LITORALPRESS

Fecha: 31-12-2024
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: “Entregamos protección en ciberseguridad en términos absolutos, no relativos”

Pág. : 28
Cm2: 467,4

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

Héctor Lazo, Gerente General de Eknow

“Entregamos protección en ciberseguridad en términos absolutos, no relativos”

Eknow se distingue por su compromiso con la investigación y el desarrollo tecnológico, de tal forma que todos sus servicios tienen el sello del conocimiento avanzado. Desde los servicios de auditoría de red a las soluciones en Seguridad de la Información, la empresa ha sido reconocida en el mercado como líder del sector. En entrevista con Héctor Lazo, CEO y fundador, conversamos sobre cómo la ciberseguridad debe evolucionar hacia la gestión de riesgos y el cumplimiento normativo.

El conocimiento avanzado y su foco en investigación, ¿han sido rasgos de Eknow desde sus orígenes?

De alguna manera sí. Comenzamos hace 19 años, en 2005, con una visión muy audaz, que fue invertir nuestros recursos en investigación y desarrollo, más que vender equipos y tecnología. Digo audaz porque hace veinte años la mayoría de las empresas en tecnología tenían como norte la comercialización de productos para lograr crecimiento en volumen de ventas, mientras que nosotros fuimos fieles a nuestra filosofía de desarrollar la mayor cantidad de conocimiento posible y un alto nivel de especialización. Hoy, muchas de esas empresas tienen un excelente posicionamiento en el mercado, pero desde el punto de vista técnico-académico no equiparan nuestra gestión. En cuanto a conocimiento metodológico-técnico, nosotros llevamos la delantera.

¿Reconoce el mercado este sello de la empresa?

Absolutamente. Siempre hemos evolucionado a partir de paradigmas basados en la metodología. A lo largo de los años nos hemos vinculado con el mundo de las universidades de distintas maneras, y de hecho la primera comercialización de plataformas de e-learning la hicimos en la Universidad de Concepción en el año 2007 para clientes como LAN Chile y SQM, Además, dicha especialización hoy en día la estamos proyectando en dictar un diplomado para la formación de auditores líderes en ciberseguridad.

¿Cómo comienza Eknow a entrar en el mundo de la ciberseguridad?

Luego de consolidarnos como expertos en capacitación para la gestión tecnológica, nos iniciamos en el proceso de auditoría en redes y plataformas TI. Entendimos muy temprano que se debía analizar y comprender siem-

LITORALPRESS

Fecha: 31-12-2024
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: "Entregamos protección en ciberseguridad en términos absolutos, no relativos"

Pág. : 29
Cm2: 431,8

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

pre cuál era el rendimiento y la configuración óptima para cada cliente, logrando dominar aspectos como latencia, cadencia, la lógica de los micro-cortes de red o el jitter de la comunicación en internet. Comenzar a desarrollar el servicio de auditoría nos otorgó la madurez para entender y tomar decisiones adecuadas desde el punto de vista de la transformación y optimización tecnológica que las empresas necesitaban y nos encaminaron a los grandes temas que hoy son el eje central para todos nuestros clientes: la continuidad operativa y la ciberseguridad.

"Comenzar a desarrollar el servicio de auditoría nos otorgó la madurez para entender y tomar decisiones adecuadas desde el punto de vista de la transformación y optimización tecnológica que las empresas necesitaban y nos encaminaron a los grandes temas que hoy son el eje central para todos nuestros clientes: la continuidad operativa y la ciberseguridad"

Es decir, sin ciberseguridad no hay continuidad operativa...

La continuidad operativa converge con la ciberseguridad. En Eknow trabajamos con un framework de buenas prácticas a nivel de continuidad operativa, el cual constituye la base estructural de la ciberseguridad. A través de nuestra experiencia, hemos comprendido la lógica de los criterios operacionales, la gestión de recursos de red, los conceptos de arquitectura y la definición de topologías. Esto nos ha permitido entender cómo debe funcionar una red para garantizar un servicio óptimo a los usuarios. "Las redes tienen un objetivo: ser un servicio esencial para las plataformas tecnológicas, preservando la integridad de los datos y la eficiencia de las comunicaciones".

En la actualidad, nuestro enfoque en auditoría, continuidad operativa y ciberseguridad nos posiciona como una de las empresas más especializadas de Chile. Además, hemos evolucionado hacia un rol académico, formando ingenieros que han desarrollado su carrera profesional dentro de nuestra compañía. De este modo, Eknow no solo lidera en tecnología, sino que también impulsa la formación académica y profesional del sector.

En una década, ¿ha crecido el nivel de conciencia de las empresas respecto a la importancia de la ciberseguridad?

Hay más conciencia, claro que sí, pero falta muchísimo, ya que no existe una comprensión de lo que es la ciberseguridad a cabalidad. Cuando una empresa no tiene los recursos, percibe la ciberseguridad como un gasto, sin entender que es una inversión y que una brecha puede provocar multas, pérdidas económicas, de reputación o el robo de información. Es eso lo que falta, entender la ciberseguridad como una inversión y garantizar la Seguridad de la Información.

A su juicio, ¿por qué falla la seguridad en Chile?

Hay tres factores fundamentales. El primer punto es que las inversiones no se enfocan en una disciplina integral denominada Seguridad de la Información, dado que los recursos, en la mayoría de las empresas, se concentran únicamente en aspectos tecnológicos. El segundo punto implica que las empresas y sus responsables no tienen una visión clara y orquestada de cómo priorizar adecuadamente las inversiones. El aspecto clave aquí son los criterios de decisión, ya que la inversión en ciberseguridad debería basarse predominantemente en el riesgo, algo que no se aplica de forma consistente. El tercer punto, y el más importante, es entender que la inversión tecnológica asociada a la ciberseguridad debe estar guiada por las labores vinculadas a la Seguridad de la Información, como el Compliance y la Gestión del Riesgo. En conclusión, antes de invertir, siempre se debe exigir un análisis de riesgo bajo un marco referencial de las probabilidades reales y el impacto de las amenazas, aplicando exclusivamente sobre los activos propios de la compañía.

Pero las empresas sí están invirtiendo...

Claro, pero muchas veces bajo criterios espurios; el mero hecho de hacer una inversión correcta no garantiza un buen resultado pues se podría carecer de criterios operativos. Por ejemplo, un problema muy usual es que en determinados casos se elige una determinada tecnología, pero no los protocolos adecuados. Por ejemplo, muchas de las empresas que han sido atacadas por malwares cuentan con un buen antivirus, pero no lo tienen actualizado.

Entonces, ¿cuál es el camino que deben seguir las empresas en materia de ciberseguridad?

Por eso, al momento de planificar la inversión en ciberseguridad, es fundamental solicitar una evaluación del estado actual de la compañía y sus activos, definir criterios claros para el análisis de riesgos, considerando la probabilidad e impacto de las amenazas sobre los activos propios de la compañía y las vulnerabilidades detectadas. A partir de esto, se deben establecer planes de mitigación y priorizar las inversiones, siguiendo este camino se puede fortalecer la plataforma tecnológica de ciberseguridad. Esta es la secuencia correcta, pero en la mayoría de los casos no se aplica así.

Es necesario comprender que la ciberseguridad es un componente tecnológico que debe ser la última etapa con la asignación

LITORALPRESS

Fecha: 31-12-2024
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: "Entregamos protección en ciberseguridad en términos absolutos, no relativos"

Pág. : 30
Cm2: 427,2

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

"Buscamos liderar en tecnología, pero también impulsar la formación académica y profesional del sector"

de recursos y luego la adquisición de tecnologías específicas. Lo primero siempre debe ser un diagnóstico basado en la gestión de riesgos sobre los activos, para determinar qué hacer y cómo. En resumen, el riesgo define la prioridad y la prioridad define la adquisición.

Como empresa, ¿de qué manera están abordando este desafío?

Estamos trabajando con universidades en la formación de ingenieros en ciberseguridad y en las metodologías que definan objetivamente la gestión del riesgo. De esta manera, proponemos el levantamiento de los activos críticos, proyectamos las amenazas sobre dichos activos, y desarrollamos la matriz de riesgo en base a la probabilidad e impacto relativo a la afectación que tiene sobre la compañía. Debe haber una metodología detrás de las decisiones; sino es así, la ciberseguridad no sirve de nada.

¿Por qué la metodología particular de Eknow puede garantizar una ciberseguridad completa?

En Eknow, a través de un servicio de GAP Analysis y aplicando correctamente las tecnologías, podemos garantizar en un 100% la postura de ciberseguridad entre los usuarios de las redes que administramos. Nosotros no hablamos de protección en términos relativos, lo hacemos en términos absolutos: llevamos 5 años sin incidentes que hayan elevado a una crisis de ciberseguridad entre nuestros clientes. Y si nosotros podemos, todos pueden. Las tecnologías que proveen de niveles altos de ciberseguridad están disponibles hace más de 20 años y si no se han implementado es porque se desconocen o porque se consideran muy complejas; una tecnología de referencia es la norma 802.1x.

Por ejemplo, que los usuarios se conecten a la red y automáticamente los sistemas de red le asignen una IP sin una validación o perfilamiento, ¡esto no es correcto!; que los usuarios puedan conectarse a una red local sin tener su antivirus actualizado, ¡tampoco!; también el permitir que en un servicio de Ethical Hacking, se pueda realizar un escaneo de puertos y la pregunta es: ¿por qué un administrador de red permite dicha acción? ¿Por qué en la primera instancia no se bloquea la IP del atacante inmediatamente?; o por ejemplo un usuario ya autenticado con el factor de doble autenticación (MFA) cuando dicho usuario realiza un movimiento lateral ¿Quién o qué sistema dentro de la compañía, lo aísla o lo desconecta, si trata de realizar una acción no autorizada? Todos estos son ejemplos de potenciales brechas de seguridad, que se pueden cerrar con la tecnología adecuada, pero para hacerla realidad en una compañía, lo que falta es aplicar los controles adecuados, definir las políticas y establecer los criterios de inversión.

Así como Eknow puede garantizarlo, ¿existen marcas que desde su lado también puedan hacerlo?

Por supuesto. Tecnológicamente, el futuro se define así: NAC para proteger dentro de la LAN, SASE para proteger tecnologías en la nube y SIEM para la gestión de incidentes. En casos específicos, hemos incorporado DLP (Data Loss Prevention). Trabajamos estrechamente con fabricantes de los cuales somos partners autorizados y certificados, como Fortinet, Cisco y Kaspersky; además de Safetica, el cual es un aliado estratégico en el mercado actual. Junto a Safetica, hemos establecido un centro de experiencia en DLP, diseñado para atender a clientes finales, ofreciendo un servicio de ciberseguridad en el marco de la reciente aprobación de la Ley de Protección de Datos en nuestro país.

A nivel de mayoristas, ¿cómo es la relación de Eknow con ellos?

En lo particular, nosotros tenemos una fuerte cercanía con Tecnoglobal, que es el mayorista que nos apoyó desde el inicio. Hoy trabajamos juntos en cada gran proyecto, con excelentes resultados.

¿Qué tendencias en ciberseguridad podemos esperar para 2025?

La tendencia clave será replantear la ciberseguridad como un enfoque integral orientado a la Seguridad de la Información, centrado en el cumplimiento normativo, la gestión de riesgos, la adopción de estrategias holísticas como Zero Trust y la automatización de la ciberseguridad. /ChN