Éxito en ciberseguridad, lo que une al Real Betis y al Ayuntamiento de Marbella

efe.com/andalucia/2024-05-10/exito-en-ciberseguridad-lo-que-une-al-real-betis-y-al-ayuntamiento-de-marbella

10 mayo 2024

Álvaro Vega I Córdoba, (EFE).- El Real Betis es mucho más que un equipo de fútbol, tiene cuatro tiendas y un centro logístico, y el Ayuntamiento de Marbella tiene más empleados que la Diputación de Málaga y lo que les une es la visión que despliegan sobre la ciberseguridad, lo que les permite avanzar en sus negocios y servicios.

La empresa israelí 'Check Point' ha reunido en Córdoba a especialistas del sector alrededor de la ciberseguridad para analizar los riegos de los ciberataques y el blindaje digital ante amenazas en dispositivos, donde la Inteligencia Artificial (IA) juega ya un papel esencial en la defensa, y también en los ataques.

Así lo ha dicho a EFE el director técnico de 'Check Point' Iberia, Eusebio Nieva, para quien "es cierto que ahora tenemos mucha más ayuda que la que teníamos antes, sobre todo por parte de la IA, a pesar de que también es una herramienta que están utilizando los ciberatacantes para ataques. Es más aliado de los defensores que de los atacantes, por ahora".

De hecho, su compañero de empresa, Víctor Molina, ingeniero responsable de uno de sus departamentos, destaca en su intervención en la jornada que generalmente "el vector de entrada es el correo electrónico", que se puede generar mediante IA. Y para no dejar duda, generó al principio de su exposición la suplantación de una mensaje de correo de la Agencia Estatal de Administración Tributaria con un aplicativo que "se puede encontrar buscando durante una hora en internet".

Ayuda adicional

Nieva explica que la IA "está siendo utilizada de forma masiva por los defensores como una ayuda adicional para reconocer y prevenir esos ataques. Creo que ahora es una de las herramientas que tenemos más importantes dentro de nuestro arsenal para reconocer los ataques".

Éxito en ciberseguridad, entre el Betis y Ayuntamiento de Marbella. El director técnico de 'Check Point' Iberia, Eusebio Nieva, durante una entrevista con EFE. EFE/Salas

El responsable de Sistemas y Ciberseguridad del Real Betis Balompie, Luis Quintero, ha puesto de manifiesto que la entidad "ha crecido mucho en muy poco tiempo" y que por ello "nos hemos tenido que apoyar en la tecnología", dado que "hacemos mucho más que fútbol".

En esta línea, ha explicado que la transformación comenzó en 2016, cuando entonces el club disponía de cortafuegos tipo 'pyme' y una situación similar en todo lo relativo a la seguridad informática. "Estos datos hace ocho años eran nefastos", ha asegurado.

Por ello, para afrontar el crecimiento, como abordar abrir cuatro tiendas y un almacén logístico, poner "una empresa funcionando en dos meses", lo que ha hecho esdotarse de soluciones, que llegan a conocer si el móvil por el que se accede a su aplicación móvil el abonado está comprometido y bloquea su acceso y le informa de la vulnerabilida d.

El usuario, el mayor riesgo de la seguridad

El jefe de Servicio de Nuevas Tecnologías del Ayuntamiento de Marbella, José Alonso Ayllón, que ha expuesto que la institución municipal dispone de 130 sedes y 4.000 trabajadores, ha destacado que el mayor riesgo para la seguridad informática "es el usuario".

Ayllón ha hecho énfasis en los servicios críticos que se gestionan desde el ámbito municipal, como son la Policía Local, los Bomberos y Protección Civil y la necesidad de garantizar la disponibilidad de las herramientas informáticas que se utilizan, debido a que

“si no funcionan, no se saben utilizar las que usaban antes”, como puede ser un callejero que no sea digital.

El experto ha descrito que “a veces el detalle más insignificante te tumba el sistema de seguridad” y ha puesto como ejemplo que hace unos días la monitorización centralizada que tiene el Ayuntamiento de Marbella ha impedido entradas ilegítimas en una cuenta de correo electrónico especifica del municipio, 423 desde la propia Marbella, tres desde Asia y dos desde Estados Unidos.

El responsable técnico de Marbella ha insistido en la necesidad de contar con sistemas redundantes de comunicaciones o de alimentación eléctrica. “A veces tenemos soluciones sencillas y nos damos cuenta cuando ha sucedido la emergencia. A veces las soluciones no vienen de la IA”, ha subrayado.

En opinión del responsable de información y datos del grupo agroalimentario Migasa, Luigi Gutiérrez, la seguridad se basa en la “segmentación y parcheo”, el “monitoreo continuo” y las “actualizaciones y parches”, una política que aplica en la maquinaría de producción de la que es el cuarto envasador del mundo de aceite de oliva.

Diferentes fases de un ataque

En opinión del responsable técnico de ‘Check Point’ para España y Portugal, “en ciberseguridad siempre hay que estar atento a las diferentes fases de un ataque, entre otras cosas porque cada una de ellas nos puede dar una pista de cuándo va a producirse en concreto, ya que hay fases en las cuales hay una primera intrusión, que es, digamos, la cabeza de playa con la que consiguen los atacantes entrar dentro de la compañía”.

En todo caso, “el problema es que una vez que ha ocurrido esa emergencia, lo que tenemos que tener es un plan de actuación. Y ese plan tiene que haber sido creado con antelación, porque si no, lo más probable que puede ocurrir es que no podamos actuar de manera correcta, como en cualquier emergencia”.

Para Nieva, “los planes son importantísimos, pero si tenemos defensas preventivas que son capaces de detener esos ataques o de avisarnos de que se pueden producir o de que se están produciendo, vamos a ganar mucho más antes de la emergencia”. EFE