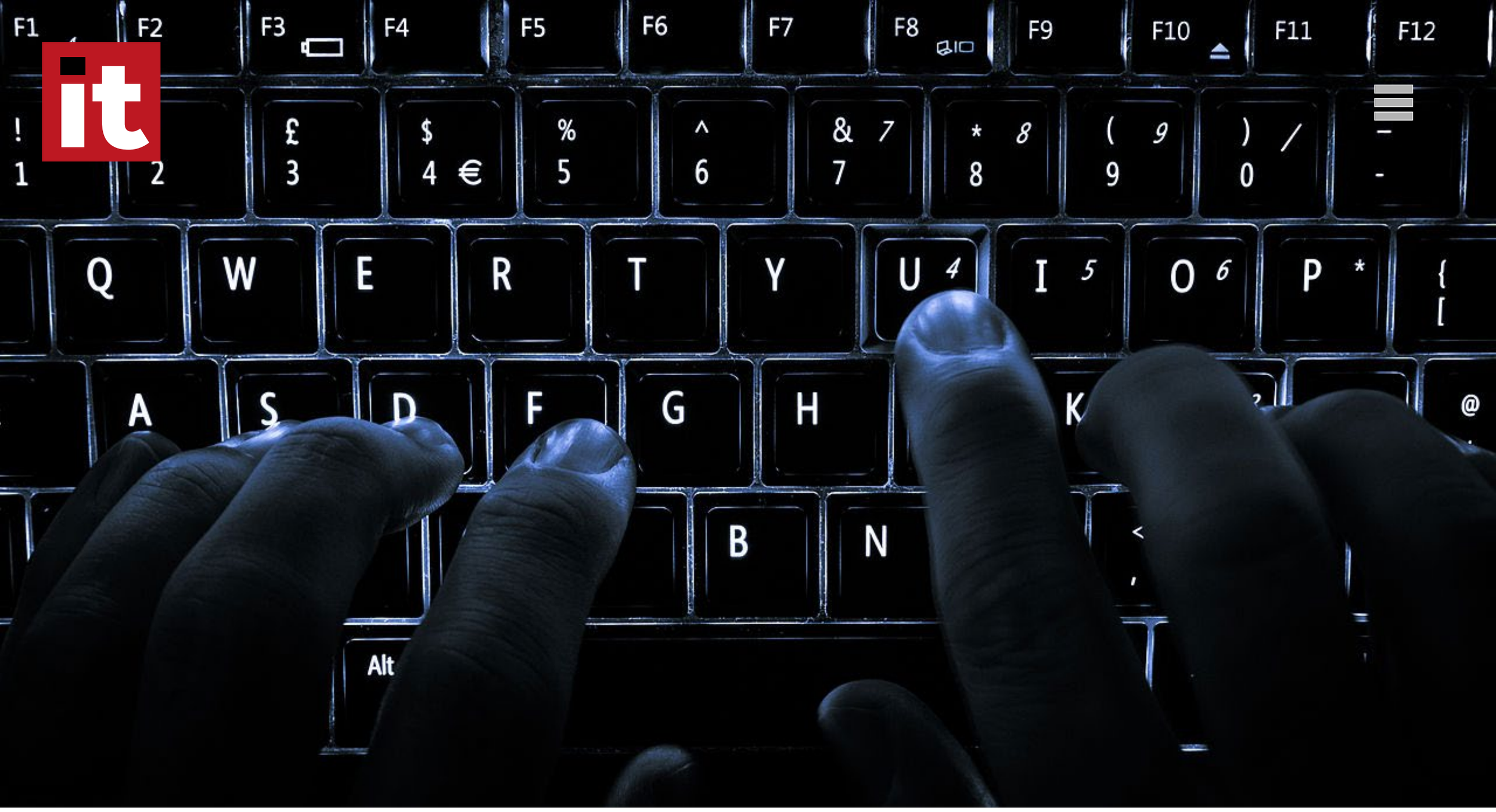


Los ATM **ante el reto de la** ciberseguridad

gmv
INNOVATING SOLUTIONS

Este es un documento producido por

www.ituser.es
www.itreseller.es

Accede a nuestras publicaciones digitales

CÓMO USAR ESTE DOCUMENTO

Con el fin de obtener la mejor experiencia de uso de esta revista, es **imprescindible** seguir estos sencillos pasos que te indicamos a continuación:

Paso 1. Asegúrate de disponer de las versiones más actualizadas de Adobe Reader y Flash Player. Si no las tienes instaladas, puedes descargarlas aquí:

Adobe Acrobat Reader y Adobe Flash Player

Paso 2. Accede al enlace de descarga y la publicación se abre en el visor del navegador.

Paso 3. Busca la opción guardar como que, dependiendo del navegador que utilices, podrá ser un icono o estar incluída en la barra de menú, y guarda la revista en la carpeta donde almacenes los documentos en tu equipo.

Paso 4. Accede a dicha carpeta y usa el botón derecho del ratón para hacer clic en el fichero de la revista.

Paso 5. Selecciona Adobe Reader como aplicación predeterminada para abrir este tipo de documentos.

Paso 6. Una vez abierta la revista, habilita la visualización a pantalla completa, y puedes iniciar la lectura de la revista con todas las capacidades interactivas disponibles.

Los ATM **ante el reto de la** ciberseguridad

En los últimos años los cajeros automáticos se han convertido en blanco de bandas criminales organizadas, las cuales utilizan a hackers para lograr penetrar en los sistemas y robar grandes sumas de dinero. Así lo explica GMV que destaca que la protección del propio cajero es la única forma efectiva de prevención.

La evolución que ha experimentado el cibercrimen llega a sectores que, hasta hace pocos años, eran poco propensos a sufrir robos a gran escala. Uno de estos sectores es el de los cajeros automáticos, unas "máquinas" que conceptualmente todo el mundo sabe cómo funcionan y cuyas técnicas de ataque perseguían, inicialmente, el robo de dinero en efectivo. Esta práctica criminal "tiene muchos años de vida", destaca Juan Jesús León Cobos, director de productos y nuevos desarrollos en GMV Secure e-Solutions. "Como es natural, con el paso del tiempo los ataques han evolucionado y han pasado de ser con fuerza, robar los propios cajeros o hacerlos explotar, a los ataques físicos más sutiles como extraer el dinero mediante pinzas especiales antes de completar la retirada de efectivo y después engañar al cajero para que no lo contabilice".

Aparte de los ataques dirigidos a obtener efectivo, a día de hoy el ataque a cajeros que la industria considera como más preocupante es el denominado skimming. Este ataque pretende obtener la información de la bandas magnéticas de las tarjetas, y si es posible el PIN, con objeto de clonar tarjetas falsas o realizar compras

Checker ATM Security

Clicar para ver el vídeo

CHECKER ATM SECURITY, LA SOLUCIÓN PARA PROTEGER LOS CAJEROS AUTOMÁTICOS DE CIBERATAQUES

Con una base instalada de más de 100.000 cajeros en 19 países, Checker ATM Security es una de las soluciones líderes del sector.

A grandes rasgos, este producto permite a las entidades financieras controlar el software que se ejecuta dentro de los cajeros automáticos de su red, de tal forma que sólo el software conocido y permitido por la entidad pueda ejecutarse dentro de la "máquina".

Y es que Checker ATM Security preserva el software de aplicaciones, las librerías y la integridad del sistema operativo, gracias a la utilización de firmas criptográficas y un disco duro cifrado que ha sido específicamente diseñado para su uso en cajeros automáticos.

¿Cómo se logra esto? A través de la utilización de "la tecnología más avanzada", la cual controla de manera efectiva los procesos "legítimos" y previene las infecciones del malware mediante la "protección exhaustiva" de lo que se conoce como "lista blanca".

Para ello, Checker ATM Security ha sido diseñada y desarrollada a medida para las plataformas de autoservicio financiero, permitiendo la administración centralizada de la seguridad (incluido el control de las aplicaciones en ejecución), la gestión de los recursos locales y remotos a los que se puede acceder desde la máquina o de las comunicaciones autorizadas.

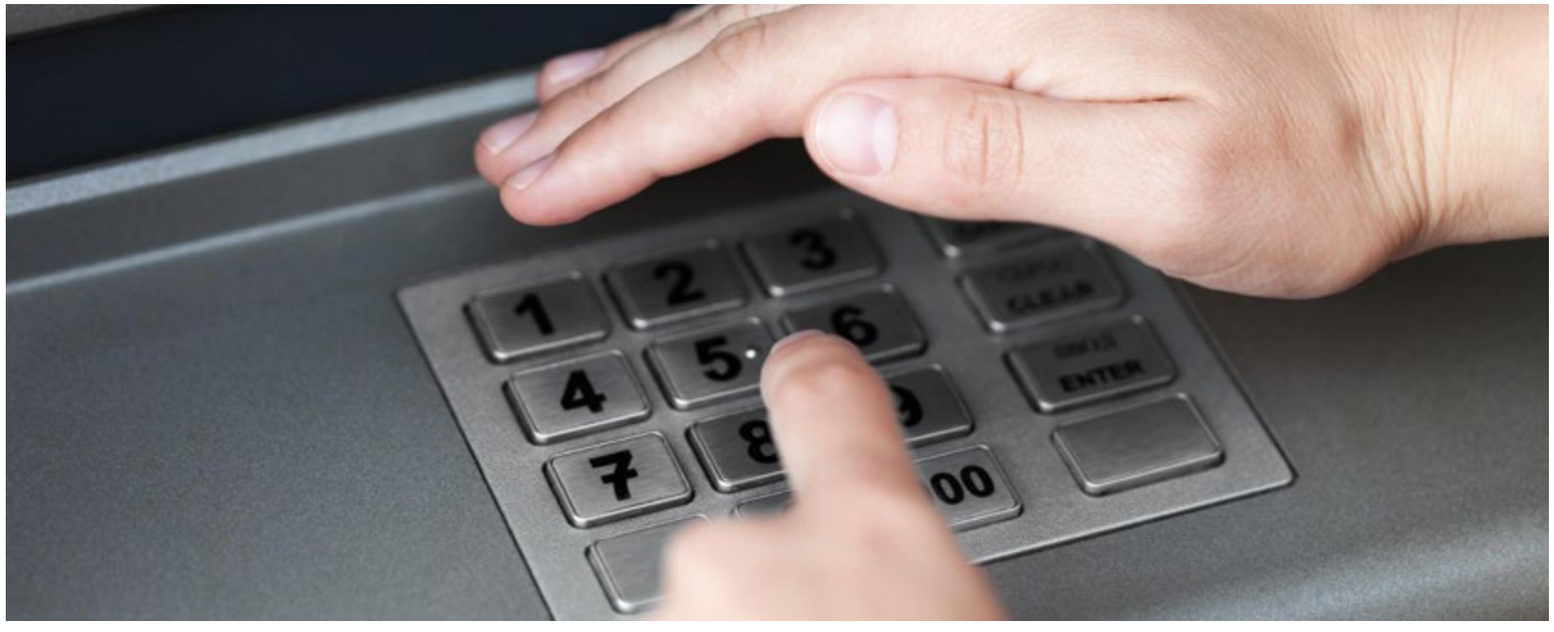
Mediante férreos controles de seguridad, asegura un entorno de alta protección, cortando en su origen cualquier infección causada por virus, troyanos, gusanos y otros programas maliciosos, y evitando también que cualquier software peligroso que se ejecute en el interior del cajero pueda acceder a sus recursos más sensibles.

fraudulentas por teléfono o por Internet. No obstante, y tal y como explica Juan Jesús León Cobos, "este tipo de amenaza está en decadencia" gracias a la irrupción de las tarjetas con chips.

Ataques lógicos

Conscientes de la importancia que puede suponer el robo a cajeros automáticos, los cibercriminales han evolucionado y ahora centran sus esfuerzos en los que se conoce como ataques lógicos. Básicamente, estos consisten en la utilización de dispositivos electrónicos externos, como pueden ser las llaves USB o un ordenador, y software malicioso para hacerse con el control de las máquinas.

Este método tiene el potencial de causar grandes pérdidas económicas como ya se ha demostrado en Asia, con los ataques al First Bank de Taiwán o el Goverment



Sólo la mitad de los 500.000 cajeros automáticos que están instalados en Europa Occidental cuentan con la protección adecuada contra ciberataques

Saving Bank de Tailandia. En estos dos casos “bandas criminales consiguieron penetrar en los sistemas informáticos del banco y desde allí introdujeron los programas maliciosos en los cajeros”.

A grandes rasgos, “esta nueva estrategia consigue infectar muchos cajeros a la vez, aumentando enormemente la cantidad robada a la vez que prescinde de la necesidad de infectar los cajeros físicamente uno a uno”, explica Juan Jesús León Cobos. “Los ciberataques pueden ahora proporcionar fácilmente varios millones de euros por banco atacado, y con un riesgo mucho menor”.

Sin embargo, “estos ataques requieren de las capacidades técnicas necesarias para hackear un banco, lo cual no está al alcance de cualquiera”.

Uno de los factores que han hecho que se extienda este tipo de ataques ha sido “la llegada de Windows” hace ya algunos años. La mayoría de los cajeros automáticos cuentan con el sistema operativo de Microsoft, lo que “ha facilitado la interoperabilidad” al “estandarizarse”, consiguiendo un ahorro de costes, pero posibilitando a cambio la aparición de nuevas amenazas.

¿Están las entidades protegidas?

Este tipo de ataques comenzaron en países de Latinoamérica y Europa del Este para, posteriormente, “trasladarse a Asia”. Desde hace “unos dos o tres años aproximadamente” se han producido casos en países de Europa Occidental como “el Reino Unido, Francia e, incluso, España”.

ACCIONES A ADOPTAR PARA MANTENER LOS ATM A SALVO

¿Qué acciones se pueden llevar a cabo para mantener protegida los cajeros automáticos? Juan Jesús León Cobos realiza una serie de recomendaciones.

- **Instalar un software específico** para protección de cajeros y operarlo adecuadamente.
- **Mantener la red de cajeros automáticos separada** de las demás redes corporativas.
- **Asegurarse de que cualquier servidor que se encuentra dentro de la red de cajeros automáticos está protegido,** cuenta con todos los parches de seguridad actualizados y se han llevado a cabo las pruebas pertinentes de seguridad.
- **Todo el software del cajero debe pasar un control de seguridad antes de ser instalado.** En la medida de lo posible, se deben evitar las actualizaciones automáticas, incluidas las del sistema operativo, que no reciban el visto bueno previo de los responsables de seguridad.

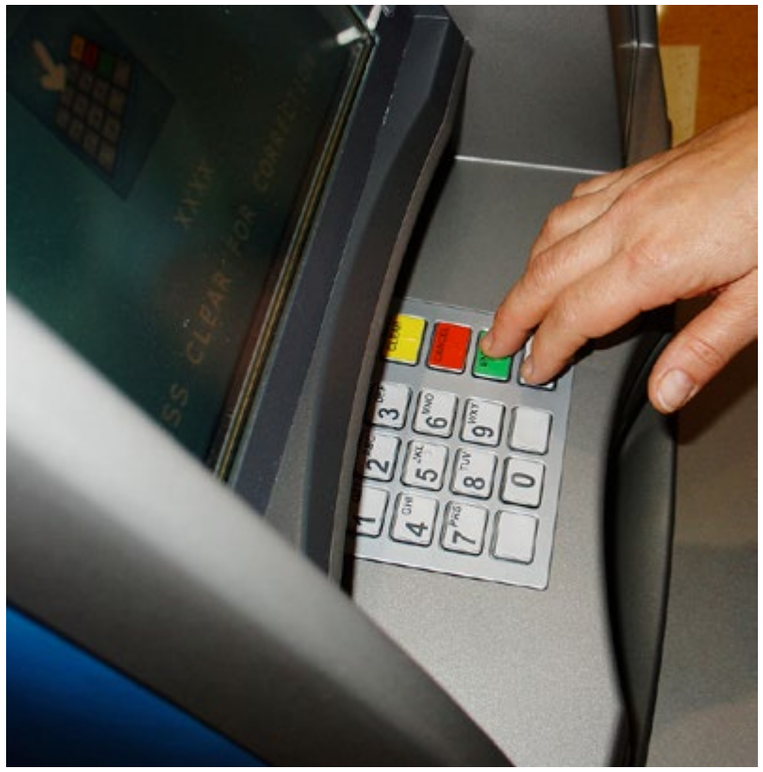
En la actualidad, y a nivel mundial, existen unos tres millones de cajeros, “de los que, aproximadamente, 500.000 se encuentran en Europa Occidental” y “sólo la mitad cuentan con la protección adecuada”.

No obstante, Juan Jesús León Cobos destaca que hay entidades que sí que han invertido en proteger sus cajeros automáticos para evitar problemas.

Dos han sido los factores que han hecho que los bancos hayan tomado conciencia. El primero, el fin del soporte para Windows XP. “La mayoría de los cajeros automáticos tenían este sistema operativo instalado. Cuando Microsoft anunció el fin del soporte, se comenzó con la migración a otras plataformas, sobre todo Windows 7, y se incrementó la inversión en seguridad”.

El segundo factor ha sido los ataques sufridos por otras entidades. “Los ataques a entidades bancarias de Asia dejaron patente la necesidad de que se incremente la cooperación entre los equipos de seguridad TI de las entidades financieras y los que se encargan de gestionar la seguridad de los ATM. Al comprobar que la amenaza era real, decidieron invertir en proteger sus sistemas y evitar ser víctimas de un ciberataque que, por otro lado, supondría además de una pérdida económica importante, un daño a su reputación e imagen”.

En el caso de España, Juan Jesús León Cobos reconoce que, a nivel general, las entidades financieras están bien protegidas. No obstante, asegura que, en algunos casos, el presupuesto es clave a la hora de proteger sus sistemas “y hasta hace poco tiempo tanto las entidades financieras españolas, como las europeas, han sufrido una crisis profunda”.



Tendencias

De cara al futuro, “los ataques a través de la red” serán protagonistas. Aunque todavía no son significativos, “esta técnica ya se ha comenzado a utilizar”.

Y es que, y tal y como explica Juan Jesús León Cobos, “los cibercriminales están muy bien organizados; son bandas internacionales cuyas técnicas se han sofisticado mucho”. Lograr “hackear un banco europeo” puede suponer millones de euros “y la coordinación no es tan complicada como era antes”.

Cómo prevenir los ataques

¿Cómo se puede prevenir estos ciberataques? “A través de la instalación de programas de seguridad en los propios cajeros”, explica Juan Jesús León Cobos. “Los casos de ataques con éxito mencionados antes tienen en común que sus cajeros no contaban con la protección adecuada”.

GMV lleva diez años protegiendo cajeros de estos ataques mediante su producto Checker ATM Security. “Este programa, diseñado y construido con tecnología 100% española, protege en este momento más de 100.000 cajeros en una veintena de países en todo el mundo y es posiblemente el producto más avanzado que un banco puede adquirir hoy en día para estar a salvo de ciberataques”.

Juan Jesús León Cobos finaliza recordado a las entidades financieras la necesidad de entender a qué se enfrentan. “Las organizaciones criminales son capaces de coordinar decenas de robos de dinero en cuestión de minutos”. El potencial de las amenazas lógicas “es enorme”, al igual que los beneficios que pueden obtener los cibercriminales. Por eso es clave proteger de la mejor manera los cajeros automáticos.

Enlaces relacionados

- Estrategia de GMV para este año
- Productos de GMV para proteger los cajeros automáticos
- Aumentar la seguridad de la banca, objetivo de GMV y el proyecto Trespass
- GMV extiende a América Latina su solución de seguridad para cajeros