Alumnos de Tknika, en Errenteria, participan en una sesión de Cyber Range en la que aprenden a neutralizar ciberataques.
FOTOS ARIZMENDI

Enseñar a hackear para proteger

Cyber Range. Alumnos de FP de ciberseguridad testean en Tknika un sistema para aprender a contener los ataques informáticos. «Nos enseñan cómo actúa el criminal para hacer el bien»

VERÓNICA MELO

La seguridad es uno de los principales quebraderos de cabeza en los entornos digitales. El robo de datos está a la orden del día, y si algo temen las empresas, y los particulares, es que 'alguien' se introduzca en su sistema. En Errenteria, en el centro de investigación aplicada de la educación y la Formación Profesional vasca, Tknika, están probando una herramienta para reforzar la formación de sus alumnos de ciberseguridad, el Cyber range.

Está planteado como un juego, se trata de que los estudiantes, en un entorno seguro, pongan a prueba sus conocimientos para que se conviertan durante unas horas en piratas informáticos. «Les planteamos una serie de retos que tienen que ir superando en entornos que nosotros mismos creamos», explica Jon Labaka, director ejecutivo del centro. «En realidad les enseñamos a hackear para que, en un futuro, puedan proteger», resume. «Cuando aprenden a atacar un sistema, también aprenden a detectar sus debilidades».

Como todo lo que se hace en Tknika, es un proyecto en pruebas y tiene el objetivo de ser compartido con otros centros. «Ahora estamos probando, viendo qué funciona, qué se puede mejorar a través de la experiencia de los propios alumnos, cómo tienen que plantear los retos los profesores... La idea es instalarlo en 25 centros de FP, así que cuando llegue a ellos estará totalmente perfilado y habrá terminado su tiempo en Tknika», describe Labaka.

Una sesión de Cyber range es intensa. En grupos de tres, los alumnos tienen que superar retos en un tiempo asignado. La concentración es máxima y la competitividad también. «Es la gammificación de lo que han aprendido en ciberseguridad en un entorno amigable», expone Ibai Peña, responsable del área de ciberseguridad en Tknika. «Es un ejercicio muy pegado a la realidad».

Jon Bilbao reconoce sentirse «tenso» con la sesión que le ha tocado. «Está difícil porque no te dan muchas pistas. Te obliga a ser proactivo», explica. «Primero tienes que conocer cómo actúa el criminal, saber por dónde te puede venir el ataque para luego hacer el bien. Es una buena técnica», cuenta. Ese aspecto ético es algo en lo que desde los centros se insiste. «Es un pilar fundamental que como sistema educativo nos toca trabajar, pero no es algo novedoso», dice Labaka.

Otro alumno que da fe de que los retos son «complicados» es Aitor Pérez, que afirma que pese a la intensidad, se lo está pasando bien. Decidió estudiar ciberseguridad porque lo veía compatible con sus estudios de robótica. «Los usuarios no son tan conscientes de la necesidad de protegerse. Espero que las empresas sí lo sean y demanden profesionales».

La preocupación por el uso de los datos en un entorno digitalizado es constante. «Bien utilizados, los datos te abren múltiples posibilidades, pero si te los roban o te los usurpan, tienes un problema», comenta Labaka. «En la formación de estudiantes de FP es muy importante que todos aquellos que utilizan datos

Dentro del grueso de los delitos informáticos conocidos, más del 90% son estafas cometidas a través de internet. De los 4.338 casos denunciados en Gipuzkoa en 2021, se lograron esclarecer 50. En este sentido la Fiscalía de Gipuzkoa en su última memoria aprecia un «desmedido aumento de denuncias por delitos de estafa cometidas a través de Internet (carding, phising, pharming, vishing, smishing, spamming, etc.)», si bien reconoce que «un gran número» de ellas «se archivan provisionalmente de manera automática por falta de autor conocido». Esto se debe a que por lo general las IP desde donde se realiza la estafa «apuntan a uno o varios países extranjeros y la cuenta bancaria beneficiaria del importe estafado suele estar en otro distinto». Además, señalan desde la Fiscalía que cuando consiguen identificar a una persona detrás de una estafa, resulta ser una víctima a la que han robado los datos y usurpado la identidad para la comisión del delito. Estos casos también se archivan por las mismas razones.

Difícil de agilizar

Jorge Bermúdez afirma que, «mientras las cosas sigan como están, resulta difícil agilizar la persecución de estos delitos», y lo hace en parte por la labor policial, limitada por la falta de medios. «Muchas veces la lucha contra el cibercrimen es una cuestión vocacional. Lo que sucede es que tras unos cuantos años en los que se adquiere experiencia, muchos de estos agentes acaban abandonando estas unidades por la sobrecarga de trabajo y el escaso reconocimiento, con una retribución básica y una categoría funcionarial en la que no se ve reconocida su alta especialización», apunta Bermúdez, quien considera que «el estudio, perfeccionamiento y especialización de la policía tiene que ser una apuesta clara y decidida» si en el futuro se quiere reducir esa cifra negra de casos sin resolver.

LAS CLAVES

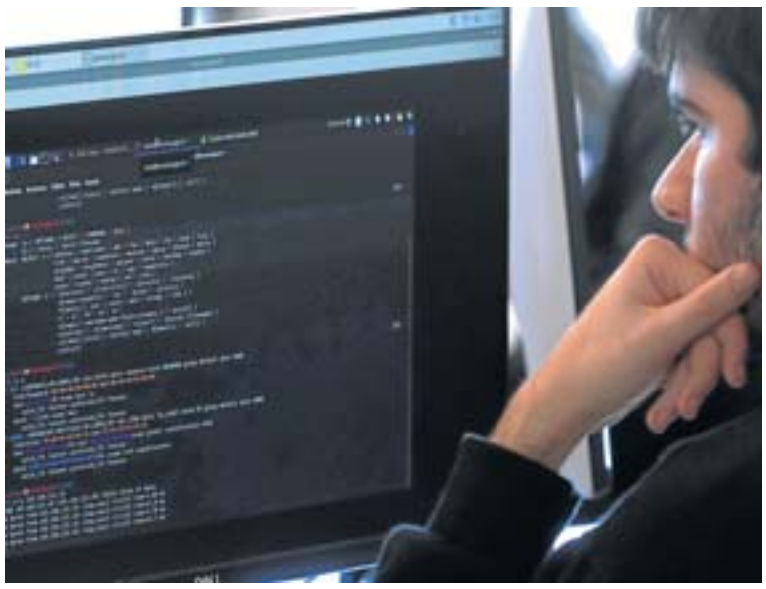
ANONIMATO

«La tecnología pone cada vez más fácil las cosas a quien quiere ocultar su identidad»

SEGURIDAD

«El perfeccionamiento y especialización de la policía tiene que ser una apuesta clara y decidida»

Dos alumnos escudriñan las pistas informáticas que les han dejado los profesores.



Los estudiantes califican como «tensas» las sesiones de Cyber Range.

sean conscientes de la necesidad de gestionar entornos seguros».

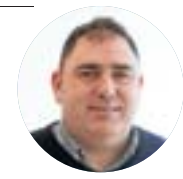
En Euskadi ocho centros de Formación Profesional imparten la especialidad de Ciberseguridad, tres de ellos en Gipuzkoa (Zubiri-Manteo y Politekniko Easo en Donostia, y Uni Eibar Ermua). Más allá de esta formación especializada, Labaka tiene claro que desde los centros educativos hay que trabajar desde dos perspectivas diferentes: la cultura general de la ciberseguridad y la específica de las redes informáticas.

«El 70% de las intrusiones están vinculadas a una decisión personal. Es decir, una persona que no ha tomado la opción correcta», señala Labaka. «Un click a un anuncio falso, abrir un correo que parece del banco pero que no lo es...», describe. «La otra parte tiene que ver con las redes informáticas. Ahí estamos más acostumbrados a utilizar usuario y contraseña. Es en este área donde enseñamos a los alumnos de informática a crear entornos seguros».

Muestra de la cantidad de ataques que se pueden recibir, Tknika tiene instalados 100 servidores aislados del resto de máquinas para comprobar la intensidad del trabajo de los hackers. Llegan a contabilizar 90.000 ataques en tan solo un minuto. «Antes eran personas, ahora están automatizados».

TESTIMONIOS

Jon Labaka
Director General de Tknika



«La idea es instalar 25 equipos de Cyber Range en centros de FP»

Ibai Peña
Responsable de ciberseguridad

«El objetivo es verificar la capacitación a través de retos»

Jon Bilbao
Estudiante

«Son clases tensas en las que te obligan a ser proactivo»

EL DATO

70%

de las instrusiones ciber están vinculadas a la toma de decisión de una persona que no ha sido la correcta, un click a un anuncio falso, la apertura de un correo sospechoso o anotar los datos personales en una web no segura.

Interior aplicará el reconocimiento facial automático para resolver crímenes

Las imágenes de los escenarios de delitos se compararán con un fichero de 5 millones de fotos de fichados por la Policía a partir de esta primavera

MELCHOR SÁIZ-PARDO

MADRID. Será en el mes de abril. O, a lo sumo, en mayo. Estos son los plazos en que el Ministerio del Interior se mueve para comenzar a utilizar la herramienta que muy probablemente va revolucionar la investigación policial: el sistema automático de reconocimiento facial.

Según los documentos e informaciones recabados por este periódico, el programa, que se denomina ABIS (Sistema Automático de Identificación Biométrica, por sus siglas en inglés), será capaz de identificar en segundos a la persona que aparezca en cualquier grabación de cámaras «públicas y privadas» y facilitar una identidad si el sujeto en cuestión está en las bases de personas fichadas de la Policía y la Guardia Civil. Las policías autonómicas, por el momento, no van a cebar con sus reseñas los archivos que usará el ABIS, pero está previsto que lo hagan en el futuro.

Esta herramienta casi de ciencia ficción, que viene testándose desde hace años en la Sección de Antropología Forense de la Comisaría General de Policía Científica, cotejará las imágenes grabadas en los lugares de los crímenes con las 1.347.120 reseñas que ha introducido ya en el sistema el instituto armado y las 3,5 millones de fotografías «indubitadas» de sospechosos que el CNP está acabando de volcar. En dos o tres semanas, según los responsables de Interior, el enorme archivo de fichados, «salvo problemas técnicos», deberá estar operativo y listo para usarse con el ABIS.

Los informes del ministerio y las numerosas respuestas del Gobierno a preguntas parlamentarias afirman que en ningún caso las fuerzas de seguridad del Estado recurrirán al ABIS para el control de personas en espacios públicos, como sí hace desde hace años de manera masiva el Gobierno chino. Tampoco –promete el Ejecutivo– se utilizará nunca para cotejar con bases ajenas a las de los sujetos fichados, como podría ser el fichero fotográfico del DNI.

«ABIS se utilizará exclusivamente en investigaciones llevadas a cabo por las fuerzas de seguridad del Estado en materia de prevención, investigación y detección de infracciones penales», asegura el Gobierno.

1.500 terminales en aeropuertos y pasos fronterizos

Thales, la gran empresa militar francesa detrás del ABIS, además de trabajar en el proyecto de reconocimiento facial automático para resolver delitos, está embarcada en la implantación en todas las fronteras españolas de 1.500 terminales para la identificación de pasajeros también a través del reconocimiento de las facciones del rostro. El 'Entry Exit System' estará implantado en mayo con escáneres faciales en todas las fronteras del país: 44 aeropuertos, 33 puertos y cuatro pasos terrestres.