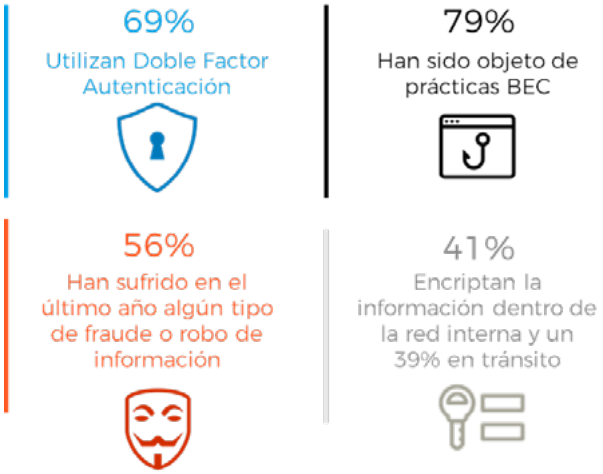
José Manuel Martínez Carpintero
Lead Consultant en CONVISTA

¿A qué esperas para dotar a tus pagos en SAP del más alto nivel de seguridad?

Una reciente encuesta a nivel mundial, dirigida a los departamentos de Tesorería, sobre fraude y los controles llevados a cabo para combatirlo, ha arrojado las siguientes conclusiones:

- Un 56% de los encuestados han experimentado fraude cibernético o robo de información en los últimos 12 meses.
- Un 79% de las corporaciones han padecido fraude vía BEC (Business Email Compromise). Este tipo de ataques, generaron unos costes en el ejercicio 2018 por valor de 8.000 millones de euros
- El 69% de las empresas utilizan un doble factor de autentificación, a la hora de autorizar transacciones en sus plataformas de pago o ERP.
- Un 41% de las compañías encriptan información dentro de la red interna y al menos un 39% cifra la información en tránsito.



Si bien estos datos, transmiten cierto grado de concienciación, que, en materia de seguridad, están adoptando las corporaciones a nivel mundial, los mismos, se reducen drásticamente en el ámbito local.

El mejor plan de seguridad es aquel que es global y que integra elementos como la protección de información mediante encriptación/firma digital, doble factor de autentificación en procesos/tareas clave, continua formación interna a empleados (evitar BEC fraude, phishing, …) alta segregación de roles y delimitación de funciones, entre otros.

Las empresas tienden a focalizarse en un único elemento de los citados, haciéndolas vulnerables.

Lógicamente, la dinamización de los factores de protección en una compañía requiere de dedicación de recursos. Inversión, que, por otro lado, debe de ser mayor cada año, ya que como arrojan los datos de las encuestas, el número de amenazas crece anualmente de forma exponencial.

Del análisis de esta encuesta también se han extraído importantes inputs, sobre los cuales, las empresas deberían poner el foco y emprender acciones, en pos de reducir su exposición a la estafa y al robo cibernéticos.

Analizaremos todos ellos, desde el punto de vista de su aplicación concreta, en el ERP de SAP.

MAYOR SEGREGACIÓN DE ROLES Y MENOS PERMISOS POR USUARIO

Una correcta segregación de roles debe ocupar un lugar destacado en toda estrategia integral de seguridad y en el departamento de Tesorería, más si cabe, ya que permite reducir de forma significativa, el riesgo de amenaza de fraude dentro de la organización. A través de SAP GRC, pueden automatizarse controles y alertas sobre transacciones Z “bespoke”, incorrectas asignaciones de transacciones incompatibles con determinados roles, roles template no funcionales, etc.

MONITOR DE ANOMALÍAS /SANCTIONS SCREENING

En el área de pagos, es recomendable tener una herramienta que habilite a la corporación, la posibilidad de establecer un circuito de aprobación, que involucre a diferentes perfiles del área

financiera y que permita el acceso y navegabilidad del pago a las facturas registradas, así como trazabilidad del mismo una vez que el pago sale de la organización. Ambas posibilidades, las ofrece el módulo de comunicación bancaria de SAP (Bank Communication Management SAP BCM).

La existencia de "listas negras" dentro de la propia organización o la explotación de servicios de "Santions Screening" que ofrece la plataforma SWIFT u otros terceros, permiten alertar a los departamentos de tesorería sobre beneficiarios y cuentas bancarias susceptibles de sospechas fundadas.

Disponer de una integración con este tipo de servicios a través de BCM, permite a los responsables financieros poder anticipar el bloqueo o cancelación de un pago que haya salido como consecuencia de una amenaza BEC, phishing, ….

El propio módulo de comunicación bancaria de SAP permite establecer el envío de alertas personalizadas, en función del resultado de la validación de la información recogida en los ficheros, contra esas "listas negras", incrementando la capacidad y velocidad de reacción.

Las nuevas modalidades de pago como faster payments o SEPA Instant Transfer no dejan mucho margen de actuación para cancelar una transacción, por lo que este tipo de integraciones en tiempo real, pueden evitar quebraderos de cabeza al área tesorera.

> "El factor humano constituye el eslabón más frágil de la cadena de seguridad. Motivo por el cual, el esfuerzo en el aprendizaje del equipo humano para la detección y ejecución de procedimientos de actuación frente a este tipo de amenazas, se presume clave"

FORMACIÓN AL PERSONAL

Los expertos en seguridad coinciden, en que el factor humano constituye el eslabón más frágil de la cadena de seguridad. Motivo por el cual, el esfuerzo en el aprendizaje del equipo humano para la detección y ejecución de procedimientos de actuación frente a este tipo de amenazas, se presume clave en una correcta resolución de las mismas. El casi 80% de los encuestados confirmaban que el fraude BEC, era la amenaza más generalizada a la que se enfrentan en el día a día sus compañías. BEC basa su éxito en la vulnerabilidad del factor humano, lo cual está teniendo un efecto devastador en la industria de pagos.

Esta formación tiene que ser continua y recurrente. Las amenazas evolucionan a una velocidad sorprendente y la capacitación del personal tiene que ir de la mano.

PROTECCIÓN DE LA INFORMACIÓN (ENCRIPTACIÓN)

La encriptación está ligada a la comunicación y constituye la principal herramienta de protección de información.

Una simple transformación de un texto, clave de cifrado mediante, convirtiéndolo en incomprensible para aquellos que no dispongan de la clave de descifrado. Garantizando que el texto solo será accesible para los agentes que quiera el emisor.

En el marco del departamento de tesorería, el volumen de información intercambiada con los bancos es elevado, estratégico y de máxima criticidad por el impacto que puede tener la vulneración de dicha información. SAP ofrece herramientas, en el propio ERP, para encriptar los ficheros de pago generados utilizando la funcionalidad de Secure, Store and Forward. Con un certificado y la utilización de librerías de cifrado estándar, estaremos en disposición de proteger la información intercambiada.

DOBLE FACTOR DE AUTENTIFICACIÓN

A la hora de aprobar una transacción financiera, se antoja necesario implementar un proceso de doble verificación que garantice la autenticidad de la persona que ejecuta la acción. SAP BCM, aparte de desplegar un circuito de aprobación acorde a la estrategia de apoderamiento de cada empresa, habilita la posibilidad de integrar durante el proceso de autorización un doble factor mediante token y smartcard a través del servicio SAP Authentication 365 o productos de terceros especializados en materia de seguridad.

SWIFT a través de su servicio 3SKey, ofrece la alternativa STP ("straight through processing") más segura: un token único para las entidades bancarias a través del cual establecer un doble factor, insertar firma digital e encriptación soportada por los bancos. Siendo los bancos los únicos poseedores de la clave de descifrado para convertir en claro la información de los ficheros de pago recibida.

CONCILIACIÓN TESORERA

Un aspecto que puede erigirse como fundamental en la rápida identificación de operaciones bajo sospecha, está en la correcta conciliación de las operaciones bancarias en nuestro ERP de SAP. Disponer de una herramienta que de forma automatizada nos facilite propuestas diarias de conciliación, repercutirá de forma positiva en diferentes ámbitos de la empresa (estados de origen y aplicación de fondos, cash application) y no en menor medida, puede contribuir a la rápida detección de anomalías, previniendo de futuras y recurrentes actuaciones de fraudulentas. Para alcanzar altas cuotas de conciliación en las cuentas transitorias de tesorería, CONVISTA dispone dentro del catálogo de soluciones de la Treasury Suite (CTS), una específica para ayudar a las compañías a alcanzar ratios de conciliación (matching) del 90%. Herramienta testada en clientes de muy diversa índole de negocio y avalada por los mismos.

Podemos concluir, que SAP ofrece mecanismos de protección en cada uno de los elementos clave en el marco de seguridad. Factores que permiten contrarrestar y agilizar la actuación del equipo de Tesorería, frente a los ataques de agentes externos e internos a la organización.