Revista GERENCIA
Noticias, análisis e información

02/11/2020

¿Qué sectores hoy son el principal blanco de los ataques a la seguridad y cómo enfrentar estas amenazas?

Rosina Ordoqui, CEO de Hacknoid.

Existe una tendencia a pensar que algún sector podría estar a salvo en lo que se refiere a los ciberataques, sin embargo, las estadísticas y evidencias muestran que aun aquellas empresas de tamaño mediano que suelen pensar "nosotros no tenemos atractivo alguno para ser un objetivo", pueden llegar a serlo por varias razones. Así lo destaca Rosina Ordoqui, CEO de Hacknoid, empresa especialista en ciberseguridad.

"El mundo de los ciberdelincuentes no se limita a niños probando herramientas al azar, sino que es básicamente un negocio en sí mismo, y solo al estar expuestos a Internet en algún sentido, en un primer 'barrido' que se realice para ver qué empresas, organizaciones o cualquier tipo de negocio se encuentra vulnerable, ya resulta atractivo sumarse a este negocio, aunque se trate de monedas que irán a engordar una alcancía mayor. Por tanto, quienes están más descuidados, serán objetivos más apetecibles para aquellos ciberatacantes que están buscando volumen y no saña contra una organización o tipo de organización en particular", explica la ejecutiva.

Más allá de esta realidad, las tendencias a nivel global, llevan a enfocar la atención a aquellos escenarios que, por coyuntura o por valor, tienen mayor probabilidad a ser exitosamente explotados. "En estos casos, hoy por ejemplo, encontramos en particular el mundo de la salud y el de gobierno. Debido al Coronavirus y, por ende, las dificultades económicas que afrontan los gobiernos, las instituciones de estos sectores están siendo objetivo por el foco de la población en general en esta temática, que hace más engañar y hacer que alguien caiga", detalla la profesional.

"Por el lado de los consumidores, es más sencillo que alguien caiga ante un engaño que provenga de estas instituciones y, por el lado de un ataque directo, en este tipo de organizaciones se puede filtrar más fácilmente cuando las mismas están con el foco y energía localizado en atender emergencias y urgencias con prioridades altas, de forma constante", explica Rosina Ordoqui.

Más allá de todo lo expuesto, casi ninguna industria ha dejado de tener algún tipo de ataque en este último año, con diversos modelos de ataque y jugando en diferentes momentos de distracción de los involucrados. "El cibercrimen no es una mera diversión, sino un negocio que maneja millones de millones en el mundo cibernético y la 'dark web', un submundo incógnito, que maneja sus propias reglas del estilo mafia, dentro del cibermundo", añade la ejecutiva.

¿Qué tipo de ataques son más comunes?

Actualmente se encuentran en primer plano los ransomware: programas que "secuestran" la información de la víctima hasta que esta se disponga a un pago por su rescate. Este "secuestro" se da a través de la encriptación de sus datos, por tanto, la víctima debe pagar un rescate para obtener el código que logrará desencriptar sus datos. Por ende, recién cuando lo obtenga podrá continuar la operación del negocio, debido a que este tipo de ataques, logra inmovilizar la tecnología de la organización o gran parte de esta en pocos segundos o minutos.

“En este sentido, correr contra el tiempo es un desafío de la ciberseguridad que día a día se hace más imperante en las empresas, debido a que los ciberatacantes cuentan con tiempo suficiente y se perfeccionan cada día más y, por el lado de las organizaciones, cada día se necesitan más recursos (herramientas y especialistas) para lograr cerrar todas las ‘puertas’ de forma rápida y eficiente”, enfatiza la CEO de Hacknoid.

Cabe aclarar que son puertas que no se cierran una vez y queda todo listo y en orden. La dinámica de las tecnologías, los cambios en las organizaciones, las puestas en producción, e incluso de los errores humanos, cuando se instala o configura cualquier dispositivo/sistema/aplicativo, pueden abrir nuevas puertas de vulnerabilidad que debemos estar aptos para detectar de forma temprana, para exponernos el menor tiempo posible.

“Hacknoid provee una parte importante de la ecuación automatización-recursos humanos que es necesaria para una gestión práctica y ágil en los tiempos que corren, permitiendo apoyar a las empresas en este reto”, explica la profesional.

“Dejar todo en mano de profesionales es muy costoso y poco eficiente en términos de prioridades operativas para estar realizando tareas que requieren periodicidad marcada y recurrencia”, advierte Rosina Ordoqui. “Allí pueden entrar las herramientas y/o plataformas que provean de un apoyo técnico eficaz y de menor costo, para enfocar a los especialistas en el trabajo que realmente requiere de la intervención humana, dejando a Hacknoid actuar de forma automática, proveyendo de data procesada y útil hacia los tomadores de decisión con foco en el negocio, que es en definitiva lo importante”, agrega.

“En este contexto, Hacknoid aporta desde la escala de directivos y auditores en su propio lenguaje, hasta para los técnicos en su propia jerga también, completando un círculo virtuoso de entrega de información hacia una gestión de vulnerabilidades de excelencia”, concluye la profesional.

Indice de Noticias

Contáctenos

Dirección: Sucre 2235, Ñuñoa, Chile
Teléfono: (562) 2433 5500
Email: info@emb.cl

Visite también: