Ajustadores Ltda.

NOTI-AJUSTES

NUMERO 172 ENERO DE 2010

TRANSACCIONES ELECTRÓNICAS DE FONDOS

La mayor cantidad de fraudes por manipulación que sufren en este momento las empresas se originan en la debilidad de los procesos de aseguramiento de la integridad de la información contenida en los formatos para el trámite de pagos, matrícula de proveedores, modificaciones en los archivos maestros, etc.

Rara vez las organizaciones consideran que las áreas de Control Interno o de Auditoría deban involucrarse en este tipo de actividades; lo cual resulta siendo un costoso error.

Siempre hemos sugerido que en la etapa de diseño de los procedimientos y documentos para la automatización de procesos relacionados con la administración de recursos financieros, se cuente con el apoyo de las dependencias de Control Interno o de personas con conocimientos acerca de los riesgos que se corren al depositar excesiva confianza en los procesos de transferencia electrónica de fondos, como los ofrecidos por las entidades bancarias.

El procedimiento para efectuar pagos por transferencia electrónica, usualmente comienza con la matrícula de las cuentas del beneficiario de dichos pagos en el sistema de la empresa deudora. Para ello, basta con digitar los datos del beneficiario, como son nombre, NIT, número de cuenta y nombre de la entidad bancaria correspondiente. Una vez hecho lo anterior, la persona autorizada prepara una relación con los pagos a realizar, para que otra persona diferente sea quien los apruebe y ordene la distribución de los fondos entre las cuentas de cada beneficiario de pagos.

Hasta este punto, la operación se rodea de cierto nivel de seguridad. Pero, si no se han tomado las precauciones mínimas necesarias, tarde o temprano alguien desde el interior o el exterior de la empresa hallará la manera de explotar en su propio beneficio las debilidades de este sistema.

Por ejemplo, si el archivo maestro de proveedores no ha sido suficientemente blindado,

podría ocurrir que alguien con acceso sin restricciones a esta base de datos pueda ingresar a la misma, e incluir un nuevo beneficiario de pagos. Con un proveedor falso en la base de datos, el siguiente paso es sencillo: hacer aparecer una factura, falsa por supuesto, de este proveedor que existe solamente en la base de datos, pero que nada provee a la empresa. De esta manera, cuando se ordene el pago, el sistema indicará que dicho proveedor sí es válido, que figura en la base de datos y que se le puede, en consecuencia, hacer el pago solicitado. Este fraude se puede materializar por que lo normal es que las personas que tramitan los pagos en las empresas se encuentran muy alejadas de quienes compran y reciben los bienes y servicios. De esta forma, quienes aprueban los pagos a menudo no tienen idea de lo que están aprobando, lo que si bien es una sana práctica de segregación de funciones, acaba facilitando el pago de acreencias inexistentes.

Otra forma un poco más elaborada de hurto consiste en abrir una cuenta bancaria a nombre de un proveedor existente (tarea muy fácil, considerando la fragilidad de los requisitos de los bancos para abrir cuentas bancarias). Con la constancia expedida por el banco acerca de la existencia de la cuenta bancaria a nombre de la empresa real, basta con dirigir una comunicación a la empresa víctima, solicitándole modificar la cuenta de destino para consignar de ahora en adelante los dineros que se le adeudan al proveedor legítimo. Si el cambio se hace sin ninguna verificación (confiando en la certificación bancaria) los pagos que en lo sucesivo se hagan al proveedor legítimo, irían a parar a manos del delincuente que lo ha suplantado; pero no en su perjuicio, sino en el de la empresa que pagó a quien no correspondía, sin verificar si en realidad la nueva cuenta pertenecía a su proveedor.

El manejo seguro de los archivos maestros de proveedores resulta esencial. El ingreso de nuevos datos a este archivo debe ser considerado como una operación de alto riesgo, y en consecuencia rodearse de las mayores seguridades. Lo mismo debe hacerse con las solicitudes de modificación de datos, como cuentas bancarias, direcciones, etc. No se debe creer ciegamente en cartas o comunicaciones recibidas, por el simple hecho de estar impresas en papel con membrete y logotipo de una empresa conocida. Los recursos actuales permiten capturar en Internet logotipos, formatos, firmas de representantes legales y demás características de seguridad de la correspondencia de las empresas, con suma facilidad.

Establezca períodos de latencia para efectuar cambios en las condiciones pactadas de pago con sus proveedores, anunciando que cualquier modificación solo se hará efectiva dentro de un número determinado de días.

Durante este tiempo, personal de auditoría o control interno podrán verificar la realidad de la solicitud de modificación.

asr@une.net.co