elEconomista.es 17/10/2019

EL ECONOMISTA
Prensa: DIARIO
Tirada: 20.563
Valoración: 6.584 €
Sección: ECONOMIA
Difusión: 13.847



ISTOCK

# CIBERSEGURIDAD

# Las universidades son las terceras instituciones más atacadas

**Noelia García** MADRID.

Datos es sinónimo de ataque. Hoy, los *hackers* tienen cada vez más capacidades para atacar a personas y empresas y acceder a su información confidencial. Las personalidades de ámbito público son especialmente vulnerables.

Según el estudio de *Ciberseguridad en el sector universitario*, llevado a cabo por Deloitte, el 80 por ciento de las universidades participantes declararó haber sufrido algún incidente en los últimos 12 meses. De ellas, el 62 por ciento ha sufrido entre dos y cinco ciberataques y el 10 por ciento recibió más de diez. Y es que a más digitalización, mayores riesgos y más responsabilidad de asegurar los datos.

El año pasado, los investigadores de Kaspersky –compañía internacional dedicada a la seguridad informática con presencia en aproximadamente 200 países– detectaron 931 ataques a más de 130 universidades en 16 países. Los atacantes buscan credenciales de empleados y estudiantes, sus direcciones IP y datos de ubicación. En la mayoría de los casos crean una página web de apariencia idéntica a la original, que engaña a los usuarios para introducir sus claves de acceso y entrar en los sistemas digitales de las universidades.

**Para contribuir a una mayor seguridad en las evaluaciones se utilizan 'softwares' antiplagio**

España fue, en 2018, el tercer país que más ciberataques recibió. De hecho, este tipo de ataques han aumentado un 600 por ciento en cuatro años en España, ya que en 2014 el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) registró en torno a 18.000 incidentes y en 2018 superaron los 111.000. Por ello, un 69 por ciento de los directivos y responsables de TI cree que las soluciones de seguridad con las que trabajan sus empresas están desactualizadas, aunque más de la mitad (51 por ciento) afirma que han adquirido soluciones de ciberseguridad durante el último año para abordar potenciales problemas en este ámbito, según un nuevo estudio de VMware en colaboración con ForbesInsights.

Según el Centro Criptológico Nacional (CCN), adscrito al CNI, ya se registran tres agresiones *críticas* diarias. Además, los *hackers* roban en la actualidad, a nivel internacional, por valor del 0,8 por ciento del PIB mundial y el ataque por excelencia, el *ransomware*, ha aumentado un 350 por ciento.

## Repunte estacional

Hoy, las instituciones educativas ocupan el tercer lugar a nivel mundial, en términos de vulnerabilidad en ciberseguridad. Y los investigadores de Proofpoint –empresa de seguridad empresarial– aseguran que hay un repunte estacional en el *phishing* con temas universitarios, especialmente entre junio y octubre, mientras los estudiantes se preparan para la escuela y cerca del comienzo del otoño. Una campaña universitaria típica de *phishing* es de volumen medio –miles o decenas de miles de mensajes por día–. Las campañas generalmente no están orientadas geográficamente, sino que están vinculadas a universidades específicas con plantillas de *phishing* desarrolladas para portales de administración de bibliotecas y estudiantes. Los actores de amenazas distribuyen mensajes que contienen enlaces o archivos adjuntos HTML que dirigen a las víctimas a portales de inicio de sesión universitarios clonados.

Pasa a la página siguiente >>>

elEconomista.es 17/10/2019
EL ECONOMISTA
Prensa: DIARIO
Tirada: 20.563
Valoración: 7.853 €
Sección: ECONOMIA
Difusión: 13.847


>>> Viene de la página anterior

Según Proofpoint, los daños de los ataques entre 2013 y 2017 fueron: la pérdida de propiedad intelectual por un valor aproximado de 3.400 millones de dólares debido a acceso no autorizado; 31,5 terabytes de datos académicos y robo de propiedad intelectual de universidades comprometidas; 7.998 cuentas universitarias fueron comprometidas con éxito en todo el mundo; y 3.768 cuentas comprometidas que pertenecían a profesores de universidades con sede en Estados Unidos.

David Emm, investigador de seguridad de Kaspersky, indica que "la información que se podría obtener a través de un ataque de *phishing* –correos fraudulentos que buscan infectar o robar información– que tenga éxito en este tipo de instituciones puede ser particularmente valiosa: sus bases de datos contienen muchos tipos de investigaciones de impacto y exclusivas sobre diversos temas, desde la economía hasta la física nuclear. Además, dado que muchos de ellos colaboran con importantes fabricantes para sus doctorados, los actores de amenazas pueden acceder a datos que contienen no solo una experiencia única, sino también información privada y potencialmente comprometedora sobre las empresas".

Asimismo, la prevención es la mejor herramienta para combatir los ataques. Emm indica que "un consejo clásico, pero muy válido tanto para el personal como para los estudiantes, es comprobar la barra de direcciones del sitio en el que se van a introducir los datos confidenciales. Pero como este método se basa únicamente en el factor humano, la principal recomendación para las instituciones educativas es utilizar la autenticación de dos factores, y para los usuarios, una solución de *software* con capacidad *antiphishing*".

## Secuestro de datos

Los principales enemigos para las instituciones educativas son "el *ransomware* –*malware* que secuestra tus datos y te pide un rescate para recuperarlos– como principal amenaza, junto con el *phishing*", afirma Ivan Mateos, *sales engineer* en Sophos Iberia.

Fuentes de la Universidad Pontificia Comillas aseguran que ellos están "haciendo un gran esfuerzo en campañas de concienciación interna, ya que profesores y alumnos son claves para la prevención y detección de amenazas. En los últimos 12 meses no hemos sufrido incidentes graves o brechas de seguridad que hayan requerido notificación a la autoridad competente, pero continuamente estamos observando intentos de ataque y rechazándolos satisfactoriamente".

Asimismo, Isaac Marco, director de Tecnologías de la Información (IT Director) en la Universidad a Distancia de Madrid, Udima, explica que ellos están "más expuestos que otras universidades por el hecho de que el cien por ciento de la interacción con nuestros estudiantes se hace a través de un campus virtual". "La gran mayoría del *software* que utilizamos para estos servicios es Software Libre, y esto quiere decir que el código fuente es público y puede ser estudiado por cualquier persona, incluso por los malos".

**La seguridad completa en el mundo de Internet no existe, pero sí buenas prácticas relacionadas**

Por su parte, Benjamín Sádaba, director de Infraestructuras de Unir, asegura que "la seguridad completa en el mundo de Internet no existe: hay buenas prácticas basadas en una valoración de los riesgos asociados con estar conectados a Internet". "Cuando recibimos algún ataque concreto y localizado procedemos al bloqueo sistemático del tráfico en cuestión, y en caso de necesidad contactamos con el proveedor de conectividad para que pueda encargarse del bloqueo de forma más efectiva", añade.

Pero por mucho que las universidades pongan todo su empeño en protegerse, siempre hay un agujerito por el que se cuelan los malos. Por ejemplo, en la madrugada del 10 al 11 de enero de 2019, la Universidad de Valladolid fue víctima de un *hackeo*. Asimismo, en el mes de febrero, un grupo de ciberdelicuentes que se hace llamar *Digital Research Team* aseguraba haber accedido a las bases de datos de varias instituciones públicas españolas. También, esta semana, la cuenta oficial de Twitter de la Universitat Jaume I (UJI) de Castellón ha sufrido un *hackeo* y ha publicado insultos y amenazas de muerte dirigidos a la alcaldesa de Castelló, Amparo Marco.

## Empleo y salarios

Aunque los sueldos superan de media los 45.000 euros, muchos puestos no llegan a cubrirse por falta de perfiles cualificados. La escasez de profesionales revierte en una mejora de los sueldos. La remuneración de un *ethical hacker* va de los 35.000 euros a los 70.000 euros en ciudades como Madrid y Barcelona, mientras que la de un *cybersecurity manager* oscila entre los 45.000 euros y los 90.000 euros al año. Según la *II Guía Spring Professional del mercado laboral*, elaborada por Adecco y dirigida a directivos de recursos humanos, CEO y directores generales, los *cybersecurity managers* son los mejor pagados en el ámbito de las telecomunicaciones. Además, cada vez es mayor el número de compañías, de todos los tamaños y sectores, que llaman a las escuelas de formación y empresas que ofrecen cursos especializados preguntándos por la formación necesaria para sus profesionales.

**La escasez de profesionales revierte en una mejora de los sueldos: hasta 70.000 euros**

David Emm, investigador de seguridad de Kaspersky, afirma que "el verdadero problema de la ciberseguridad no es el desempleo, sino la falta de cualificación. De acuerdo con distintos estudios, existe una brecha de casi tres millones de puestos de trabajo en la industria a nivel mundial. En Europa, la previsión es que exista una escasez de 350.000 profesionales de la ciberseguridad para 2022". Asimismo, añade que no es un "problema de falta de talento o de jóvenes prometedores que aspiren a trabajar en la ciberseguridad, sino que muchos de los roles en los que se demandan nuevos profesionales están en áreas poco conocidas y por tanto no hay suficientes candidatos para estos puestos".

La formación en ciberseguridad abarca un gran abanico de conocimiento y posibles puestos a cubrir. Así, por ejemplo, desde los Servicios Informáticos de la Universidad Complutense de Madrid indican que "se ha creado una unidad para desarrollar el Esquema Nacional de Seguridad (ENS), la Unidad de Seguridad y Protección de la Información (USPI), y se ha creado la figura del Delegado de Protección de Datos (por obligación legal) para la protección de datos personales.

Héctor Baragaño, director de Desarrollo de Negocio e Innovación Digital de Esic, comenta que "el puesto dedicado a esta función es la de CISO –*chief information security officer*– y será una de las profesiones más relevantes". Este perfil puede alcanzar un salario de 120.000 euros anuales, pues debe encargarse de velar por la privacidad de las empresas, ha de prevenir ciberataques y capacitar a los empleados para evitar prácticas que puedan afectar a la seguridad informática de la compañía.

Por su parte, Ivan Mateos también indica que, afortunadamente, en España "estamos viendo un incremento notable de la oferta formativa sobre ciberseguridad. Asignaturas relacionadas con este ámbito antes no aparecían en carreras de informática y telecomunicaciones y, sin embargo ahora, la gran mayoría de centros las han ido incorporando a su plan de estudio. Por otra parte, tanto universidades públicas como privadas así como escuelas de formación, e incluso fabricantes del sector, van aumentando esta oferta con cursos, charlas, certificaciones, foros y otras fórmulas, donde desde los más jóvenes hasta personas con muchos años de experiencia laboral pueden ir aumentando sus conocimientos".

Pero no solo las universidades han implementado cursos de posgrado para especializar a los profesionales tecnológicos, sino que el gigante Google tambien está tomando partido en esta batalla. El buscador ha lanzado un nuevo proyecto con el que pretende promover la ciberseguridad en nuestro país a través de la formación y concienciación a las pequeñas y medianas empresas, principales objetivos de ciberataques junto con los particulares, en tanto que tres millones de ellas carecen de sistemas de protección contra *hackers*. Google les ofrece herramientas para estar más protegidos e impulsar el ecosistema a través de líneas de acción educativa, de emprendimiento y empleabilidad.

ISTOCK