amenazas persistentes avanzadas, algo que sólo se pueden permitir los estados.

¿Y el año pasado?

45 en todo el año.

¿A qué obedece el aumento de incidentes?

Cada año aumenta un 15 o 20% el número de incidentes que gestionamos. El incremento se debe, no sólo a que se produzca un mayor número de ataques, que también, sino que hemos mejorado nuestra capacidad de detección, monitorización y vigilancia de la red. Cada sonda gestiona entre 10 y 15 incidentes al mes.

¿En Canarias hay sondas?

Sí, dos en el Gobierno de Canarias y vamos a desplegar otra en la Universidad de Las Palmas de Gran Canaria. Hemos llegado ya a un punto de madurez en el que los organismos son conscientes de que tienen problemas, deben aplicar medidas y piden ayuda para formar parte del sistema de alerta temprana del CCN-CERT.

¿Están los gobiernos preparados ante estos ataques?

De acuerdo a los últimos acontecimientos podemos pensar que sí, pero la realidad es que necesitamos mucho más recursos técnicos, personales y económicos para atender esta amenaza.

¿Las empresas están concienciadas del peligro o solo una vez que son atacadas?

Empiezan a ser conscientes cuando son atacadas, pero ya se va llegando a un nivel en el que apuestan por implementar medidas antes de tener el problema.

¿Cuáles son las medidas mínimas que debe tener cada empresa o institución para no ser víctimas de un ciberataque?

La solución es el Esquema Nacional de Seguridad, que contiene 75 medidas. La seguridad es un servicio integral. No hay una solución en un momento dado, sino en su conjunto, por lo que hay que tener procedimientos, organización y una estructura de seguridad.

¿Podría exponer varias recomendaciones imprescindibles?

Tienes que asegurar tu perímetro, tener una política de interconexión adecuada y unos cortafuegos correctamente configurados. Primero debes determinar tus activos a proteger, el tipo de servicio que prestas, hasta qué punto es sensible, la gestión de riesgos y ver en qué eres vulnerable. Nosotros categorizamos como los sistemas como de categoría básica, media o alta y en función de eso aplicamos medidas más o menos exigentes.

¿Cómo pueden protegerse los ciudadanos?

Deben ser conscientes de dónde se están moviendo en el mundo virtual y tener capacidad de detección y respuesta. Hay que tener cuidado con el uso de los dispositivos y configurar su seguridad para limitar lo que se expone. El uso de las redes sociales implica que mucha gente sepa mucha información de ti y hay que tener en cuenta medidas de seguridad, pero no entrar en paranoias. Hay una cosa típica que son los vectores de infección, es decir para que alguien entre en tu sistema tiene que infectarte, normalmente con un correo electrónico dirigido, que asumes como legítimo porque habla como tú, en tu idioma y de una temática que das por buena porque coincide con lo que expones en las redes sociales. El problema es que lo gestionas, le das a un enlace y abres un PDF, un Word o la macro de un Excel que viene con un código dañino.

¿Ahora hay más ciberataques?

Se tiene esa sensación porque, de repente, se le ha dado mucho bombo y platillo. Han tenido mucha repercusión mediática. Los dos últimos son WannaCry y Petya. Otra incidencia que hubo fue por ejemplo el Struts2, una vulnerabilidad de Java en servidores web Apache y ésa sí que nos hizo daño, pero no tuvo tanta repercusión, porque quizás con WannaCry quien estaba detrás pretendía también que tuviese esa repercusión mediática.

¿Cuáles son los objetivos de los ciberataques? ¿Ganar dinero? ¿Destruir información?

Hay varias cosas. El estado que quiere hacer ciberespionaje quiere pasar desapercibido y nunca va a generar ruido, a no ser como el caso de las elecciones en Estados Unidos, que a lo mejor se intentó cambiar la opción de voto, pero esos son análisis posteriores. Lo que está claro es que cuando detrás de esto hay un beneficio económico, entonces el cibercrimen tiene presencia. Cuando se secuestran ordenadores lo que se busca es que se pague un rescate. También hay hackers que prestan sus servicios para que alguien pueda realizar un ataque.

¿Un gobierno tiene la capacidad de verdad de influir en el voto de los ciudadanos de otro país?

Esperemos que no, pero eso sí que nos genera cierto desasosiego.

¿Es muy difícil de demostrar?

Sí, muy difícil, pero después de lo que vimos en las elecciones de Estados Unidos, este año en Europa han habido muchas elecciones y los estados han estado muy preocupados para evitar que eso pasara, que hubiera una opción de influencia sobre el voto del ciudadano, porque eso es lo más sagrado que tenemos y atentar contra eso es atentar contra lo más sagrado que puede tener cualquier sociedad.