PlantaDoce.

ADN

Vanesa Díaz: “En cinco años toda nuestra información sanitaria puede estar en jaque”

La consejera delegada de LuxQuanta, empresa dedicada a la fabricación de claves cuánticas de variable continua, asegura que hay que empezar a pensar en un sistema nuevo de ciberseguridad con capacidad para aguantar los ataques de computación que están a la vuelta de la esquina.

D. Quiñonero
27 abr 2023 - 04:58

Mayor inversión en ciberseguridad para protegerse de los ataques. Vanesa Díaz es especialista en telecomunicaciones por la Universidad de Cantabria y está especializada en desarrollo de mercado, marketing y telecomunicaciones ópticas. Díaz es consejera delegada de LuxQuanta, empresa dedicada desde 2021 a la fabricación de claves cuánticas de variable continua, advierte de que tanto las entidades públicas como privadas deben hacer un ejercicio de autoconciencia y revisión constante para combatir a los *hackers*, y asegura que “hay que empezar a pensar en un sistema nuevo de ciberseguridad, con capacidad de aguantar el ataque de una computación tan potente como la que está a la vuelta de la esquina”.

https://www.plantadoce.com/adn/vanesa-diaz-en-cinco-anos-toda-nuestra-informacion-sanitaria-puede-estar-en-jaque

El presente contenido es propiedad exclusiva de PLANTADOCE EDICIONES, SLU, sociedad editora de PlantaDoce (www.plantadoce.com), que se acoge, para todos sus contenidos, y siempre que no exista indicación expresa de lo contrario, a la licencia Creative Commons Reconocimiento. La información copiada o distribuida deberá indicar, mediante cita explícita y enlace a la URL original, que procede de este sitio.

Pregunta: ¿El sistema está preparado para controlar el volumen de datos que manejan las empresas?

Respuesta: Hoy en día casi toda la información que transmitimos está encriptada y controlada. Ahora mismo, los computadores no tienen la capacidad para hackear esas llaves. No obstante, en cinco o siete años habrá ordenadores cuánticos que podrán poner en jaque toda nuestra información sanitaria en tránsito. Por eso, hay que empezar a pensar en un sistema nuevo de ciberseguridad, con capacidad de aguantar el ataque de una computación tan potente como la que está a la vuelta de la esquina.

P: ¿Cómo está España en materia de ciberseguridad?

R: No tengo las cifras de España pero estoy segura de que es equiparable a cualquiera de los países más potentes de Europa. Estamos trabajando de manera diligente en nuestra seguridad. No obstante, tenemos que concienciarnos más porque la situación a nivel geopolítico se está volviendo más complicada, cada vez hay más problemas de espionaje entre los países y también hay grupos de ciberataques que se dedican a lucrarse a través de romper la seguridad de empresas privadas o públicas. La gente se está volviendo más consciente de que la inversión debe de seguir escalando porque la picardía de nuestros enemigos es más alta y están mejor equipados. China lleva invertido decenas de billones y dispone de la red terrestre y satélite más grande de esta tecnología.

P: ¿La filtración del Hospital Clínic de Barcelona se podría haber evitado?

R: Hoy en día tendríamos que ser capaces de soportar una gran cantidad de ataques. La picaresca de los hackers es cada vez más potente y están mejor equipados, precisamente por la inteligencia artificial, porque es capaz de confundir a las personas sin darte cuenta. Si en ese momento no teníamos la herramienta para evitar un ataque, a raíz de estos fallos se diseñará y encontrará una.

“Todos somos susceptibles, incluso los usuarios privados, de que alguien se haga con nuestra información y puedan usarla en nuestra contra”

P: **La Generalitat planteaba en ese momento que sufría una media de 4,3 millones de ataques diarios. ¿Es un problema sistémico?**

R: Es sistémico. La cifra que comparte la Generalitat es la que va a reportar cualquier empresa o incluso una cifra mayor. Siempre va a haber alguien fuera que va a intentar hacer dinero de una manera fraudulenta. No es que los centros de datos estén más expuestos que un hospital, que un banco o cualquier otro sector. Es inherente a la sociedad humana en el mundo digitalizado. Se generan oportunidades

El presente contenido es propiedad exclusiva de PLANTADOCE EDICIONES, SLU, sociedad editora de PlantaDoce (www.plantadoce.com), que se acoge, para todos sus contenidos, y siempre que no exista indicación expresa de lo contrario, a la licencia Creative Commons Reconocimiento. La información copiada o distribuida deberá indicar, mediante cita explícita y enlace a la URL original, que procede de este sitio.

para que la gente de manera fraudulenta se lucre. Habrá que legislar para ayudar y habrá que hacer frente a ello.

P: ¿Cómo se puede prevenir?
R: Todos somos susceptibles, incluso los usuarios privados, de que alguien se haga con nuestra información y puedan usarla en nuestra contra. Tenemos que hacer un ejercicio de autoconciencia constante y pensar en los medios en los que nos movemos, y en función de eso evitar que alguien nos robe la información. Esto mismo debe hacer cualquier entidad, además de hablar con expertos de ciberseguridad para protegerse. Es posible que instauremos una serie de medidas útiles hoy, pero que de aquí a cinco años el enemigo se ha equipado con herramientas más punteras.

P: ¿Qué puede hacer la Administración?
R: Lo que están haciendo es concienciar de las herramientas que tenemos y de los riesgos que hay fuera. A nivel gubernamental, europeo, se debe informar a la entidad pública o privada de los riesgos a los que nos estamos presentando y darle a entender dónde podría encontrar las herramientas que podría utilizar para los ataques.

P: ¿Faltan expertos en ciberseguridad en las empresas de la salud?
R: No creo. Cuando ocurre una brecha, la información es muy sonora, pero nadie se plantea que los expertos en ciberseguridad no estén acertados en otras empresas. Yo creo que la concienciación es bastante uniforme y homogénea y todos somos conscientes del tipo de información que se está manejando.

“Nuestra responsabilidad es poner el foco en lo delicado de la información que estamos cediendo”

P: ¿Qué pueden hacer los pacientes?
R: Nuestra responsabilidad es poner el foco en lo delicado de la información que estamos cediendo, en este caso estamos confiando que la entidad en la que depositamos la información se haga cargo. Creo que lo que hacemos es correcto y al final hay un movimiento social y mundial que entiende lo delicado de esta información y la pone en valor. La última ley europea de protección de datos muestra que lo que hacemos esta correcto que es darle la importancia que tiene a esa información que estamos volcando.

P: **¿Existen más expertos en ciberseguridad que nunca?**
R: Sí, cada vez se crean más. Actualmente, existe la figura del director de seguridad de la información y ciberseguridad (Ciso, según sus siglas en inglés), que es la

El presente contenido es propiedad exclusiva de PLANTADOCE EDICIONES, SLU, sociedad editora de PlantaDoce (www.plantadoce.com), que se acoge, para todos sus contenidos, y siempre que no exista indicación expresa de lo contrario, a la licencia Creative Commons Reconocimiento. La información copiada o distribuida deberá indicar, mediante cita explícita y enlace a la URL original, que procede de este sitio.

persona encargada de la ciberseguridad en una entidad, esta figura es relativamente nueva. Al trabajar en remoto se genera más información en tránsito y digital que es susceptible de ser boicoteada. El volumen de inversión en ciberseguridad ha ido subiendo en los últimos años.

P: ¿El riesgo en ciberseguridad puede ser un freno a la digitalización del sector?
R: No, para nada. Los recursos que vamos a tener del lado de la sociedad que se digitaliza y del número de mentes siempre va a ser mayor que las personas con intenciones dudosas. Siempre vamos a estar por delante de la gente que quiere hacer un mal uso de esta digitalización. Es parte del progreso. En la historia de la humanidad siempre ha habido novedades que se han introducido y con ellas también ha habido riesgos.

“Siempre vamos a estar por delante de la gente que quiere hacer un mal uso de esta digitalización”

P: ¿Qué cambios recomendaría para poder mejorar la ciberseguridad?
R: Revisar los sistemas de seguridad que están implementados, tanto en entidades públicas como privadas. Revisar si el plan que tengo es potente e intentar alcanzar un plan de seguridad óptimo, y revisarlo periódicamente porque las circunstancias pueden cambiar y la capacidad de mi atacante irá mejorando. Los ciudadanos debemos hacer un ejercicio de autocrítica y pensar si estamos protegidos o tenemos que ser más diligentes.

P: ¿La inteligencia artificial aumentará el peligro de ciberataques?
R: Sí, ya lo está haciendo. Hay formas de ataque como el *fishing* en los llegaban correos spam en los que te decía que habías ganado un premio, o te entregaban un paquete con un enlace para que rellenaras los datos. Hasta la fecha era más fácil de discernir, porque la redacción no era muy buena en ciertos aspectos. Con las herramientas de inteligencia artificial se puede conseguir un tono de mensaje muy bueno, máquinas que son capaces de replicar el tono de voz de cualquier persona. Para contrarrestarlo, por ejemplo, la Policía Nacional está empezando a establecer una serie de pautas en este sentido para anticiparse a estos ataques. El trabajo de las empresas privadas y de la administración es darle a la gente la noción del riesgo que podemos correr potencialmente.

https://www.plantadoce.com/adn/vanesa-diaz-en-cinco-anos-toda-nuestra-informacion-sanitaria-puede-estar-en-jaque

El presente contenido es propiedad exclusiva de PLANTADOCE EDICIONES, SLU, sociedad editora de PlantaDoce (www.plantadoce.com), que se acoge, para todos sus contenidos, y siempre que no exista indicación expresa de lo contrario, a la licencia Creative Commons Reconocimiento. La información copiada o distribuida deberá indicar, mediante cita explícita y enlace a la URL original, que procede de este sitio.