KPMG

Delitos financieros en tiempos de pandemia

2020 - 2021 KPMG EN VENEZUELA

62.

62 ANIVERSARIO

La pandemia ocasionada por el COVID-19 presenta un impacto significativo y socioeconómico a escala mundial, Venezuela no se escapa de esta realidad. Nuestro entorno empresarial se encuentra afrontando el reto de adaptar su estrategia e implementar soluciones tecnológicas para poner en marcha los planes que den respuesta a sus necesidades, y esto ha generado una alta demanda del espacio digital debido al aislamiento social. Sin embargo, es importante entender los riesgos existentes que vulneran la privacidad y seguridad de datos, los cuales pueden traer como consecuencia el incremento de delitos informáticos.

Algunos de los delitos que se han suscitado durante este período han sido:

1 *Phishing*

Usado para obtener de forma fraudulenta información confidencial de la posible victima con el propósito de cometer actos de extorsión, secuestro, estafa, fraude, legitimación de capitales; entre otros, a través de los siguientes métodos:

- Teniendo contacto y manteniendo conversaciones a través de las distintas vías digitales con las posibles víctimas, a fin de engañarlos con la obtención de algún premio o la venta de un bien, producto o servicio, ya sea haciéndose pasar por personas de vínculo social, laboral, de negocios o interés con la víctima.

- Atacando la red y equipos de una organización, al modificar y redirigir el tráfico a sitios fraudulentos.

2 Ataque DDoS

Ataque DDoS (denegación de servicios) puede inhabilitar un servidor, un servicio o una infraestructura y se puede implementar a través de la saturación del ancho de banda del servidor para dejarlo inaccesible, o por agotamiento de los recursos del sistema de la máquina, impidiendo así que esta responda al tráfico legítimo.

3 *Ransomware*

Ransomware o secuestro de datos, es una forma de malware que bloquea los archivos o dispositivos privando a la organización de la operatividad del negocio y del libre acceso de su información financiera, por ejemplo. Esto con el objetivo de reclamar un pago online anónimo a través de medios digitales (criptomonedas, criptodivisas o criptoactivos) para restaurar la operatividad y libre acceso a la información. Esto se puede lograr a través de mensajes por correo electrónico que con frecuencia tienen dominios no reconocidos o mensajes no esperados. También es ocasionado por el mal uso de la web al visitar páginas que no son reconocidas, al dar clic en publicidades y descargar Apps poco convencionales o de reciente creación.

Para aterrizar más la importancia de conocer y entender cómo operan los perpetuadores con los delitos informáticos, ejemplificamos con los siguientes escenarios a nivel corporativo

Actualmente, la crisis sanitaria mundial generada por el COVID-19 ha planteado un gran desafío a la ciberseguridad, provocando que miles de personas deban estar conectadas al mismo tiempo para atender sus necesidades personales y de trabajo, generando diversas vulnerabilidades.

Inversiones, compras de bienes, servicios y productos

La situación que vivimos está adaptando al entorno corporativo a interactuar con mayor frecuencia a través de medios digitales. Procesos como la contratación y la inversión de capital pueden ser vulnerados si no son debidamente ejecutados, ya que existen individuos o grupos delictivos que aprovechan la circunstancia para aparentar ser algo que no son, con el propósito de estafar e inclusive lavar dinero al ofrecer cubrir las necesidades de la sociedad.

Para reducir la vulnerabilidad, es crucial y primordial asegurar que la gente, los equipos y la sociedad estén alerta y advertidos sobre cómo los criminales están intentando tomar ventaja de esta crisis global. La siguiente lista contempla ejemplos que pudiéramos identificar al momento de aplicar una debida diligencia en las contrataciones:

- Empleados deshonestos, fantasmas o inmersos en actos irregulares
- Usurpación de identidad
- Testaferros
- Entidades identificadas como empresas maletín, intermediarias, ficticias y/o inmersas en actos irregulares.

Plataformas de conferencia

A consecuencia del COVID-19, se han creado nuevos dominios web, muchos de los cuales son maliciosos o sospechosos. Como ejemplo figuran las aplicaciones para interactuar de forma remota, espacio en el que se producen ataques durante las videoconferencias a través de las cámaras de video ya que se apoderan del control de las pantallas compartidas y del contenido que se genera. Además de poder sustraer información confidencial, se pueden ejecutar archivos en el dispositivo de la víctima. Por esta razón, la ciberseguridad se convierte en una prioridad para evitar poner en riesgo los activos digitales que estén presentes en la red.

Aplicativos móviles

A pesar de atender y proteger los ordenadores, los móviles se han convertido en la principal vía que usan los ciberatacantes para sustraer datos y vulnerar la seguridad. Este tipo de acciones suelen suceder a través de aplicativos poco seguros y páginas web que contienen enlaces maliciosos y conexiones a puertos USB desconocidos. Estas maniobras se han generado a través de apps, juegos o aparentes encuestas de estilo de vida. Los usuarios realizan descargas haciendo caso omiso de los términos y condiciones, por lo que los desarrolladores de este software aprovechan para infiltrarse fácilmente en los dispositivos. En la mayoría de los casos, pueden ver datos personales de los usuarios, incluso, acceder a la cámara y al micrófono sin dejar ningún tipo de rastro.

¿Qué podemos hacer para protegernos?

- Mantenernos informados y/o capacitados en los temas relacionados al ciberataque y la ciberseguridad.
- Proteger el trabajo remoto a través de la utilización de equipos corporativos y en cuanto a equipos personales, mantener actualizado el sistema operativo y todas sus aplicaciones, además de contar con antivirus con el fin identificar los posibles ataques.
- Cumplir con el reglamento general de protección de datos que mantenga la organización.
- Incorporar adecuadas herramientas inteligentes que puedan alertar algún comportamiento sospechoso.
- Informar a los colaboradores sobre la protección de contraseñas y las precauciones antes ataques de phishing o smishing.
- Evitar compartir contraseñas y no permitir el acceso remoto a otros usuarios.
- Evitar conectarse a redes wi-fi públicas para manejar información confidencial.
- Evitar vincular los dispositivos móviles a las aplicaciones asociadas a redes sociales.
- Crear contraseñas de difícil cifrado y evitar reutilizarlas para múltiples sitios y aplicaciones.
- Evitar la descarga de contenidos piratas.
- Aplicar la resiliencia en los sistemas de información.

Integrity & Excellence KPMG

En KPMG, nuestra red global de profesionales en ciberseguridad comprende que sus operaciones no pueden detenerse por los riesgos cibernéticos. Los profesionales de KPMG reconocen que la ciberseguridad debe gestionar estos riesgos y no intentar eliminarlos a costa de la sustentabilidad de las operaciones.

KPMG le permite conocer y fortalecer el estado de su ciberseguridad frente a un ciberataque y, como conocedores de los cambios presentados por los nuevos escenarios, disponemos de servicios y especialistas en materia de ciberseguridad y riesgos tecnológicos con el fin de brindar soluciones sostenibles.

Contacto

Ivan Briceño
Socio Líder de Consultoría de Riesgo
y Servicios Forenses
ibriceno@kpmg.com

Juan Manzano
Director de Cyber & CIO Advisory
jmanzano@kpmg.com

Alfredo Sthory
Gerente de Servicios Forenses
asthory@kpmg.com

Yanina Yánez
Consultor Senior de Servicios Forenses
yyanez@kpmg.com

Edwin Adrian
Consultor Senior de Servicios Forenses
eadrian@kpmg.com

Conoce la oferta de servicios de KPMG en Venezuela.

http://brochure.kpmg.com.ve/

kpmg.com/ve/

@kpmg_ve **KPMG en Venezuela**