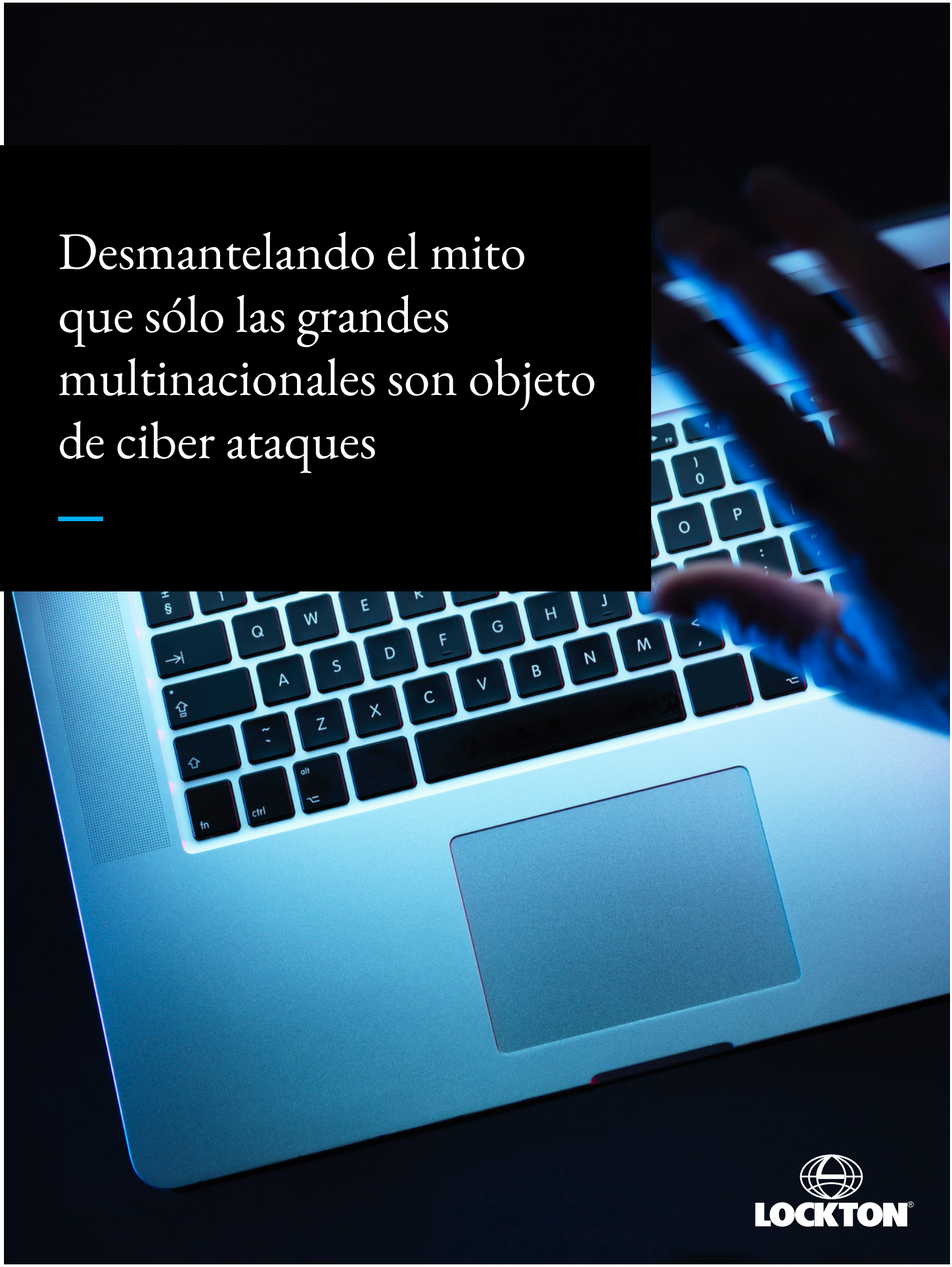
Desmantelando el mito que sólo las grandes multinacionales son objeto de ciber ataques



Los encabezados globales están salpicados de historias de “hackeos”, brechas de información o ataques de ransomware impactando a grandes organizaciones. Esto crea la falsa impresión de que las empresas pequeñas están menos en riesgo.

Cuando organizaciones tales como eBay, British Airways o Equifax sufren brechas a causa de una incidencia o ciber ataque, las noticias rápidamente se esparcen por el mundo. Y esto es entendible, claro, dado que estos ataques pueden potencialmente afectar la información de millones de individuos globalmente.

Pero en nuestros news feed no aparece la historia del contador, que no puede acceder a su computadora por una semana debido al ataque de un malware, o el caso del cirujano plástico al que le fueron retenidos los detalles de sus pacientes a cambio de un rescate. El hecho de que estos ataques estén fuera de la vista pública y que no se reporten en las noticias no quiere decir que no estén sucediendo.

Estimando los ciber ataques a empresas pequeñas y medianas

De hecho, casi la mitad de todos los ciber ataques (43%) están dirigidos a pequeños negocios, de acuerdo a los datos recolectados por SCORE, mentores d pequeños negocios en EUA.

Evidencia anecdótica sugiere que los ciber cirminales ven a los pequeños negocios como objetivos más fáciles pues frecuentemente carecen de los recursos necesarios para invertir en seguridad de TI y proveer de capacitación en ciber seguridad para sus empleados.

Una pequeña empresa es hackeada cada 19 segundos. Un estudio de Hiscox muestra que ahora es más probable que no (59%) de que ocurra una incidencia en pequeñas y medianas empresas.

Un estudio realizado en 2019, por SMB (Cyberthread Study), que entrevistó a más de 500 tomadores de decisiones de niveles directivos en compañías con 500 o menos empleados, reveló que dos de tres de los negocios entrevistados (66%) no creen que serán víctimas de un ciber ataque.

Y esto explica la falta de acciones al respecto. Una de tres pequeñas empresas (35%) ha confirmado que no han instalado un software de seguridad en los últimos dos años, de acuerdo con un estudio realizado por la (FSB). Cuatro de diez (40%) no actualiza su software de forma recurrente, y una proporción similar no realiza un respaldo de su información y de los sistemas de TI. Menos de la mitad (47%) tienen una política estricta de contraseñas para sus aparatos.

Además, los negocios pequeños no necesitan ser un “objetivo” para sufrir un ciber ataque. El malware de MotPetya, afectó a miles de computadoras en el mundo y mientras sí, incapacitó a compañías multinacionales, el daño colateral a pequeños y medianos negocios fue indiscriminado. Como uno de las piezas de malware con mayor propagación

jamás vista, a las primeras horas de su aparición el NotPetya se había diseminado a incontables pequeñas y medianas empresas alrededor del mundo.

Los pequeños negocios son sujetos, colectivamente, a casi 10,000 ciber ataques al día, de acuerdo con la FSB. El año pasado se vio un incremento de 424% de incidencias en nuevos pequeños negocios, frecuentemente a causa de intentos de phising, malware, ransomware y solicitudes de pagos fraudulentas.

Comentarios recientes del CEO de FSB Policy & Advocacy, Martin McTague, subrayan lo siguiente: "Se ha encontrado que existe una escala de riesgos que enfrentan las pequeñas firmas todos los días en la arena digital. El tema es que este tipo de crimen muchas veces es pasado por alto muy a menudo y cada vez más, en este clima de incertidumbre política, Se deben realizar pasos significativos, para salvaguardar a estas pequeñas firmas y por ende a la economía.

Los riesgos son altos, con una potencial pérdida de ingreso y daño reputacional, así como responsabilidades con terceros, particularmente en los casos en donde la relación con el cliente se ha visto deteriorada debido a que se ha comprometido su información con implicaciones legales. Si a esto se le añaden gastos adicionales tales como gastos de regulación de cumplimiento, honorarios legales, investigaciones técnicas y pérdida de clientes, los costos complementarios a un ciber ataque pueden comprometer la estabilidad de un pequeño negocio.

10% de los pequeños negocios que han tenido alguna incidencia en el 2019 se vieron forzados a cerrar como resultado de dicho ataque, de acuerdo a un reporte conducido por Zogby Analytics comisionado por la Alianza de Ciber Seguridad Nacional de EUA.

Recomendaciones

Para reducir su exposición al riesgo, las pequeñas y medianas empresas deberían invertir en tres componentes: recursos, educación y seguros.

- Pese a que es aceptado que las pequeñas y medianas empresas deban concentrar sus recursos en el conocimiento de su propia industria, dejar a un lado las amenazas a la seguridad y los riesgos de negocio que esto conlleva se vuelve un riesgo latente para dichas firmas. Si el dueño de un negocio no tiene el entendimiento de cómo proteger su negocio y tampoco cuenta con personal de TI encargado de velar por la seguridad de las operaciones del negocio contra ciber ataques, debe buscar un socio comercial que tenga este rol, invertir en este recurso. El soporte adecuando en Ti es la primera línea de defensa. Estamos trabajando en una era en donde este no es un gasto discrecional, de hecho los expertos en ciber seguridad dicen que se deben asignar un presupuesto de al menos 3% de los gastos totales de la compañía solamente a este tipo de recursos. Se debe considerar también el escenario que alguien de nuestros empleados esté comprometiendo el negocio ya sea entregando la información a la competencia o reteniendo la información sensible de los clientes para solicitar rescate. Este es un evento cada vez más común y que puede ser evitado con medidas de ciber seguridad bastante simples.
- Invertir en la educación de los empleados. Sabemos que los errores humanos y el fallo de sistemas son responsables del 52% de las brechas de seguridad- no hay firewalls o anti-virus que protejan de un simple error de un empleado. Contraseñas débiles, compartir información sensible por error, dar "clic" en ligas falsas o documentos adjuntos dañinos- 1 de 323 emails que se envían a os pequeños negocios son maliciosos.
- El seguro de cyber es la tercera pieza del rompecabezas de ciber seguridad. Mucha gente cree erróneamente que la cobertura ya está incluida dentro de alguna de las pólizas que ya tiene contratadas. Si bien pudiera haber un traslape de alguna cobertura (suele pasar en algunos programas), las coberturas tradicionales de seguro carecen en profundidad y en amplitud de las condiciones que el seguro de cyber si tiene, además que en caso de incidencia es mejor contar con una asesoría con experiencia en reclamaciones de este tipo.

Una póliza de cyber, protege a los negocios con riesgos relacionados a la infraestructura de TI y sus actividades. Cubre riesgos que resultan de ataques maliciosos así como de incidentes que pasan inadvertidos pero que sí causan daños a los sistemas o información de los negocios.

El seguro de cyber va a reembolsar algunos de los costos que enfrentará el negocio al tratar con un incidente, pero además generalmente cubrirá las responsabilidades que tenga ante terceros derivadas de dicho evento.

Un beneficio significativo de la póliza de cyber es la de los servicios de asesoría que se brindan cuando hay una incidente, ya que el asegurado tiene acceso inmediato a consultores expertos, ayuda que resulta bienvenida sobre todo cuando un negocio está en un una posición vulnerable. Las ciber amenazas crean considerable presión, confusión y preocupación y el tener acceso inmediato a un equipo que incluye forenses en TI, abogados y equipos de manejos de crisis y relaciones públicas, ayudan a la correcta toma de decisiones a un negocio que se encuentra en una posición difícil.

Tomar estos simples pasos para mitigar los riesgos cibernéticos es esencial. La naturaleza de nuestro mundo digital es tal que los ataques cambian todo el tiempo y el panorama de las amenazas es muy dinámico. Lo que es claro es que cualquier negocio que ignore la ciber seguridad está tomando un riesgo importante para el mismo negocio, para sus clientes y para sus socios de negocios. El mensaje que se pretende dejar en claro es que las pequeñas y medianas empresas no son inmunes. Los dueños de estos negocios deben estar conscientes de que el peligro es real y tomar acciones apropiadas para mitigar el riesgo. Estar siempre al pendiente y realizar las debidas investigaciones ya que los defraudadores están haciendo lo propio.

Para mayor información, contactar a:

Felix Leguizamo Domínguez
fleguizamo@mx.lockton.com

UNCOMMONLY INDEPENDENT