esadealumni

MAYO 2021

De directiva/o a consejera/o

5 tips con Abel Navajas,

cofundador de Woonivers, app 'tax-free' para viajeros y comercios

Esade Alumni celebra la 1ª edición de los Premios TFM MUA

Especial Seguridad Informática para Empresas

varios dispositivos entre sí, como ordenadores con dispositivos móviles, cuya finalidad es autentificar todas las identidades de los usuarios que pretendan entrar en las cuentas de la organización", añade.

A medida que las empresas maduran, lo hace también el mercado, que cada vez más apuesta por ofertas de servicios más flexibles y elásticos a través de modelos de prestación ofrecidos en modo "Security as a Service". Una de las ventajas de este tipo de servicios es que, a nivel presupuestario, permite gestionar la seguridad como un gasto operativo, en lugar de un gasto de capital. "Dichos servicios permiten a las empresas liberar recursos internos, mejorar su postura de ciberseguridad y beneficiarse de la experiencia, talento y conocimientos de empresas líderes en el sector. Otra tendencia que se observa a nivel organizativo es que la ciberseguridad va más allá del establecimiento de medidas de protección. Una buena ciberseguridad debe incluir capacidades organizativas de detección y respuesta", comenta **Lluís Vera**.

Hoy la demanda principal de las empresas es tener servicios de evaluación de vulnerabilidades basados en inteligencia artificial y soluciones de protección continua y piratería ética automatizada, ya que lo que más destaca en la seguridad puede ser suplantación de identidad, estafas virtuales que se manifiestan en todos los ámbitos a nivel personal y empresas, secuestros falsos a cambio de un rescate real... **Andrea-Giaime Bodei** explica que normalmente las empresas se supone que utilizan el *hacking* ético para simular ataques informáticos y proceder a las soluciones que lo impiden.

Pero también hay muchas preocupaciones a nivel de usuario: "Qué antivirus ponemos, qué aplicaciones podemos instalar, qué acciones podemos desarrollar y cuáles no... El entorno privado está asumiendo el equipo de trabajo como

> "Hoy la demanda principal de las empresas es tener servicios de evaluación de vulnerabilidades basados en inteligencia artificial y soluciones de protección continua y piratería ética automatizada"

parte de los equipos domésticos y esta convivencia es un reto para la ciberseguridad", puntualiza **Rubén Mora**. "Tenemos que buscar tecnología capaz de permitir la convivencia e intentar que trabajo y vida personal convivan sin mezclarse. No hay que olvidarse de que este reto ya estaba identificado por los expertos en ciberseguridad, pero actualmente es una tendencia que ha venido a quedarse", añade. Las estrategias de ciberseguridad encaminadas en el Zero Trust han de permitir armonizar la creación y desarrollo de las actividades de negocio con la combinación de los nuevos entornos de trabajo —teniendo en cuenta que muchos de ellos se desarrollaran en espacios que el trabajador combinará con su esfera más personal—, siendo un reto garantizar la seguridad del negocio y el respeto a su intimidad. Esta transformación es un tema fundamental para entender la ciberseguridad de este 2021.

PRIVACIDAD DE LA INFORMACIÓN

La incomodidad y la dilatación en la realización de todo proyecto por tener que aplicar medidas de seguridad son constantes en todas las organizaciones, pero no hay mayor riesgo que el no saber a qué riesgos nos enfrentamos para poder identificar todas aquellas medidas de seguridad que se deberían aplicar desde el inicio para poder evitar incidentes que puedan tener un impacto grave en la organización. En este sentido, la privacidad, desde el diseño y por defecto al que obliga el RGPD y la LOPD-GDD, así como la mayoría de las normativas de seguridad que velan por la privacidad de la información, por su disponibilidad, su integridad y confidencialidad, es uno de los procesos básicos que toda empresa debe llevar a cabo en su operativa cotidiana, comenta **María González**. Además, cualquier violación de seguridad que afecte a la privacidad de las personas o a la integridad de los datos de estas puede suponer un perjuicio importante para las organizaciones. "Sobre todo desde el punto de vista de penalizaciones económicas, como las consecuencias desastrosas en los procesos de negocio por no proteger la alteración o eliminación de datos por parte de terceros no autorizados", añade **Miguel Ángel Arroyo**.

Testimonios

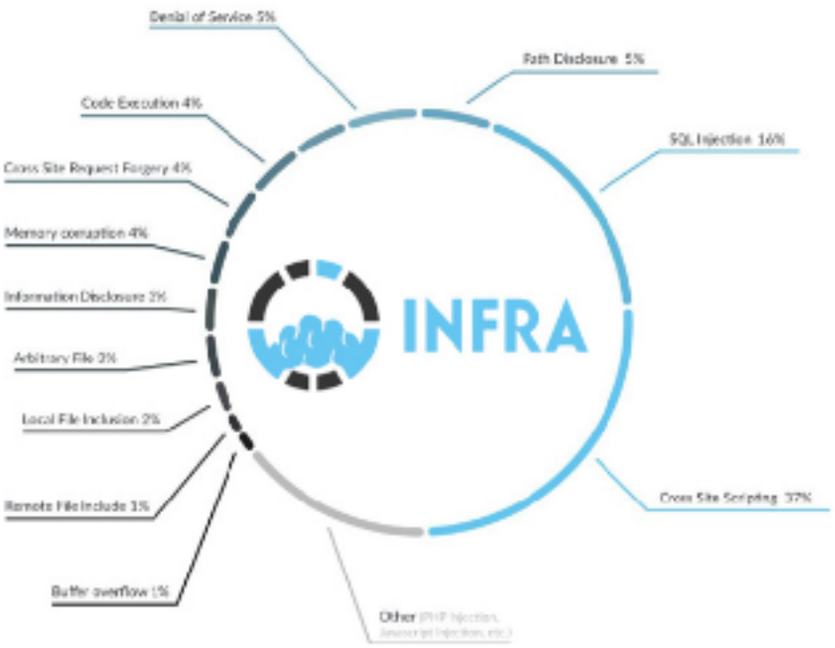
ANDREA-GIAIME BODEI
CEO de INFRA

MARÍA GONZÁLEZ
Responsable Técnica del Área de Ciberseguridad de ABAST

MIGUEL ÁNGEL ARROYO
Business Security Manager en SEMIC

ANSELM GARCÍA
IT Services Operations Manager de IDISC

INFRA, asesoramiento tecnológico y ciberseguridad



INTELLIGENCE FRAMEWORK PTE. LTD.

OFICINAS
Dirección postal:
19 CECIL STREET #04-01
THE QUADRANT AT CECIL
SINGAPORE (049704)
E-mail: info@infrascan.net
Web: www.infrascan.net

PERSONAS DE CONTACTO
CEO de INFRA: Andrea-Giaime Bodei

INFRA crea soluciones automatizadas que incluyen tecnologías de escaneo y *hacking* ético para evaluación e inteligencia que descubren vulnerabilidades conocidas y desconocidas en redes de computadoras y aplicaciones web.
El *hacking* ético tradicionalmente es realizado manualmente por un analista, así que los resultados no son homogéneos y estandarizados. Además los escáneres solo encuentran vulnerabilidades basando su búsqueda en datos públicos y antiguos, pero no encuentran problemas nuevos. Los escáneres comunes solo proporcionan informes técnicos, faltando informes ejecutivos y la evaluación de riesgos. Al automatizar, INFRA reduce el tiempo para analizar la seguridad y obtener más información sobre la competencia. El valor agregado de nuestra plataforma es brindar informes técnicos y también gerenciales, con calidad constante y permitiéndole repetir el análisis en cualquier momento.

PRODUCTOS Y SERVICIOS

- INFRA Cloud: compruebe si su nube y sitios web pueden ser pirateados.
- INFRA VM: todas las ventajas de INFRA Cloud, para chequear redes privadas.
- INFRA Cube: dispositivo de seguridad para analizar servidores, PCs y IoT.
- INFRA Mainframe: servidor clúster para analizar grandes redes a nivel *enterprise*.

VENTAJAS Y PUNTOS DIFERENCIALES

- Utiliza la tecnología Machine Learning para encontrar nuevos tipos de vulnerabilidades.
- Herramientas integradas para respaldar el análisis y mejorar los resultados.
- Identifica los tipos de pruebas a realizar en función de los resultados de pruebas anteriores.
- Valida continuamente los resultados de los análisis, repite las pruebas, actualiza los informes y envía alarmas.