Un referente en el sector de la Ciberseguridad

Arturo Díaz

MNEMO es una empresa del ámbito de las Tecnologías de la Información, de capital español, que inició su actividad empresarial en el año 2001 en Madrid, desarrollando grandes proyectos de Nuevas Tecnologías y de Seguridad IT, fundamentalmente en empresas del sector Financiero (50%); Público (40%) e Infraestructuras Críticas (10%).

Una de las características principales de compañía es su fuerte proyección internacional, muestra de ello es que actualmente tiene oficinas permanentes en España, México y Colombia, con proyectos activos, además, en Ecuador, Panamá y Perú.

La vocación de MNEMO es la Ciberseguridad y la Tecnología, ambas estrechamente ligadas por el proceso imparable de globalización y el mundo digital, que caracteriza al universo en el que vivimos. Esto ha provocado un significativo esfuerzo inversor en I+D+i, lo que ha impulsado a MNEMO a construir una importante cartera de productos propios, que constituye, no sólo uno de sus mayores atractivos de valor añadido, sino también una de sus principales palancas de innovación y escalabilidad.

Su equipo profesional está formado por casi 700 personas, constituyendo un grupo muy sólido técnicamente y con muchos años de experiencia en el mercado que incorpora, desde su inicio, mucho talento para innovar.

¿Qué nos puede decir específicamente del Observatorio de Ciberseguridad y por su presencia simultánea en cinco ámbitos de gran relevancia?

Los servicios son el producto de nuestra metodología MNEMO Arkadia, desarrollada a medida para incluir todas las necesidades que puede tener una organización en materia de Ciberseguridad, de forma que se asocie a cada necesidad el área de actividad, funciones y servicios que se prestan desde el SOC-CERT para resolver aquella.

La visión de MNEMO que sirve de base a la Metodología MNEMO Arkadia, es un modelo de evolución de la seguridad con mejora continua, que es el enfoque que aconsejamos a nuestros clientes, y que se plasma en nuestra oferta de servicios integrales de Ciberseguridad.

La principal característica que provee la Seguridad Conectada es que cada uno de sus componentes, servicio o tecnología, está retroalimentando al resto y se beneficia de la comunicación multidireccional, actuando la arquitectura corporativa como un solo "organismo", independientemente de donde se produzca una alerta o incidente. Toda la arquitectura reaccionará con medidas preventivas y paliativas, al igual que un sistema inmunitario. Permite desplegar una malla de defensa integral y conectada.

¿En qué consiste la visión de la Ciberseguridad según MNEMO?

Durante los últimos años, MNEMO ha desarrollado un amplio portafolio

de servicios relacionados con la Ciberseguridad. Derivado de este esfuerzo, la compañía ha consolidado un conjunto de competencias claves que son la base de nuestra diferenciación.

Desde el punto de vista tecnológico y de conocimiento destacan: Capacidad para diseñar e implantar unidades SOC/CERT homologables según estándares internacionales del máximo nivel de exigencia (certificación FIRST de la Carnegie Mellon University).

MNEMO cuenta con un modelo propio de SOC/CERT basado en una arquitectura tecnológica diseñada en el área de I+D+i. Capacidad para elaborar Inteligencia Preventiva, basada en una Inteligencia de Amenazas y Gestión de Vulnerabilidades avanzadas en relación a las prácticas normales de mercado. Inteligencia de Amenazas más allá de la integración de listas negras procedentes de terceros o de generación propia: desarrollo de análisis de grafos para el descubrimiento de amenazas ocultas ("quién/qué está detrás de los ataques percibidos"). Gestión de Vulnerabilidades más allá de la mera notificación de los incidentes a los equipos de Sistemas para que ellos generen las reglas de protección: generación y diseminación automática de "defensas" relacionadas con las amenazas identificadas.

¿Qué perfiles tienen sus clientes?

MNEMO tiene presencia permanente en España, Colombia y México, a través de oficinas propias. Además, ha operado en más de 11 países diferentes, mediante oficinas de proyecto. Asimismo, dispone de distintos Centros de Operaciones de Seguridad SOC–CERT, certificados por prestigiosas organizaciones internacionales.

De forma muy global, el foco del negocio en estos mercados se centra en tres grandes ámbitos: Empresas del Sector Financiero; Sector Público, con especial mención en Gobierno Central (ministerios y/o secretarías), Instituciones Públicas; Industria, concretamente en infraestructuras críticas.

En todo caso, cada mercado presenta fuertes particularidades. Sin embargo, las necesidades en materia de Ciberseguridad tienden a ser cada vez más comunes, y se pueden poner en práctica medidas preventivas aprendidas en otros países, facilitando con ello una escalabilidad de las Tecnologías de Ciberseguridad

Tienen ustedes dos Centros de Operaciones de Seguridad (SOC), el primero de ellos en México desde 2013. ¿Qué nos puede decir del segundo SOC, en este caso implantado en Madrid y en qué consiste su actividad?

El nuevo SOC de MNEMO en España, consta de una superficie total de 200 m2 y se distribuye en una sala principal del centro de operaciones, con una capacidad total de 40 operadores y personal de gestión del centro de operaciones, una sala de laboratorio con capacidad para 7 técnicos, una sala de crisis debidamente acondicionada y una esclusa de acceso a esta zona protegida.

La sala del centro de operaciones, está dotada de un *videowall* para el control de operaciones con un total de 16 pantallas de control en una configuración con un área de visualización de más de 10m2 para el correcto control de las operaciones de seguridad en tiempo real. Aparte de los controles de acceso biométricos generales de acceso a la planta, toda la zona segura del SOC está controlada mediante una esclusa que da acceso a la zona con controles de acceso dobles mediante biometría facial.

Todos los sistemas están protegidos contra interrupciones eléctricas, mediante el uso de Sistemas de alimentación ininterrumpida locales adecuados, además de los medios de protección del propio edificio donde se ubican las instalaciones. Todas las instalaciones están protegidas contra incendios mediante sistemas de extinción de agua nebulizada de última generación. Tanto los accesos generales de la planta, como la sala de servidores que aloja los sistemas de información, poseen controles de acceso mediante biometría facial y registro en video digital. Los accesos al propio edificio cuentan con un sistema de control de accesos independiente y vigilancia 24 horas. Dentro de la zona de seguridad, se encuentran las instalaciones del CERT/Forense con 7 puestos de trabajo y dotada con los equipos especiales requeridos para esta actividad concreta.

Los servicios que se proveen y que han sido descritos anteriormente se prestan en modalidad Cloud, estando todas las soluciones desarrolladas modularmente bajo un principio de hiperconectividad basada en APIs, y virtualización para su despliegue.

¿Qué finalidad y alcance en el servicio tiene el Cyber Threat Intelligence (CTI)?

Cyber Threat Intelligence tiene como finalidad específica introducir una capa de inteligencia sobre las operaciones de ciberseguridad para adelantar los riesgos y amenazas. Así mismo, permite conocer las motivaciones y objetivos de los diferentes incidentes y amenazas globales, como de los clientes. Dentro de esta área, se encuentra el bloque de inteligencia, cuyo objetivo es satisfacer las necesidades puntuales de inteligencia y ciberinvestigaciones de los clientes de MNEMO, siendo un servicio bajo demanda.

Descríbanos qué es el Mnemo Labs.

Es el servicio desarrollado por MNEMO para dotar a nuestros laboratorios de las mejores tecnologías para la adquisición de evidencias a tiempo real, la búsqueda y análisis de *malware*, el análisis de tráfico y la realización de servicios de Análisis Forense Digital.

Los laboratorios proporcionan el análisis de las posibles amenazas a las que pueda estar expuesta una organización en términos de Tráfico y Malware. También, tiene la capacidad de identificar Amenazas Persistentes Avanzadas (APT).

¿Qué objetivo tiene su servicio Análisis de Vulnerabilidades Evolutivo?

Comprende cinco servicios: El servicio de Análisis de seguridad de activos externos se encarga de realizar, de manera continua, un escaneo de las vulnerabilidades que puedan afectar a los activos externos de la organización, notificando todas aquellas vulnerabilidades que sean detectadas.

El servicio Auditoría Continua de Seguridad Interna se encarga de la auditoría de seguridad de forma periódica contra la infraestructura y activos internos identificados por el cliente.

Mediante el servicio de Bastionado y Hardening Intelligence SOC, se articulará el conocimiento generado a través de los analistas de seguridad y de inteligencia para la reducción de riesgos relacionados con la seguridad IT y prevención en la exposición ante amenazas y ataques de cada uno de los sistemas que se encuentren en la infraestructura tecnológica.

El Red Team modela y desarrolla ejercicios de ciberseguridad que tienen como meta la simulación de escenarios

de robo de información y otros activos susceptibles de comercialización no autorizada por parte de adversarios, competidores y delincuentes.

El servicio de Auditoría del código permite ofrecer una visión de los riesgos de seguridad a que se enfrentan las aplicaciones, mediante su auditoría de seguridad, tomando como referencia las diferentes calificaciones estándar del mercado para determinar la criticidad de las vulnerabilidades encontradas y así poderse generar un informe de conformidad con los estándares OWASP, CWE, MISRA, NIST, PCI y CERT.

¿Cuáles son los retos a medio plazo de la compañía, una de las más reputadas y punteras del sector de la ciberseguridad?

El esfuerzo para afrontar estos grandes desafíos deberá hacerse desde la realidad actual del negocio de MNEMO, que la podemos resumir en los puntos siguientes: Portafolio de servicios orientado a un mercado claramente en expansión durante los próximos años: "Servicios de Ciberseguridad", que crecerá globalmente por encima del 8% anual. Grandes productividades latentes derivadas del desarrollo ya hecho de servicios e infraestructuras que admiten una gran escalabilidad respecto del volumen de negocio actual (SOC/CERT, NERV, Laboratorios y Ciberinvestigaciones, principalmente). Estructura orgánica muy orientada a la realidad de los mercados, con un escaso desarrollo de lo Corporativo.

En todo caso, dado que el objetivo clave es lograr un fuerte incremento de las ventas de los servicios recurrentes de alta escalabilidad, la expansión geográfica en Latinoamérica ("mercado natural de MNEMO") es la iniciativa estratégica de mayor relevancia, desde el punto de vista de la cuenta de resultados en los próximos años, ya que es en esta geografía donde se tienen identificadas más oportunidades de venta de dichos servicios y gran parte de las acciones que implica.

¿Quién es Raúl Sánchez? Háblenos de su trayectoria profesional y por qué y cuándo aceptó su actual cargo.

Me incorporé a MNEMO en el año 2005. Soy un apasionado por el mundo de la tecnología con un fuerte compromiso por los negocios, desarrollando mi faceta comercial dentro de la compañía. Después de esta etapa ocupé el puesto de director de Alianzas y Cuentas Estratégicas y durante este periodo conseguí que empresas líderes en el sector financiero confiaran en MNEMO como proveedor de servicios de ciberseguridad. En el año 2016 fui nombrado CEO de la compañía.

Que MNEMO siga siendo un referente en el sector de la ciberseguridad, es una de mis competencias como CEO, donde uno de mis principales retos es aportar valor y confianza con una relación cercana al negocio de nuestros clientes, en un ámbito tan delicado como es la ciberseguridad ■