

Los Riesgos Cibernéticos que han tomado a las empresas por sorpresa: La cadena de Suministro

¿Recuerdas cuando en septiembre del año pasado varias páginas web de entidades gubernamentales en Colombia empezaron a fallar?

Resultó que una empresa proveedora de servicios de IT había sido hackeada con un ransomware, afectando a decenas de organizaciones estatales (incluyendo al Ministerio de Salud y Protección Social y al Consejo Superior de la Judicatura) y a más de 700 empresas en varios países de Latinoamérica.

Pero eso no fue todo. Tan solo unos meses después, una importante empresa de Telco en Centroamérica también sufrió un ciberataque similar, impactando las operaciones móviles de miles de usuarios en Nicaragua, Costa Rica, Guatemala, Honduras y El Salvador. ¿La lección? Los riesgos cibernéticos pueden propagarse como

un virus a través de tus proveedores y cadenas de suministro.



El Eslabón Más Débil

Veámoslo así: una cadena de suministro implica todos los procesos y organizaciones involucradas en crear y entregar un producto o servicio, desde los materiales hasta el consumidor final. Y para los hackers, infiltrarse a través de un proveedor es mucho más fácil que intentar acceder directamente a su objetivo.

Esos incidentes demostraron que, al atacar a un solo proveedor, se puede impactar a un montón de empresas en todo el continente. El riesgo empieza desde que estableces relaciones con tus proveedores y los conviertes en parte de tu red empresarial. Las consecuencias financieras y de reputación pueden ser catastróficas.



El Respaldo que No Sirve de Nada

Aunque la empresa proveedora tenía sistemas de respaldo (*backup*), cometió el grave error de tenerlos en el mismo ambiente tecnológico donde ocurrió el ataque. Así que no pudieron recuperar nada después del incidente.

En ambos casos (Colombia y Centroamérica) se evidenció que atacando a un proveedor se puede afectar a un número considerable de actores en toda la cadena, lo que pone en relieve que el riesgo comienza desde que se establece una relación con los proveedores y se les convierte en parte de la red de las empresas contratantes.

La lección: no confíes ciegamente en los backups de tus proveedores, busca alternativas para blindarte aún más.

En la experiencia de WTW manejando reclamos asociados a ciberataques, los terceros (a menudo proveedores que almacenan datos de clientes o empleados) son responsables del 30% de las pérdidas por violación de datos de un total de 2,350 notificaciones en 65 países.



El Mercado de Seguros Reacciona

Estos ataques a cadenas de suministro históricamente han sacudido la industria de seguros cibernéticos. Después de un ataque masivo en 2020, las aseguradoras empezaron a excluir coberturas para este riesgo específico y a pedir más información detallada sobre el acceso que tienen los proveedores a los sistemas de las empresas aseguradas.

Es muy posible que después de los incidentes de Colombia y Centroamérica, los requisitos se endurezcan aún más en Latinoamérica.

Así que, si quieres contratar un seguro de este tipo, prepárate para que revisen con lupa tus medidas de ciberseguridad en las cadenas de suministro.



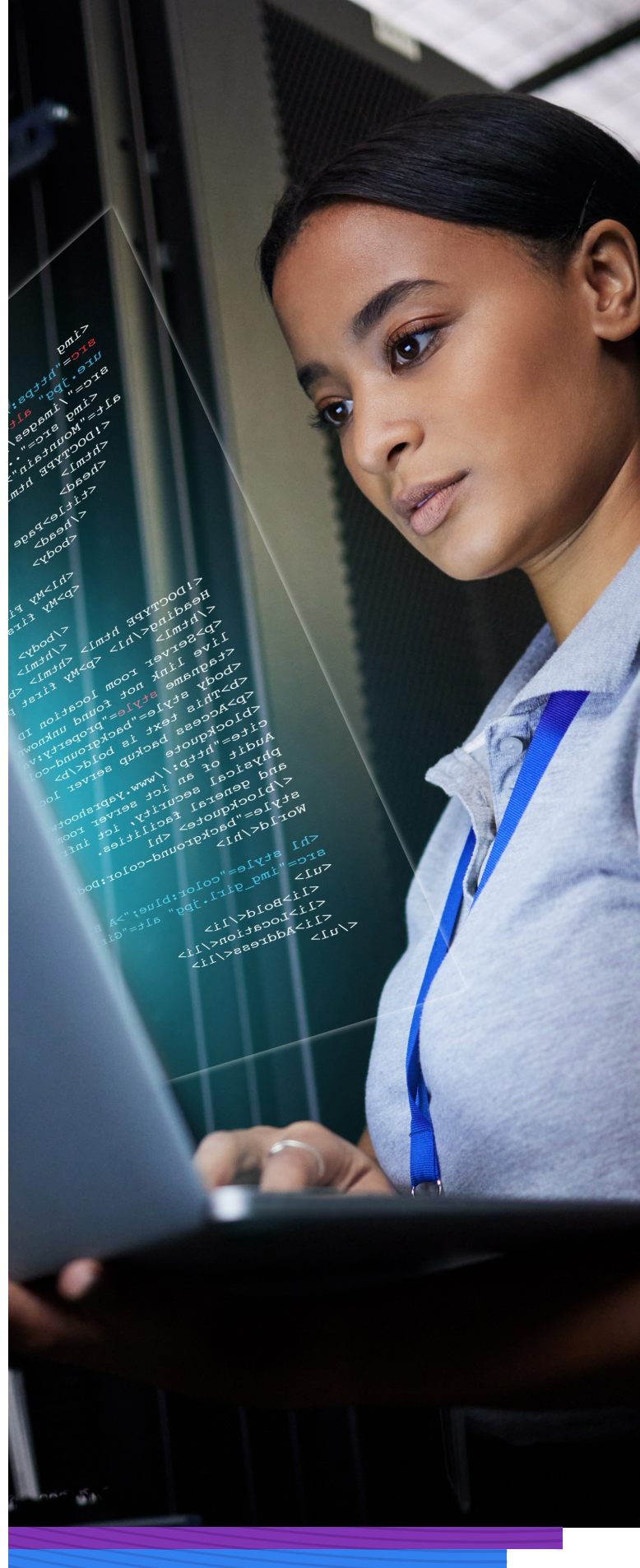


Recomendaciones Clave para no ser el próximo:

Desde WTW y con el fin de dar apoyo a nuestros clientes, te presentamos una lista de las principales recomendaciones que nuestros expertos en ciberseguridad sugieren ha puesto sobre la mesa:

- Evalúa a fondo la seguridad y capacidades de tus proveedores.
- Firma contratos sólidos que definan sus responsabilidades.
- Clasifica y cifra tus datos según su sensibilidad antes de compartirlos.
- Establece controles de acceso estrictos.
- Audita y supervisa periódicamente a tus proveedores.
- Implementa un plan robusto de backups y recuperación de datos. No dependas solo del proveedor.
- Capacita a todos tus empleados en concientización de seguridad. ¡Es clave!
- Revisa continuamente tus estrategias ante la evolución constante de las amenazas cibernéticas.

En resumen, la ciberseguridad (particularmente de la cadena de suministro) es un tema que no puede esperar. Hay que estar siempre un paso adelante de los ciberdelincuentes, revisando riesgos y actualizando medidas de mitigación, si no quieres ser el próximo titular por un ataque a tu proveedor.



Contactos:

Marcela Visbal

Finex Product Development Leader LatAm

M: + (57) 311 804 4188

marcela.visbal@wtwco.com

Rodrigo Flores

Regional Cyber Manager LatAm

M: + (52) 55 4383 8517

rodrigo.flores@wtwco.com

Acerca de WTW

En WTW (NASDAQ: WTW), proporcionamos soluciones analíticas basadas en datos en las áreas de personas, riesgo y capital. Potenciando la visión global y la experiencia local de nuestros profesionales presentes en más de 140 países y mercados, te ayudamos a perfilar tu estrategia, a mejorar tu resiliencia organizacional, a motivar a tu personal y maximizar tu rendimiento y aportamos la perspectiva que te impulsa.

Aviso Legal (Disclaimer)

WTW ofrece intermediación de seguros, y servicios de consultoría a través de entidades legales debidamente registradas ante los reguladores de cada país donde WTW opera. Para más detalles sobre las licencias y regulaciones de las entidades legales de WTW que operan en su país por favor referirse al sitio web de WTW: <https://www.wtwco.com/en-GB/Notices/global-regulatory-disclosures>.

Es un requisito normativo para nosotros considerar nuestros requerimientos de licencias locales antes de establecer cualquier acuerdo comercial. y/o contractual con nuestros clientes.

Las informaciones compartidas en esta publicación son consideradas precisas en la fecha de su comunicación, indicada en este documento. Estas informaciones pueden haber sido cambiadas o reemplazadas posteriormente y no se deben clasificar como precisas o adecuadas después de esta fecha. La presente publicación ofrece un resumen general sobre el tema al que se refiere. No aborda necesariamente todos sus aspectos ni todos los productos disponibles en el mercado. No es la intención que se la utilice (ni debe utilizarse) en reemplazo de asesoramiento específico referido a situaciones individuales.

WTW no ofrece (y no debe suponerse que la presente constituye) asesoramiento en materia contable, jurídica, regulatoria o tributaria. Si tiene previsto adoptar medidas o tomar decisiones sobre la base de los contenidos de esta publicación, le recomendamos consultar primero a un profesional apropiado para recibir asesoramiento específico en la materia. Es probable que parte de la información contenida en la presente se haya obtenido de fuentes externas que consideramos confiables, no obstante, lo cual no garantizamos ni asumimos responsabilidad por la exactitud de dicha información. Las opiniones expresadas no necesariamente reflejan las de WTW