Seguros en enfoque: el avance de la tecnología, la aceleración de innovaciones y la amenaza de los riesgos cibernéticos

Escrito por: Ronaldo de Andrade - 11/08/2022

Brasil camina a pasos largos para la innovación de seguros basada en el uso, consumo y experiencia del usuario, escenario fuertemente impulsado por el día a día tecnológico de la vida moderna, que está cambiando estándares y creando nuevas necesidades de mercado.

Si por un lado este movimiento de transformación que estamos vivenciando y construyendo abre infinitas posibilidades y un camino fértil para la innovación, por otro lado los ataques cibernéticos son actualmente un riesgo real y representativo que requieren acciones preventivas y mitigatorias por parte de las empresas (¡y de las personas!).

La inteligencia de datos en el campo

Los efectos de la tecnología están por todos lados. En el campo, el avance de las redes de alta velocidad – por medio de la conectividad 5G – está tornando los cultivos más inteligentes y dinámicos.

El uso de IoT, la llamada “Internet de las Cosas”, tecnología utilizada para integrar dispositivos a Internet, así como el uso de datos históricos para tomas de decisiones (variedades plantadas, mejores épocas para siembra y corte, entre otros), elevan las oportunidades de éxito de los empresarios del sector.

Del otro lado, consumidores también son beneficiados por los avances tecnológicos, con mayor disponibilidad de productos y menores costos, derivados de una producción y almacenamiento más inteligentes, que resultan en optimización del flujo de la producción nacional.

Toda esta integración y conectividad amplían horizontes, trayendo posibilidades concretas de seguros personalizados para reflejar la realidad del campo, pero también amplían riesgos en el ambiente virtual, y quien no esté alerta está destinado a perjuicios en larga escala.

Porque redes inteligentes y autónomas deben necesariamente ser resilientes y adecuadamente protegidas de los crecientes y cada vez más sofisticados ataques cibernéticos.

Según una alerta del FBI para el sector del agroindustria conteniendo cinco ejemplos de empresas atacadas por el ciber-crimen, una hacienda localizada en los Estados Unidos sufrió daños financieros de US\$ 9 millones debido a un apagado temporal de sistemas.

El perjuicio se derivó de un ataque de ransomware, en el cual un grupo desconocido obtuvo acceso a la red interna del productor rural usando credenciales comprometidas. El incidente, ocurrido en enero del 2021, es uno de los peores impactos de los ataques de ransomware citados

por el departamento de investigación americano.

Innovación en seguros en el área de salud

Otro sector muy impactado por la tecnología, el área de la salud ha avanzado de forma importante en el uso de inteligencia de datos. Cada vez más gadgets recolectan datos y referencias de nuestro cuerpo, como lectura de ritmos cardíacos, niveles de ejercicios, estrés y sedentarismo, por ejemplo, trayendo parámetros importantes para el área médica, seguros de salud y operadoras.

¿Imagine un seguro salud en que el costo mensual disminuye o aumenta con base en esos datos que son recolectados en tiempo real al respecto de su salud y nivel de actividad física?

Operadoras están atentos a ese nuevo mercado, que ya es una realidad. De acuerdo con un estudio realizado por [Check Point Research](#) (CPR) al inicio del 2022, el área de la salud fue el segundo sector que más sufrió [ciber-ataques](#) en el período del 2020 al 2021. Atrás solamente del sector minorista, instituciones de salud y sus plataformas tuvieron un aumento del 64% de los ataques en Brasil.

En diciembre del 2021, la plataforma ConecteSUS, que emite el certificado de vacunación de covid-19, [quedó fuera del aire](#) después que el Ministerio de la Salud fue blanco de un ataque hacker. La plataforma pasó 13 días sin funcionar, perjudicando a millones de brasileños que utilizaban el servicio para comprobar su vacunación.

Los riesgos de los carros conectados...

¿Y si su carro tuviese total conectividad con las operadoras de seguros auto, con el 5G facilitando la transmisión de trayecto, modo de dirección, tiempo en tránsito y, principalmente seguridad al volante? Estos son parámetros que están en constante recogida y las empresas están en franca evolución para que las aseguradoras evalúen y flexibilicen su cuenta de seguros mes tras mes.

Por otro lado, hay diversos escenarios en los cuales los choferes pueden ser víctimas de ataques que amenazan su seguridad en carros conectados.

La investigación “Cyber Security for Connected Cars: Exploring Risks in 5G, Cloud and Other Connected Technologies”, publicada por la consultoría de ciber-seguridad Trend Micro, evaluó 29 escenarios reales de ataques cibernéticos en el modelo de amenazas DREAD 1 en análisis cualitativo de riesgo, teniendo como blanco carros conectados, que se mostraron vulnerables por ser fácilmente descubiertos.

En este tipo de ciber-crimen, el ataque puede ser lanzado contra el vehículo o a partir del mismo, siendo que más del 17% de todas las variables analizadas fueron consideradas de alto riesgo, pues se mostraron de baja complejidad para los atacantes, que no necesitan de conocimiento más profundo de la tecnología del carro conectado, pudiendo ser explotados por invasores con poca habilidad.

Tecnología y su impacto en el sector de seguros

Toda esta tecnología, que ya es una realidad, nos coloca en un nuevo modelo de seguros que no se basa en la media o en el estándar, sino en la individualidad de cada asegurado.

En este exacto momento, miles de datos están en conexión y recogida en su smartphone o en cualquier otro device por el cual usted esté leyendo este artículo. En este nuevo mercado donde los datos son el producto core de muchas soluciones, el cuidado con conectividad y el respeto a normativas de privacidad, como la Ley General de Protección de Datos (LGPD), son puntos fundamentales de cualquier actividad que involucre tecnología y servicios.

Medidas basadas en modelos de datos para riesgos cualitativos y cuantitativos ya son indispensables para que el mercado pueda seguir este desarrollo.

Horiens, por medio de su laboratorio de riesgos, Risk Labs, cuenta con un track record de modelado probabilístico de riesgo en áreas complejas como salud suplementaria, productividad agrícola, default de garantías y continuidad operativa.

Este trabajo es realizado por medio del desarrollo y validación de modelos cuantitativos para apoyar la toma de decisiones estratégicas y tácticas de nuestros clientes, trayendo la seguridad necesaria para que la empresa pueda innovar y crecer de forma sostenible.

¿Vamos a programar una conversación sobre este tema? Accione contato@horiens.com

Fuentes: <https://www.cisoadvisor.com.br/>; olhardigital.com.br.