@ CONTACTO ASEGURADO
...entre usted y su asesor

Organización de Productores
y Asesores de Seguros
ROCAR SRL
MAT. SSN 1274

ORGANIZACIÓN ROCAR SEGUROS

Organización Rocar Seguros / www.organizacionrocar.com.ar
Brigadier Juan Manuel de Rosas 24255, Virrey del Pino, Pcia. de Bs. As.
Telfax: (02202) 494090 (líneas rotativas) / info@organizacionrocar.com.ar

DICIEMBRE 2022

Los riesgos asociados al uso de la tecnología cobran cada vez más importancia

Riesgos informáticos o ciberriesgos

Las personas y las empresas utilizan diariamente, y cada vez más, servicios informáticos y de comunicación para llevar adelante sus actividades. En muchos casos, la necesidad de contar con esos servicios es tal, que su interrupción, mal funcionamiento o el robo de información pueden poner en riesgo severamente sus actividades y responsabilidad personal, profesional o empresarial.

¿Qué tan cerca caminamos del borde de un precipicio que no es sencillo de ver? Esta es una respuesta difícil de responder. Lo cierto es que podemos comenzar por reconocer las distintas facetas de este problema (los riesgos informáticos), para posicionarnos mejor frente a ellos.

Los riesgos:

La interrupción de la continuidad del negocio es uno de los riesgos que más preocupan a los empresarios. Los negocios, para funcionar, dependen cada vez más de los sistemas. Y si por cualquier motivo los sistemas fallan o se interrumpen una gran mayoría de los negocios modernos deja de funcionar o funciona mal.

La falta de continuidad operativa tiene múltiples consecuencias: pérdida de ventas, pérdida de reputación ante los clientes, costos de recuperación, comunicaciones legales, reposición de recursos, demandas, pérdida de clientes.

El robo de información o pérdida de la confidencialidad de los datos, afecta la credibilidad de la empresa, tiene un costo de oportunidad cuando es información privilegiada y nos expone a extorsiones y demandas por afectación de la disponibilidad y privacidad de datos personales de nuestros clientes o socios comerciales.

Las transacciones fraudulentas implican también un serio perjuicio directo a la imagen y la calidad de los servicios.

El hilo más delgado

Si bien no es el único motivo por el cual los sistemas pueden quedar expuestos a un ataque intencional, la realidad es que el factor más vulnerable radica en las personas o recursos humanos que actúan en el ecosistema. Principalmente el personal propio, que habitualmente cuenta con permisos especiales para realizar determinadas tareas, puede ser engañado mediante técnicas de ingeniería social para realizar acciones que derivan en el acceso de personas no autorizadas a claves o lugares físicos que deberían ser inaccesibles para terceros. Luego suplantarán su identidad para actuar en su nombre. Algo similar sucede con los clientes, muy vulnerables por su relativamente bajo conocimiento de los riesgos de este tipo. La capacitación y creación de una cultura de prevención es una tarea que se debe comenzar de inmediato, pero difícilmente tenga un final ya que la dinámica de los riesgos y las nuevas y múltiples formas de comunicación abren permanentemente nuevas opciones a los atacantes.

Las amenazas más frecuentes

Si nos centramos en las cuestiones de Malware e Ingeniería Social, existen diversas técnicas para engañar a los usuarios. No podemos en este espacio describir en detalle un tema tan amplio, pero dejaremos los conceptos principales.

Malware: Se denomina así al software malicioso que toma diversas formas, desde infectar un equipo para desde allí propagarse en una red interna o hacia internet (worms); hasta cifrar los archivos y solicitar un rescate (ramsonware) para permitir el acceso nuevamente a la información. También a obtener puertas

Continúa en la próxima página

traseras de acceso a equipos para desde allí realizar acciones maliciosas o sustituir identidades.

Phishing: Consiste en engañar mediante páginas web o correos electrónicos a una persona para que realice una acción en la cual ingrese sus credenciales bancarias o datos de tarjeta de crédito, simulando ser el titular del servicio.

Vishing: Una variante del phishing donde se realizan llamadas telefónicas para engañar y sacar información a las víctimas con distintas excusas.

Baiting: Consiste en poner a disposición, muchas veces en forma de obsequios, dispositivos infectados con malware (software malicioso) que al utilizarse en el equipo de la persona objetivo, permiten al atacante tomar control del equipo o propagar malware.

Spyware: Software que toma información sobre nuestros usos y costumbres. Eventualmente abre puertas de acceso sin nuestro consentimiento.

Exploits: Todos los sistemas operativos reciben parches de seguridad para quitar vulnerabilidades que se detectan. Es muy buena práctica mantener el sistema con las nuevas mejoras de seguridad. Se llaman exploits a los software que aprovechan vulnerabilidades ya detectadas, que exponen a los sistemas no actualizados.

Rogue: Una de las tantas variantes del phishing: hace creer al usuario que está infectado de virus y lo invita a realizar acciones equivocadas que exponen su información o el funcionamiento del sistema.

Hacking y hacking ético: Los hackers exploran en los equipos conectados a internet procurando aprovechar fallas de configuración, vulnerabilidades por desactualización de los sistemas, puertos o medios de acceso abiertos innecesariamente, claves débiles, falta de cifrado eficiente en las comunicaciones, entre otras posibles fallas; para realizar acciones fraudulentas. El Hacking Ético, por su parte, es realizado por especialistas

con permiso y a pedido de la empresa, para encontrar esas posibles vulnerabilidades antes que un atacante malicioso y proponer las medidas correctivas en forma oportuna.

Medidas

Por la dinámica de los riesgos, cualquier lista de recomendaciones necesariamente es incompleta. Sin embargo podemos remarcar:

- La capacitación del personal y clientes. Fortalecer el eslabón débil y comunicar formalmente las políticas de seguridad de la empresa.
- Uso de anti-malware actualizado. La dinámica de aparición de nuevo malware es tal, que no actualizase es como no tenerlo.
- Actualización del sistema operativo para reducir riesgo de exploits.
- Descargar software de fuentes confiables. Existen muchos sitios de descargas cuyo software está infectado. Lo más frecuente es el Adware, es decir software de publicidad no deseada, pero pueden ser objetivos aún peores.
- Utilizar firewalls que limitan el tráfico en la red a conexiones permitidas
- Recurrir a especialistas para someter el sistema a test desde una perspectiva ética y profesional.
- Realizar respaldos lo más frecuentemente posible de la información, ubicándolos en lugares seguros y testeándolos periódicamente.
- Contar con un plan de contingencia que permita recuperar el sistema frente a una salida de servicio en el menor tiempo posible.
- Utilizar buenas prácticas para el desarrollo o implantación de software para mitigar los ataques.
- Utilizar cifrado de clave pública y VPN's en las comunicaciones para que la información no sea accesible por terceros en la red.
- Finalmente, si la prevención falla, contar con seguros que minimicen las pérdidas materiales. ◀

Hasta el próximo contacto-asegurado

MENSAJE DEL ASESOR

Existen diversos productos de seguros que apuntan a cubrir los daños patrimoniales que se derivan de un incidente informático. Se cubren daños directos del incidente: gastos de recuperación, reposición, interrupción, transacciones fraudulentas, extorsión. Por otro lado, daños a terceros, es decir la responsabilidad por exposición de datos confidenciales, personales o empresariales; finalmente los riesgos propios del manejo de la crisis: gastos de defensa judicial, gastos judiciales, administrativos o forenses. Gastos para la protección de la reputación.

Todas estas soluciones, lejos de ser virtuales, como el software o los sistemas, son concretas y apuntan a resolver problemas concretos del riesgo empresario moderno.

Les deseamos un excelente fin de año y un gran comienzo del 2023. ¡Vamos Argentina! ◀

Una realización SOFTeam+SIDEMA / www.contacto-asegurado.com / info@contacto-asegurado.com

(*) El texto de "MENSAJE DE SU ASESOR" es responsabilidad del productor matriculado remitente.