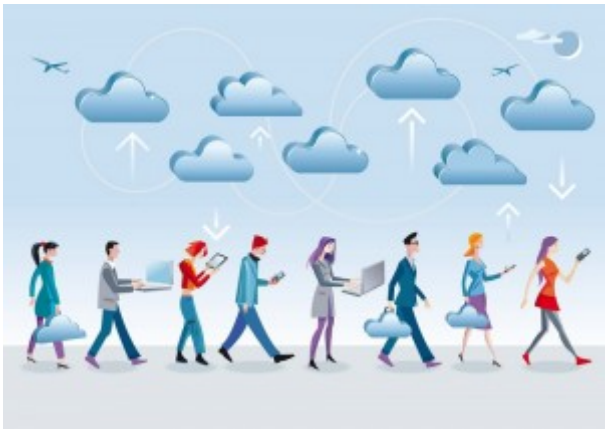
Gestión del Riesgo Empresarial en el Mundo Móvil

Como he comentado en anteriores posts, la fuerza de trabajo móvil (Mobile Workforce) permite que los empleados trabajen donde quieran. Pueden trabajar desde sus casas, que podría definirse como un lugar seguro, o en áreas públicas, como cafeterías o aeropuertos. En este último tipo de lugares es cuando el nivel de amenaza es mayor, ya que puede afectar a la integridad de los datos, pero también a la seguridad física de los empleados, lo que no ocurre en la propia oficina, puesto que se han implementado contramedidas durante décadas. A pesar de ello, no debemos olvidar que el descuido de un empleado remoto puede ser una fuente importante de riesgo que puede afectar a los activos de la empresa. A continuación, se describen las principales áreas de riesgo relacionadas con Mobile Workforce.



Riesgos

- **Activos de la empresa**

Existen dos tipos de activos: físicos (ordenadores portátiles, teléfonos móviles, tabletas) y lógicos (datos de los clientes, datos de los empleados, otra información crítica). Por lo tanto, si alguno de estos dos tipos de activos se pierde o dañan cuando están en posesión de un empleado remoto, suponen un gran riesgo para la empresa.

Además, los hackers u otras personas u organizaciones pueden aprovecharse de los trabajadores remotos para robar datos de una empresa, sabiendo que es más probable que su ataque tenga éxito al atacar a un empleado aislado, que romper las capas de seguridad de toda una organización.

- **Seguridad personal**

La seguridad de los hogares de los empleados no es tan rigurosa como la del propio edificio de oficinas y los criminales son conscientes de ello. Dado que los empleados tienen los activos en sus hogares, lo que significa que estos activos están expuestos al riesgo como un ladrón o un grupo criminal.

Ambos pueden o no ser conscientes del valor de los contenidos y revenderlos.

- **Tecnologías de la nube**

Si una empresa externaliza parcialmente o totalmente sus sistemas e infraestructuras, el riesgo típico de TI relacionado con la confidencialidad, la integridad y la disponibilidad en torno a la administración y gestión de TI, el acceso a los programas y datos, la gestión del cambio y las operaciones aún se mantiene. Además, el uso de internet en las oficinas conlleva un aumento significativo del riesgo. De hecho, los proveedores de nube tienen muchos clientes de los cuales almacenan y administran un gran valor de datos, a los cuales trataran de obtener acceso los hackers a través de una brecha en el sistema de información. Incluso los propios empleados pueden aprovecharse de los datos de los clientes y robar dichos datos para diversos fines.

- **Regulación y Cumplimiento**

Las empresas son responsables de cumplir las regulaciones con las que deben atenerse todas las partes interesadas involucradas en el trabajo móvil. En general, las empresas son responsables de la seguridad de sus sistemas de información, incluso si están externalizados. Es responsabilidad de la compañía asegurar que los datos de los clientes permanecen confidenciales. Si el proveedor de servicios en la nube o un trabajador remoto se ubica en un país donde la protección de datos no es estricta, los datos podrían estar expuestos a un riesgo.

Las empresas están obligadas a cumplir diferentes leyes y reglamentos sobre sus sistemas de información. Este reglamento puede variar en cada país. En los EE.UU., la seguridad de los datos de atención de la salud se rige por el Seguro de Salud de EE.UU. (HIPAA), mientras que en Reino Unido existe la Ley del Servicio Nacional de Salud (NHS) de 2006, la Ley de Salud y Asistencia Social de 2012 y la Ley de Protección de Datos.

Recomendaciones

Para proteger los activos y los recursos, la empresa debería de tomar algunas medidas para reducir el riesgo:

- Identificar y documentar claramente todas las áreas potenciales de seguridad y privacidad relacionadas con el trabajo móvil.
- Realizar programas de capacitación y concienciación sobre los riesgos asociados a los sistemas de información utilizados por los empleados y sus consecuencias para el propio empleado, la empresa, sus clientes y el personal.
- Contraer una póliza de seguro contra pérdidas o daños de activos, de esta forma podrán protegerse contra tales costos. Debido al trabajo a distancia la prima del seguro puede aumentar debido al aumento del riesgo.
- Supervisar los proveedores de la nube. El proveedor debe generar un informe de aseguramiento de terceros, firmado por un auditor externo, que muestre el estado de su control interno.

- Comunicaciones remotas seguras. La empresa debe informar con frecuencia para evitar el uso de áreas de conexión públicas, a no ser que se hayan implementado medidas de seguridad como conexión VPN.
- Dispositivos seguros y su contenido. Para evitar tragedias tras un robo de un dispositivo, los datos críticos deben ser cifrados y hacer uso de una contraseña fuerte. Además, debe de habilitarse el bloqueo de pantalla tras un periodo de inactividad. El antivirus debe de permanecer actualizado. Por otro lado, se debe administrar a los usuarios cerraduras de ordenadores para proteger el dispositivo físico.

Referencias:

[1] Guy Ngambeket, « Mobile Workforce Security Considerations and Privacy » ISACA Journal, volume 4 (2017): 18 – 19