

TRC Innovación y excelencia en el próximo Madrid Tech Show

La tecnología de TRC se abre paso una vez más liderando el sector y presentará sus novedades en el Madrid Tech Show

Un año más, TRC acude a Madrid Tech Show para reunirse con clientes y fabricantes de la industria tecnológica. Esta cita, considerada como uno de los epicentros nacionales de ciberseguridad, es un espacio donde presentar las tendencias y soluciones más destacadas de 2023 ante profesionales estratégicos del sector tecnológico español y europeo. Un escaparate donde descubrir avances en ciberseguridad, Inteligencia Artificial, Big Data o Conectividad.

TRC es una empresa madrileña, fundada en 1989, con sedes en todo el territorio nacional. Hoy sigue avanzando en su proceso de expansión, crecimiento y profesionalización, un proceso que se inició en el año 2020 con el objetivo de garantizar la continuidad de la actividad y la rentabilidad necesaria para continuar siendo un referente del sector. Como resultado de esta transformación, la compañía incrementa año a año sus resultados superando ampliamente los dos dígitos, con un incremento de más de 50 clientes nuevos en cartera.

Dentro de este cambio, se han incorporado perfiles de reconocida experiencia y solvencia para la gestión del día a día de la empresa. Uno de estos perfiles fue Emi-

lio Rico, actual Security Advisor de TRC, que apunta que a la cabeza de la lista de peligros de ciberseguridad se encuentran el malware, el ransomware, el phishing, el robo de credenciales y las fugas de información: “Especialmente el ransomware, que está siendo la lacra de esta época, y que deja más expuestos a los que tienen debilidades como fallas en el control de accesos, escasa seguridad de las contraseñas, vulnerabilidades del hardware y el software y falta de formación”.

De hecho, hay estudios que indican que entre el 50% y el 60% de las empresas que reciben un ataque de este tipo son incapaces de continuar con el negocio y se ven obligadas a cerrar. “En los últimos años hemos visto que este tipo de ataque se manifiesta más agresivo y más letal. Implica un efecto económico (pagar por el rescate o asumir las consecuencias); una extorsión a cambio de que no se publiquen los datos sensibles robados, algo que obviamente acarrea enormes pérdidas de reputación; y el chantaje a los clientes cuyos datos han sido robados y expuestos”, amplía Rico. Y añade que los factores principales que condicionan la exposición al riesgo de las empresas son, en primer lugar, “el factor humano, ya que se calcula que los errores

humanos causan el 95% de las vulneraciones de seguridad. Normalmente son acciones accidentales, generadas por falta de formación, pero que permiten que se produzca una brecha o se abra un vector de entrada para un posterior ataque. Después están los cambios y la evolución tecnológica constante, que exige a las empresas soportar un ritmo difícil de seguir. Los responsables de TI y de ciberseguridad de esas empresas deben estar permanentemente capacitados y tienen que ser expertos conocedores de las tecnologías que usan a diario y que cambian conti-

El Tabletop Exercise que Emilio Rico desarrollará en el Madrid Tech Show, es un ejercicio de simulación en un escenario virtual, donde se plantearán diferentes situaciones e incidentes a los que hacer frente en la resolución de una ciber crisis

nuamente, lo que hace muy difícil estar al día y no cometer errores. Y, por último, el teletrabajo y los dispositivos móviles son factores de riesgo: las empresas proporcionan portátiles, tablets y teléfonos inteligentes (smartphones) a su personal para que los empleados puedan trabajar en remoto desde cualquier sitio y en cualquier momento. Esa facilidad proporciona indudables ventajas empresariales, pero, al mismo tiempo, dificulta la protección de la información que alojan, convirtiéndose en un dolor de cabeza para los responsables de la ciberseguridad”.

Y es precisamente sobre este punto en el que se basará el Tabletop Exercise (TTX), un ejercicio de simulación, que Emilio Rico desarrollará en el Madrid Tech Show, donde planteará diferentes situaciones que pueden suceder durante un ciber incidente, en un escenario virtual para hacer frente a una ciber crisis y aprender cuáles son las mejores respuestas que pueden llevar a cabo los diferentes roles directivos en los escenarios planteados. Un ejercicio que hará identificar en profundidad los puntos de mayor vulnerabilidad de las empresas sobre los que trabajar a la hora de proteger una organización, destacando la importancia de las infraestructuras tecnológicas en nuestras vidas y la ciberseguridad como pilar fundamental. “Después de que la nueva NIS2 obligue a los comités de dirección a asumir su responsabilidad ante un ataque cibernético, para TRC, enseñar a medir a las empresas su capacidad de resolución de los problemas ante incidentes críticos es una parte estratégica propuesta dentro en nuestra cartera de servicios”, asegura Rico.

Sobre TRC

La compañía, con un enfoque integral orientado siempre al cliente, destaca por su capacidad para crear asociaciones estratégicas y alianzas con fabricantes nacionales e internacionales que impulsan la innovación tecnológica, convirtiéndose en un referente en el desarrollo y la implementación de soluciones. El 50% de la plantilla está formada por técnicos expertos y cualificados que garantizan a sus clientes que pueden diseñar y ofrecer soluciones de alto valor añadido.

TRC sigue de cerca el mercado para anticiparse a las tendencias, e incorpora continuamente los fabricantes más innovadores del mercado para dar respuesta a todas las necesidades de este entorno tan cambiante.

Desde TRC, se alinean con sus clientes con un pensamiento transformador y empleando las herramientas digitales coordinadas por su equipo de expertos con el fin de garantizar el éxito de los proyectos de transformación digital.

La participación de la compañía en los eventos más destacados del sector hace que sobresalga y enfatice su compromiso con la innovación y su papel en la construcción de un futuro tecnológico más seguro.



Emilio Rico, Security Advisor de TRC