Estrategias de ciberseguridad en la nueva realidad

El año 2020 pasará a la historia como uno de los más complicados de las últimas décadas, una crisis mundial no provocada por el mismo ser humano y que ha puesto en estado crítico la supervivencia de muchas empresas, pero, lo más importante, a muchas personas.

En los primeros meses de este año, el liderazgo de las organizaciones estuvo envuelto más en salvaguardar a su personal y lograr de alguna forma mantener la operatividad de su negocio, por lo que las cuestiones y estrategias a mediano y largo plazo se vieron interrumpidas para poder atender las consideraciones tácticas a corto plazo. Los líderes se han centrado, con toda razón, en mantenerse resilientes enfrentando presiones operativas y financieras.

Todavía estamos viendo efectos y tratando de enfrentar la realidad de corto plazo, y ya están surgiendo algunos temas, cuya atención de forma estratégica es importante.

Se están presentando rápidas expansiones de los canales de comercio digital y los comportamientos de los consumidores están cambiando drásticamente. Los ejecutivos tendrán que empezar a atender nuevos asuntos, sobre todo el cómo será la nueva realidad en los próximos años, y cómo preparase para ello.

Asimismo, tendrán que mejorar la resiliencia de su cadena de suministro, adaptarse a los desafíos geopolíticos y a las tensiones que afectan al mercado global; a los nuevos modelos de fuerza laboral y prácticas de trabajo. Tendrán que hacer todo esto enfrentando una crisis económica global y, para muchos sectores, con continuos desafíos de liquidez y deuda.

Por otro lado, hay una tendencia muy fuerte hacia la protección de datos y de privacidad que exige un cambio fundamental en la protección y gestión de datos personales. La adopción de estas nuevas normas en combinación con el impacto reputacional obliga a las empresas a incluir ciberseguridad en todos los aspectos de sus negocios.

Las empresas tendrán que evolucionar, y la tecnología tendrá un papel prioritario y básico para adaptar el negocio, digitalizando cada día más sus cadenas de valor y sus procesos, modificándolos de tal forma que permitan dar respuesta rápida a las necesidades de los clientes. Para los empresarios será cada día más común escuchar términos como "agile", "DevOps", "migración a la nube", "transformación digital" y "trabajo a distancia". Cabe destacar que la mayoría de estos conceptos ya existían antes de la pandemia, pero esta ha sido un catalizador, y su adopción, en lugar de ser un valor agregado, ahora es una necesidad.

El aumento de la dependencia de canales digitales trae consigo un aumento de riesgos e impacto de ataques cibernéticos. Lamentablemente la ciberdelincuencia en esta pandemia ha crecido y sus efectos se han potencializado.

El sondeo "Combatir el cibercrimen en la nueva realidad", realizado en julio de 2020 por KPMG en México, muestra que los ataques a las empresas han aumentado; tras la pandemia, 79% de las organizaciones enfrentan un mayor número de ciberataques en México. Asimismo, 97% de las empresas mencionan incrementos de entre 6% y más de 15% de ciberataques bajo la coyuntura actual.

Seis de cada diez (60%) organizaciones han experimentado ataques de *phishing* en el último año, siendo el más común en las compañías. Los virus y *ransomware* son el segundo más común: 43% de las empresas reciben este tipo de ataques. El *phishing* acompañado de la utilización de *malware* está siendo una combinación destructiva para los negocios en México, y los impactos de fugas o filtración de información, así como las interrupciones en los procesos son ya económicos, siendo la principal preocupación para 74% de las empresas.

En Centroamérica, el paso de la crisis ha generado una adopción acelerada de canales y métodos de pago digitales que, para muchos líderes en la región, han sido herramientas fundamentales para dar continuidad a su negocio;

sin embargo, esto también ha supuesto un reto: desde bancos hasta hospitales y organizaciones del sector salud han tenido que adaptarse a un entorno cambiante que los obliga a integrar tecnología en sus operaciones tomando a su vez la debida precaución para proteger la información de los usuarios.

Ante estos eventos y la nueva realidad es necesario adaptar las estrategias de ciberseguridad para poder protegerse nuevamente. Estos cambios tendrán que ser llevados a cabo tarde o temprano por cada organización, pues para cada reto digital debe existir una respuesta y soporte de los encargados de ciberseguridad. Dichas respuestas deben abarcar la protección al entorno del trabajo del personal, los procesos productivos y los de atención al cliente. Algunos de los cambios son:

1. Arquitecturas de seguridad distribuidas

El concepto de red interna como un entorno donde existe cierta confianza será cada vez menos común. Con el teletrabajo, las organizaciones tienen una fuerte exposición a las amenazas que existen en los ambientes cibernéticos caseros; cada conexión de los colaboradores a distancia potencializa los riesgos y amenazas cibernéticos para la organización.

El control de las estaciones de trabajo en casa (*endpoints*) será el punto focal de la guerra entre ciberdelincuentes y las áreas de ciberseguridad. En las arquitecturas actuales casi todas las herramientas de ciberseguridad están centralizadas; con el teletrabajo muchas de ellas muestran poca efectividad. Por lo tanto, la protección que se tenía en la red interna, si no es sustituida, al menos debería ser complementada con la protección y control de las estaciones de trabajo a distancia. Esto potencializará enfoques de protección como *zero trust*, escritorios virtuales remotos y gestión de dispositivos móviles.

2. Ciberseguridad a la velocidad del negocio digital

Como respuesta al distanciamiento físico, las empresas necesitarán seguir realizando sus negocios en formar remota. En este caso, modificar rápidamente aplicaciones y procesos de negocios será de suma importancia. Las empresas deben derribar las barreras entre los departamentos, unificando la tecnología operativa y las funciones orientadas al negocio para promover la resiliencia en toda la empresa.

Por lo tanto, la seguridad debe integrarse en la transformación digital de los procesos de valor del negocio para mantener la agilad de respuesta, con un sentido de urgencia colectiva sobre las necesidades más allá de las funciones de ciberseguridad y privacidad. Esto potencializa enfoques de protección como seguridad de DevOps, seguridad en entidades federadas y seguridad por diseño.

3. Seguridad en la nube

Derivado de que el entorno físico y las redes internas perderán su importancia, veremos una mayor adopción de nubes con mayor disponibilidad y capacidad de gestión a distancia. Integrar la ciberseguridad en los nuevos requisitos de transformación digital para aprovechar proveedores de servicios y aplicaciones en la nube será una necesidad para este nuevo entorno.

Uno de los problemas más graves que se tiene con la utilización de nubes es la pérdida de la gestión de identidades y privilegios en diferentes proveedores y aplicaciones en la empresa. La pandemia reveló que hay conocimiento limitado acerca de servicios y activos críticos, así como del mejor enfoque para protegerlos. Las empresas necesitan restablecer nuevos modelos de gestión de acceso y monitoreo de la actividad en activos críticos y priorizar la inversión en automatización cibernética; por lo tanto, se potencializan nuevamente conceptos como *cloud access security broker* (CASB); la gestión de cuentas privilegiadas, así como de identidades en conjunto de accesos remotos.

4. Actualizar y practicar plan de respuesta y continuidad

La gestión de riesgos cibernéticos necesita una revisión completa, de arriba a abajo. La pandemia ha demostrado que los antiguos supuestos de riesgo de la cadena de suministro son falsos. Las métricas tradicionales de resiliencia cibernética han sido una representación inadecuada del riesgo real.

Las empresas necesitan revisar su enfoque de las cadenas de suministro; definir métricas prácticas y significativas de riesgo cibernético, y centrarse en los riesgos para las operaciones a la hora de diseñar nuevas estrategias digitales. Uno de los supuestos subyacentes en la mayoría de las planificaciones de continuidad del negocio cibernético ha sido que el resto del ecosistema está operando como de costumbre, y que es posible confiar en proveedores y socios para el apoyo.

La pandemia ha obligado a los negocios a cuestionar esta suposición. Las empresas necesitan revisar los procesos de planificación de la resiliencia y probarlos, dando a los equipos de gestión de crisis las habilidades y experiencia para gestionar bajo una intensa presión. También es necesario revisar la definición del peor de los escenarios en la nueva realidad. Se requiere que la estrategia de seguridad abarque a los proveedores, con una gestión adecuada para los riesgos que representan los terceros.

La pandemia ha evidenciado que los planes de contingencia deben partir de un análisis de riesgo dinámico, con incorporación de escenarios, identificación de vínculos entre eventos y análisis de impacto en tiempo real como elementos críticos para proteger al negocio.

Nunca se ha tenido una situación donde la oferta y la demanda hayan sido afectadas simultáneamente a nivel global. El impacto de la tecnología exponencial y disruptiva obtuvo un impulso significativo como resultando de la pandemia, así que las empresas deben crear la capacidad de reinventarse para poder sobrevivir.

Equilibrar actividades tácticas y estratégicas nunca ha sido fácil; ahora es aún más difícil. Esta pandemia dejará huella en nuestra memoria, y ciertamente durante este periodo veremos una tendencia a depender cada vez más de la tecnología para subsistir. Desde hace muchos años existe el concepto de que la seguridad debe ser un habilitador del negocio, y hoy eso es una realidad. Con la necesaria transformación digital de los negocios, es indispensable que la ciberseguridad esté integrada a los procesos internos y que incluya a proveedores y clientes para generar confianza y poder realizar transacciones, que, sin una seguridad adecuada, no podrían realizarse.

kpmg.com.mx
800 292 KPMG (5764)
asesoria@kpmg.com.mx

KPMG MÉXICO
@KPMGMEXICO
KPMG MÉXICO
KPMGMX

Cuenta con más de 20 años de experiencia en riesgo tecnológico y seguridad de la información, así como en proyectos de gobierno de tecnologías de la información (TI), privacidad de datos y ciberseguridad. Rommel ha asesorado a empresas de diversas industrias como servicios financieros, aeroespacial, servicios especializados en tecnología, gobierno, entre otras. Su especialidad radica en la detección y control de riesgos relacionados con la utilización de TI, su diseño, implementación y estrategias de ciberseguridad. Rommel realiza exámenes de atestiguamiento de control interno de TI, conocidos como SOC 1 y SOC 2 para empresas en diversos países de América Latina. Egresado de Ciencias de la Informática, se ha certificado en auditoría de sistemas (CISA), como Oficial de Seguridad de la Información (CISO); en ITIL Foundation e ISO 27001.

Cuenta con más de 20 años de experiencia como asesor para gobiernos y empresas en países como Colombia, Venezuela, Puerto Rico, México, Holanda y Panamá, trabajando con organizaciones de diversas industrias para impulsar la transformación empresarial combinando innovación, tecnología, talento y procesos. Sus áreas de especialidad están relacionadas con estrategias de negocios y tecnología, transformación del negocio, arquitectura empresarial, innovación empresarial e integración de sistemas de negocios. Glenn fungió como vicepresidente de la Cámara Panameña de Tecnologías de Información y Telecomunicaciones (Capatec) y como director del Comité de Tecnología para la Cámara de Comercio Americana en Panamá (AmCham).

Si le interesa contactar a los autores de este artículo o desea información adicional, favor de dirigirse al 800 292 5764, o si lo desea escríbanos a asesoria@kpmg.com.mx

SÚPER EMPRESAS EXPANSIÓN 2020 TOP companies

ESR Empresa Socialmente Responsable Inclusión Social

UN GLOBAL COMPACT Red México