Los ataques cibernéticos en tiempos de Covid-19

Reduzca daños económicos colaterales del coronavirus.

7 de abril, 2020

LOCKTON®

En medio de la pandemia de Covid-19 se habla mucho del coronavirus y quizá no se preste suficiente atención a otro tipo de virus, el cibernético. Éste, desde luego no es mortal ni ataca al cuerpo humano, pero sí afecta la economía de las empresas y al sector productivo del país.

La principal indicación de las autoridades a la población para hacer frente a la emergencia sanitaria es “Quédate en casa”. El objetivo es disminuir los riesgos de contagio y evitar una saturación de la red hospitalaria.

Con ello, salvo los considerados esenciales, la mayoría de los sectores económicos, tanto públicos como privados, están llamados a suspender sus actividades o continuarlas vía remota. Los trabajadores, ya sea del ámbito gubernamental, empresarial, académico o social, deben preferentemente trabajar en casa. Pero realizar tareas a distancia, el comúnmente llamado “home office”, conlleva riesgos para la seguridad de los equipos de cómputo y –lo que es más grave– para el sistema informático, comprometiendo la estabilidad de los centros laborales.

En términos administrativos, la actual contingencia ha demostrado que no hay un lenguaje común en temas de seguridad cibernética. A ello se añade la falta de expertos calificados e interesados en el tema. Esto ha evidenciado la vulnerabilidad de empresas y dependencias de gobierno.

Un ataque cibernético o una infección con un virus informático puede provocar no sólo un daño económico, sino hasta poner en riesgo a las personas, en caso, por ejemplo, de verse vulnerados los sistemas de salud pública y privada, tras una eventual afectación a la red hospitalaria.

En la actual coyuntura, la noticia día con día es el aumento en el número de contagios y la cifra creciente de fallecimientos a causa de la epidemia del COVID19. Ello ha provocado que la gente centre su atención en todo lo que derive de la contingencia, desde las medidas de higiene hasta los protocolos de acción ante un caso de infección.

Es en momentos como éste cuando los delincuentes cibernéticos aprovechan la distracción de la gente para llevar a cabo ataques de mayor impacto y con más frecuencia.

Es decir, los riesgos no necesariamente son nuevos, pero las víctimas son más susceptibles en un contexto como el que vivimos. Las amenazas cibernéticas cambian constantemente y sólo podemos confiar en la experiencia y los casos ocurridos, aunque esto no nos asegura que las nuevas amenazas sean idénticas.

Tipos de riesgo y modalidades de ataque

PHISHING

En esta modalidad, los delincuentes cibernéticos se hacen pasar por una institución para contactar a las personas por medio de correo electrónico, mensajes o llamadas y solicitarles sus datos personales, información financiera y/o contraseñas, para cometer el atraco. Al encontrarse las personas distraídas, crece la probabilidad de caer en este tipo de malware (código malicioso).

RANSOMWARE

Es un tipo de secuestro virtual de información sensible. Se logra introduciendo un malware en la red de la víctima, que codifica los datos, inutilizando sus sistemas. Para liberar la información y brindar de nuevo acceso al sistema se exige un rescate, el cual suele ser en criptomonedas. El ransomware suele ser enviado vía spam o por phishing. Muchos de estos malware pueden permanecer imperceptibles por un largo tiempo hasta que su creador decida activarlo.

REMOTE WORKERS

El principal riesgo del home office es que los empleados se conectan a través de redes que pueden ser inseguras, dando la oportunidad a terceros de ingresar al sistema de la compañía.

Prevenir para no lamentar

Este escenario que pareciera catastrófico tiene, sin embargo, soluciones. Una de ellas es contar con una buena póliza de riesgos cibernéticos. Contratado acertadamente, un seguro puede cubrir las pérdidas relacionadas con vulneraciones de seguridad, a raíz de contingencias como la derivada del Covid-19.

Hay factores importantes a considerar al momento de presentar una reclamación, pues recordemos que todo debe estar relacionado con la cobertura de la póliza. Por ello es importante cuestionarse lo siguiente:

- **¿Las computadoras de los trabajadores remotos son parte del sistema informático de su empresa?**
- **¿La pérdida por interrupción del negocio fue causada por un evento cibernético?**
- **¿Un reclamo de un tercero alega un acto ilícito?**

Con estas breves preguntas es posible identificar si un evento sería objeto de cobertura, ya que toda reclamación es única y debe ser evaluada en su contexto.

Lockton, el corredor de seguros privado más grande a escala mundial, cuenta con todo el expertise para orientar a las empresas para elegir la póliza que más le convenga, en función de sus necesidades e intereses.

VACUNAS EXISTENTES:

Al margen de contar con una póliza de riesgos cibernéticos, cuya finalidad es aliviar los daños ya ocasionados, es recomendable hacer todo lo que esté al alcance para evitar la necesidad de recurrir al seguro.

Hay cuatro áreas importantes donde es deseable enfocarse. Aquí van algunas recomendaciones en cada una.

Mejores prácticas - colaboradores

Mantenga a su equipo informado con fuentes confiables, eso ayudará a:

- **Evitar las estafas de phishing que dicen tener información.**
- **Dar a sus colaboradores incentivos para mantenerse conectados.**
- **Tener una salida clara para los desafíos tecnológicos relacionados con el hogar.**

Solicite su ayuda para:

- **Cambiar las contraseñas de red y Wifi.**
- **Realizar las actualizaciones semanales (incluye avisos de seguridad).**
- **NO utilizar sistemas en el hogar para cosas de trabajo.**
- **Mantener los dispositivos bloqueados cuando se aleje del lugar de trabajo, ¡los niños están ahí!**

Mejores prácticas - tecnología

No pierda de vista la seguridad:

- Al realizar home office, es necesario habilitar un enlace, una conexión entre una red externa y la red privada de la compañía para, así, poder compartir información. Esto es posible gracias a un programa VPN (Virtual private network, por sus siglas en inglés).

  Asegúrese de que las configuraciones de VPN sean las adecuadas.
- Tenga en cuenta que la gestión de vulnerabilidades es más importante que nunca.
- Evalúe su nueva realidad para enfrentar posibles problemas.
- Revise los parches en sus dispositivos remotos.
- Cerciórese de que los dispositivos requieran autenticación de dos factores.
- Cifre unidades de computadora en casa.
- Utilice contraseñas seguras para redes inalámbricas.
- Instale un fuerte software antivirus que se actualice regularmente.
- Indique a los colaboradores que eviten conectarse a una red Wifi pública.

Mejores prácticas - ubicación física

¿Está vacía su oficina?

- Envíe a alguien a revisarla regularmente (si es posible).
- Vigile a través de monitoreo remoto las instalaciones
- Revise que las alarmas (incendio, robo, inundación, etc.) funcionen.
- Permita que los colaboradores se lleven a casa la laptop o PC de escritorio que tengan asignada en la oficina antes de orillarlos a usar dispositivos domésticos.
- Bloquee equipos informáticos y áreas de trabajo sensibles.
- Verifique si la información confidencial es accesible en las estaciones de trabajo.
- Vea la pertinencia o necesidad de mantener activa su red inalámbrica.

Mejores prácticas - respuesta a incidentes

- Desempolve su plan de Respuesta a Incidentes (RI) y pruébelo. Ahora más que nunca es necesario saber cómo actuar en caso de una contingencia cibernética.
- Tenga claro a quién debe llamar cuando ocurra algo fuera de lo normal.
- Garantice la continuidad del negocio. Sepa qué hacer si la conectividad se corta por un tiempo.
- Asegúrese de que su póliza de Riesgos Cibernéticos no cree fricciones con su plan de RI.

Para consultoría adicional y mayor información, lo invitamos a contactar a Lockton, empresa líder en el mercado y con más de 40 años de experiencia.

UNCOMMONLY INDEPENDENT