Estrategias
para mitigar los ciberataques más comunes en PYMES

Mayo 2020

LOCKTON

Las Pymes cada vez hacen más uso de la tecnología para responder a las demandas de sus clientes y aprovechar los beneficios de una fuerza comercial en movilidad, lo que las ha convertido en un objetivo para todo tipo de ciberdelincuentes.

De acuerdo a diversas investigaciones que han realizado analistas en ciberseguridad, la fuga de información, phishing y los malware son algunos de los riesgos cibernéticos que las compañías enfrentan con mayor frecuencia. Tan sólo en 2019, 54% de las empresas mexicanas sufrieron algún robo de información, de acuerdo con un estudio hecho por PayPal y Microsoft.

Por otro lado, analistas consideran que el 'ransomware' y el BYOD (Bring Your Own Device, es decir, la utilización de dispositivos personales como un celular o una memoria USB en el ámbito profesional y los dispositivos asociados al Internet de las Cosas) serán, entre otras, algunas de las principales ciberamenazas para las pymes en 2020.

Durante 2019, México recibió más de 300 millones de ciberataques, lo que representa un aumento de 31% respecto a 2018, lo que lo posiciona como el segundo país de América Latina con más ataques cibernéticos y el noveno a nivel mundial, según datos de la firma de seguridad Kaspersky.

Además, 79% de las empresas a nivel global clasifica el riesgo cibernético como una de las cinco principales preocupaciones para su organización para este 2020, de acuerdo con la encuesta 2019 Global Cyber Risk Perception Survey realizada por Microsoft.

Algunas de las consecuencias que se pueden enfrentar por este tipo de delitos son:

- Crisis mal manejada por falta de un plan de contingencia.
- Afectaciones en diversas áreas de la empresa, como imagen corporativa, jurídica, sistemas, finanzas.
- Interrupción de actividades comerciales a causa de la violación electrónica.
- Desacreditación de la empresa por parte de socios, proveedores y clientes.

Estrategias para mitigar los ciberataques más comunes.

Algunas recomendaciones para disminuir la exposición de riesgo ante un incidente son:

- **Restringir los privilegios administrativos –** utilizar solamente privilegios del administrador para la gestión de los sistemas, instalar software legítimo y aplicar parches de software.
- **Respaldar diariamente los datos importante**s – podría parecer obvio, pero si se mantiene una copia de seguridad periódica, sin conexión o fuera de línea, de todos los datos almacenados en forma segura, se contribuirá en gran medida a la continuidad de la empresa en caso que esta sufriera un ciberataque. ¡No olvide comprobar la integridad de dichas copias de seguridad!
- **Endurecimiento de las aplicaciones del usuario** - bloquear el acceso del navegador a medios conocidos para el ingreso de malware, por ej. Adobe Flash Player, anuncios web y códigos Java no confiables.
- **Lista de aplicaciones autorizadas –** permite instalar en las computadoras solamente aplicaciones de software seleccionadas. De esta forma se evita que otras aplicaciones de software no autorizadas, incluyendo malware, se infiltren en su red.
- **Inhabilitar macros no confiables de Microsoft Office** – se deben inhabilitar los “macros” de Microsoft Office que pueden automatizar tareas. Estos macros

se utilizan para automatizar la descarga de malware, de modo que deben ser bloqueados o inhabilitados.

- **Parchar Sistemas Operativos** – mantenga sus sistemas operativos actualizados y con sus vulnerabilidades totalmente parchadas. Los delincuentes cibernéticos utilizan vulnerabilidades conocidas para atacar computadoras y servidores de empresas.

- **Autenticación multifactorial** – fortalecer los controles de contraseñas utilizando autenticaciones sólidas con un "factor" adicional, por ejemplo autentificadores físicos o tokens. Cuando se tienen múltiples niveles de autentificación es más difícil que los atacantes puedan acceder a su información, incluso si han vulnerado la contraseña.

- **Transferencia de Riesgo.** Es recomendable evaluar, prevenir, mitigar y responder ante el riesgo cibernético mediante la contratación de un Seguro de Protección de Datos y Riesgos Cibernéticos.

Adicionalmente a las estrategias de mitigación antes señaladas, es una buena práctica preparar una respuesta ante un ciberataque y actualizar los planes de continuidad del negocio de la empresa.

- **Tenga un Plan de Respuesta a Incidentes (IRP – Incident Response Plan)** - Una organización que tiene un plan IRP claro, conciso y probado será capaz de tomar medidas rápidas para contener una intrusión y minimizar el daño financiero a la empresa. Tendrá una mayor probabilidad de poder responder en mejor forma a las exigencias legales y a multas potencialmente elevadas.

- **Tener un Encargado de la Seguridad de la Información (CISO –** Chief Information Security Officer) – la seguridad de la red y de los datos es un riesgo que involucra a toda la empresa y no es un riesgo que puede ser manejado sólo al interior del departamento de TI. Un CISO (o equivalente) se responsabiliza por la protección de datos y tiene responsabilidad centralizada por la gestión de los mismos. El CISO debe dirigir y coordinar la respuesta de una empresa (Asesor Legal Principal, Gestión de Riesgos, RP/Marketing, Dirección Ejecutiva) frente a un ciberataque. Esta persona debería formar parte del IRP.

Seguro de Protección de Datos y Riesgos Cibernéticos.

¿Qué cubre este seguro?

Este seguro protege a las organizaciones de cualquier tamaño frente a eventos como falta de disponibilidad de sus sistemas, violación de datos personales o información confidencial, corrupción de datos, ransomware (secuestro de datos) y publicación de contenidos electrónicos, cubriendo tanto la responsabilidad frente a terceros, como las pérdidas propias por actos maliciosos o por falla a la debida la diligencia.

Incluye soluciones para la gestión de riesgos informáticos y manejo de crisis después de presentado el incidente.

Coberturas:

Responsabilidad frente a terceros:

La cobertura protege al asegurado frente a la responsabilidad resultante por la pérdida de información confidencial personal y corporativa.

Privacidad:
Falla en la protección de los registros y la información en formato impreso o digital.

Medio:
Transmisión de un ataque informático.

Contenido:
Violación a la propiedad intelectual a través del manejo inadecuado de la información o negligencia en el manejo de contenidos electrónicos.

Impedimento de Acceso:
Restringir el acceso del cliente a los sistemas informáticos del asegurado, ej. Página web, como consecuencia de un ataque al sistema.

Reputación: Difamación o afectación a la privacidad a través de la actividad informática.

Pérdidas Propias:

Cobertura diseñada para mitigar los efectos de un incidente informático.

- **Gastos de notificación.**
- Reducción de la utilidad neta por interrupción del negocio.
- Gastos para la recuperación de datos y costos de recuperación, incluyendo el aumento de costos laborales y gastos por el uso de equipos externos.
- Daños y gastos por ciberextorsión.
- Gastos de manejo de crisis a raíz de un incidente.
- Protección ante procedimientos regulatorios por violación de regulaciones de privacidad.

¿Qué información se requiere para su contratación?

- Es necesario completar un cuestionario que busca conocer la seguridad informática y plan de respuesta a incidentes con los que cuenta la empresa.
- Estados Financieros Auditados.

- https://www.chubb.com/mx-es/empresas/chubb-cyber-riesgos.aspxs21sec.com
- grupoenconcreto.com/top-5-riesgos-ciberneticos-a-combatir-en-2020/