Seis realidades sobre la seguridad de sus activos digitales

Si Vd. es directivo de una empresa seguro que – de una forma u otra – ha debido afrontar en carne propia o de alguna persona próxima una u otra vez situaciones de crisis derivadas del empleo que en ellas se hace de información sensible. Aunque cada vez el nivel de concienciación es mayor, todo directivo debería de tener en cuenta por esa razón los seis siguientes hechos:

1) Cualquier organización trata y almacena información sensible:

Puede tratarse de a) datos personales protegidos por la legislación respecto de los individuos, b) información financiera o estratégica, o c) datos de cualquier tipo sobre los que existan derechos de propiedad intelectual.

No solo hablamos de datos o informaciones en el sentido clásico (es decir, documentos), sino de imágenes, video, audio o cualquier otro tipo de plasmación de ella susceptible de ser registrada y reproducida con finalidades distintas de las que legítimamente podrían ser empleadas.

2) La información valiosa para la empresa se utiliza

De hecho, podemos encontrarla:

- Siendo tratada, en el mejor de los casos con la finalidad para la que se obtuvo y por quien esté autorizado a hacerlo.
- Trasladándose por medios diversos: red privada o pública, cable o wireless, …entre sistemas de información y usuarios, que la procesan en una amplia gama de dispositivos.
- Almacenados a la espera de ser nuevamente utilizados. En las unidades centrales o en dispositivos móviles de todo tipo (desktops, laptops, tablets, smartphones, llaves USB, CDs, …) de los usuarios que la emplean.

3) Los accidentes ocurren y los dispositivos se pierden

Según informes del FBI y en referencia a empresas de tamaño medio/grande, algo mas de un 7% de los dispositivos móviles corporativos se pierden o son robados dentro de su ciclo de vida útil (habitualmente 3-4 años). Estas “transferencias impropias” tienen lugar en lugares públicos y pueden causar graves perjuicios económicos, cuando no la pérdida irrecuperable de información.

4) Hay delincuentes que pueden (si no se lo impiden) acceder a su información

Los activos digitales son – en la época del “big data” – bienes preciados. Y estos individuos disponen

de canales a través de los que convertirlos en dinero contante y sonante: utilizando las cuentas corrientes o los números de tarjeta de crédito de sus clientes, realizando cargos, suplantando a usuarios, administradores, etc… O porque están en condiciones de aprovechar esos datos etratégicos para sacar ventajas en situaciones de competencia.

5) La curiosidad mató al gato

Más de tres cuartas partes de las exposiciones de información reservada se producen en el interior de las propias organizaciones. Empleados o personal interno puede acceder a ella de forma "accidental" y verla o copiarla por "curiosidad".. Quizá en la mayoría de casos no trasciende, pero que en otros llegan a la prensa con la consiguiente repercusión y deterioro de la imagen corporativa.

6) Los extravíos y sustracciones tienen siempre consecuencias:

Estimaciones realizadas por algunas agencias evalúan en una media de 50.000 USD el coste de reposición (y eso en el caso en que se pueda realizar) de un laptop extraviado. Obviamente no nos referimos únicamente al coste del hardware en sí, sino también al derivado de la recuperación de la información personal que el usuario pudiera almacenar en el mismo (suponiendo que existiera backup) y del que puede representar el uso indebido de la información personal y empresarial a la que el sustractor puede tener acceso.

Nuestro consejo para minimizar este tipo de riesgos es: Encripte la información sensible. Consejo en algunos casos innecesario, porque si está Vd. sujeto a cumplir la LOPD deberá mantener, almacenar y transmitir criptografiados los datos personales de tercer nivel de cualquier formato que sean. Y si su negocio hace uso de tarjetas de crédito y está – por tanto – obligado a acatar la norma PCI-DSS, deberá también cifrar las informaciones adecuadas para salvaguardar la identidad de usuarios y tarjetas.