HACKNOID:

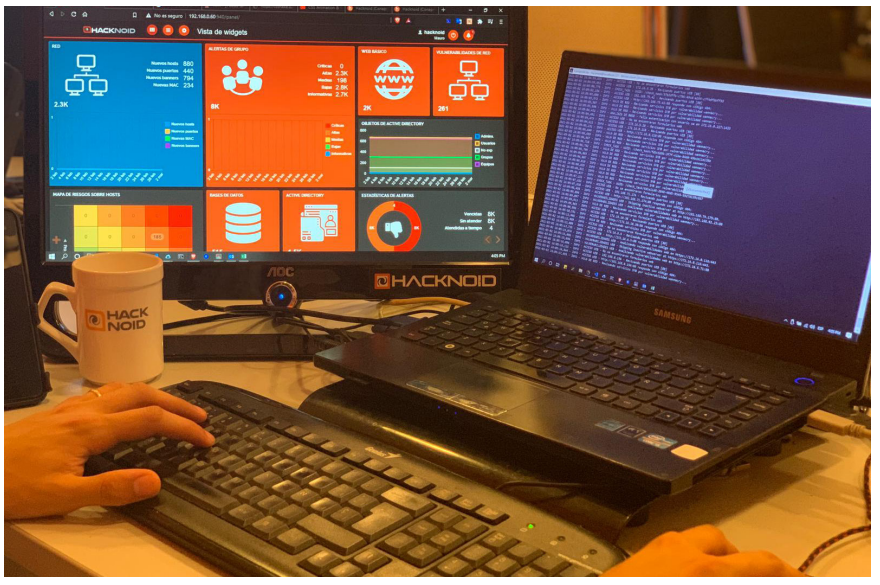
Plataforma integrada a la gestión del negocio que brinda soluciones preventivas ante ciberataques

Una propuesta para la detección temprana de vulnerabilidades en los sistemas digitales, que permita a las compañías contemplar la ciberseguridad desde el inicio y en todo el ciclo de los procesos de negocio, para evitar sus potenciales consecuencias, es lo que ofrece esta empresa con su plataforma integral.

Actualmente, un ataque a los sistemas digitales de una compañía podría significar graves pérdidas económicas y de reputación de marca, que resultan, muchas veces, difíciles de revertir. Hoy en día los procesos administrativos y operativos en empresas y organizaciones están siendo soportados, principalmente, por sistemas digitales que dan la continuidad al negocio; lo vemos por ejemplo en las transacciones de compra del retail, en la nómina de remuneraciones de recursos humanos, en el control automático de una línea de producción o el seguimiento de despachos logísticos, donde el costo de actuar tardíamente ante un ataque informático siempre es mayor al de trabajarlo de forma preventiva.

"La ciberseguridad pasó de ser un 'nice to have' a un 'must have', en cualquier organización que quiera permanecer competitiva en un mundo digitalizado, llegando a ser un elemento estructural del negocio que debe ser gestionado a nivel estratégico, táctico y operativo, con responsabilidad directa al más alto nivel de la empresa. Así, este cambio de paradigma en la manera de llevar adelante una compañía, entendiendo los riesgos cibernéticos y vulnerabilidades existentes a los que se está expuesto en cada proceso, permite alinear los esfuerzos para la continuidad operacional y expansión de nuevos proyectos, minimizando la probabilidad que ocurran siniestros por causas externas", señala Rosina Ordoqui, CEO de Hacknoid.

Con la pandemia y el vuelco a la digitalización, los directivos de las empresas necesitan tomar conciencia sobre los riesgos de no contar con buenas plataformas de prevención de ataques. "Contar con un sistema automático que navegue por todas las componentes, visibilizando las vulnerabilidades existentes, y en consecuencia, permita reducir el tiempo de exposición a ataques, hace que la probabilidad que un ciberdelincuente pueda explotar una vulnerabilidad, como denegación de servicios o encriptación de datos, por ejemplo, disminuya considerablemente, ayudando a la continuidad operacional de los procesos y el negocio", sostiene la CEO de Hacknoid, y agrega: "Cuando hablamos de continuidad de negocio, implícitamente en Hacknoid buscamos brindar la garantía de que nada va a fallar al menos en los procesos críticos y los cumplimientos regulatorios que nos permiten seguir generando ingresos. Es por esto que también la gestión de la ciberseguridad debe abordarse como un proceso de mejora continua con accountability a nivel directivo, siendo parte de la gestión de riesgos y cumplimiento de una compañía".



Hacknoid ofrece una plataforma que apoya la gestión de seguridad de la información de una forma muy simple: dar una visibilidad continua de ciberseguridad a los encargados de los procesos, de las tecnologías y de los negocios, en un lenguaje entendible por cualquiera de ellos, con el objetivo de que se tomen las acciones correspondientes de acuerdo a ese mapa general. Rosina Ordoqui concluye: "De esta forma, el apoyo principal es el de automatizar todo lo posible en cuanto a la detección de vulnerabilidades, para liberar del peso de ese trabajo al factor humano, que usualmente está ocupado en otras tareas, y poder concentrar su capacidad en la resolución de los problemas, que Hacknoid le muestra en orden de criticidad".

Descubrir, alertar y remediar vulnerabilidades

En el área de tecnologías de la información, aún existen varios procesos manuales que son llevados de una forma poco eficiente por las organizaciones. Frente a este escenario es que existe la solución del software Uruguayo-Chileno "Hacknoid", plataforma que automatizó el proceso de Ethical Hacking, consistente en: descubrir, alertar y mostrar una planificación de remediación de vulnerabilidades de los sistemas escaneados en función de su criticidad y probabilidad de ataque. Luego, una persona experta toma el resultado que automáticamente va entregando la plataforma y puede realizar las actividades específicas y técnicamente más complejas para establecer los controles correspondientes.