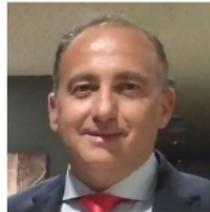


6 ESPECIAL CIBERSEGURIDAD PARA EMPRESAS

Los protagonistas



MANUEL FERNÁNDEZ
Director para España, Portugal y Latam de Advantio



DOUGLAS WAGNER
Responsable Técnico Área Ciberseguridad de ABAST



ANDREA-GIAIME BODEI
CEO de INFRA

Como no hay suficientes profesionales con experiencia en ciberseguridad en el mercado para que cada empresa tenga su propio equipo, "la tendencia es apoyarse en servicios gestionados como el MDR (*Managed Detection and Response*) para poder contar con expertos que ayuden a la empresa en esa importante tarea", explica **Manuel Fernández**.

EVOLUCIÓN DE LOS SISTEMAS DE CIBERSEGURIDAD

Los ciberataques afectan a todos los sectores de actividad y pueden llegar a cualquier tipo de organización, independientemente de su sector y tamaño. La ciberseguridad evoluciona de forma constante y, por ello, cabe esperar que, a corto y medio plazo, las partidas destinadas a la contratación de servicios y productos de ciberseguridad vaya aumentando de forma progresiva en los próximos años.



“Cuando las empresas no están bien preparadas, el impacto suele ser mayor y pueden aparecer graves consecuencias”

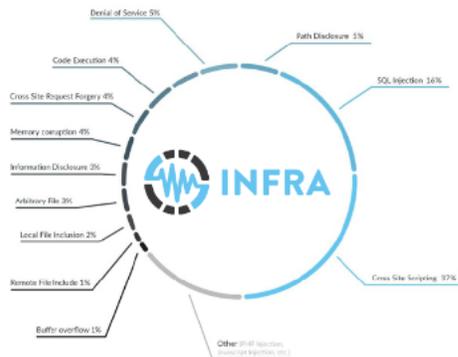
“La evolución de los sistemas de ciberseguridad sigue dos vectores. Por una parte, están las tendencias de cambio en la gestión de negocio de las empresas, donde muchas están externalizando las actividades no directamente asociadas con el negocio. En este sentido, la gestión de la ciberseguridad también está sujeta a la externalización de sus sistemas y recursos humanos, aunque sirven para la protección interna de los datos y procesos de la empresa usuaria. Por otra parte, la evolución de las amenazas va en paralelo a la evolución de las empresas. Cada mes hay nuevos retos de protección informática

a los cuales los responsables de la ciberseguridad tienen que adaptarse”, comenta **Douglas Wagner**. También añade que “hay medidas protectoras tecnológicas, procedimentales y organizativas para hacer frente a las amenazas correspondientes y a cada una de estas situaciones de nuevos tipos de amenazas y riesgos. Lo importante es estar encima de los ciberriesgos de forma continua”. La introducción en las empresas pequeñas de SOC y virtual SOC, para monitorizar 24 horas toda la infraestructura y hacer test periódicos de seguridad de manera preventiva será una de las

tendencias mayoritarias en el plazo, según **Andrea-Giaime Bodei**. “Lo que antes estaba reservado a las empresas más grandes los bancos será introducido en empresas con menor presupuesto económica”, explica.

Para **Mario Calle** las ciberseguidas son cada vez más sofisticadas ingeniosas y audaces: “En 2019 la pérdida media de una sola violación de datos fue de 4,1 millones de dólares. Sin embargo, con un marco SASE, las empresas pueden alcanzar un alto grado de protección. SASE, definió por primera vez por Gartner 2019, ahora es un marco más accesible. Busca ofrecer a las empresas una red WAN global confiable y robusta, así como protección de extremo a extremo a través de servicios avanzados de ciberseguridad en un único

INFRA, asesoramiento tecnológico y ciberseguridad



INTELLIGENCE FRAMEWORK PTE. LTD.

OFICINAS

Dirección postal:
101 Cecil Street
#14-12 Tong Eng Building
Singapore 069533
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.

Hybrid No Solutions blockchai



Entre los varios legados de pandemia, hay dos en particular que presentan el punto de partida de Numentech:

1. Pymes, autónomos, así como trabajadores en remoto nunca tan expuestos a los ciberataques como hoy.
2. Estas categorías de usuarios tradicionalmente poco consi-

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.

PRODUCTOS Y

- Desarrollo de solución para entornos *business*
- Desarrollo de solución documentos en *cloud*.
- *Managed services* para validación de soluciones