Noticias

Coronavirus x ambiente cibernético: ¿usted sabe cómo proteger a su empresa?

Escrito por: Horiens - 13/04/2020

Del mundo físico para el virtual en un chasquido de dedos. Sí, el covid-19 hizo que los cyber risks disparasen la luz roja en las agendas de las empresas. Si los ciberataques ya eran considerados unos de los grandes riesgos de la actualidad, ahora la situación quedó considerablemente más crítica.

En Brasil, la cantidad de dispositivos digitales en uso ya supera al número de brasileños. Súmese a esto el aumento del volumen de informaciones estratégicas que circula en la red, en tiempos de cuarentena para la prevención al coronavirus y, consecuentemente, home office. Todo esto crea un escenario de mayor vulnerabilidad que es una invitación para los crímenes virtuales, de los más variados tipos y proporciones.

“La necesidad de que las empresas adopten una fuerte estrategia de seguridad de la información digital nunca fue tan grande como ahora”, explica Eduardo Damião, especialista en Seguros de Riesgos Cibernéticos de Horiens.

La dimensión del problema
Ya sabemos que mucho antes del nuevo coronavirus, los cyber risks tenían lugar cautivo en la lista de los grandes riesgos del siglo. Para tener una breve idea, Internet Crime Report del FBI consolidó datos del 2019 referentes a más de 400 mil denuncias de todo el mundo, que sumaron más de US$ 3,5 mil millones de perjuicio a las víctimas.

Brasil es un blanco importante de los ciberataques. Un estudio de Symantec muestra que el país está entre los principales blancos y es el 4º en el ranking de crímenes cibernéticos, atrás solamente de los Estados Unidos, China e India.

En medio a la crisis actual, un informe del Forum Económico Mundial, divulgado en el pasado mes de marzo, incluye los ataques cibernéticos entre los riesgos que pueden traer impactos negativos en varios sectores por un período de 10 años. De acuerdo con el informe, el 75% de los cerca de 750 especialistas y líderes consultados esperan un aumento en los ataques en busca de datos o dinero en el actual escenario.

Otro estudio, de Apura Intelligence, consultoría brasileña especializada en seguridad digital, divulgó datos que contabilizan más de 63 mil eventos potencialmente fraudulentos mencionando la palabra coronavirus en Brasil.

Como se ve, datos no faltan para alertar la potencialización de los cyber risks.

¿Pero cuáles son los riesgos cibernéticos más recurrentes?
Estamos hablando de situaciones que incluyen desde robo de datos a invasiones y sabotaje de sistemas de infraestructura, energía y abastecimiento o incluso financieros, por ejemplo, con el potencial de causar efectos impactantes para la sociedad y la economía en general. Las

consecuencias pueden ser localizadas o de proporciones gigantescas. Todas, de alguna forma, traen perjuicio.

De acuerdo con datos del Internet Crime Report, del FBI – informe citado anteriormente –, cerca de la mitad de las pérdidas computadas en el 2019 ocurrió por fraudes del tipo Business E-mail Compromise (BEC), cuando el estafador engaña a los funcionarios de una empresa por medio de mensajes de e-mail para que los pagos sean realizados en cuentas controladas por hackers. Hay modalidades más avanzadas de este tipo de golpe, con invasiones a la red de una empresa para buscar informaciones de pagos y proveedores.

En el 2020, el combate al coronavirus acabó creando el ambiente ideal para el ataque de hackers. Archivos disfrazados que utilizan el nombre coronavirus están esparcidos por la red – pero no se equivoque y tenga cuidado – muchas veces el objetivo de estos archivos es dañar o cifrar datos.

Entre los crímenes cibernéticos más comunes, tanto para usuarios como para empresas, se destacan los llamados **DDoS**, ataques de negación de servicio realizados por medio de sobrecarga en los servidores de las empresas, quitando servicios del aire. Este formato de crimen tiene un impacto directo en las operaciones, causando perjuicios financieros. Pero los problemas no terminan ahí, muchas veces este tipo de crimen es una distracción planificada para quitar el enfoque de la seguridad de TI y abrir territorio para la aplicación de estafas más elaboradas.

La lista de posibles crímenes también incluye **secuestro de datos (ransonware), invasión de sistemas, instalación de vulnerabilidades, fuga de datos o contenido personal, comprometimiento de sistemas de seguridad**, entre otros.

E-mails disfrazados con remitente desconocido o bots, los llamados robots de Internet, son ejemplos de estrategias utilizadas por los hackers para cometer los cibercrímenes.

¿Cómo protegerse?
Los especialistas muestran que la cuestión no es “si” la empresa sufrirá un ataque cibernético, sino, “cuándo”. En la era de la información en que vivimos, es necesario conocer sobre el tema, entender el riesgo y sus consecuencias, de punta a punta.

Esto incluye acciones como actualizar constantemente los sistemas de tecnología, revisar periódicamente la política de seguridad digital de la empresa, campañas educativas para funcionarios y contratación de seguros específicos, por ejemplo.

“La demanda por las pólizas de cyber risks está mayor. Las empresas deben evaluar su exposición en primer lugar para entonces transferir parte de estos riesgos para una póliza de seguro que satisfaga mejor sus necesidades. Incluso no transfiriendo todos los riesgos, por medio del seguro ocurre la mitigación de los posibles daños/reclamaciones. El tema requiere atención y acción por parte de las empresas”, concluye Eduardo Damião.