Seguridad en los cajeros automáticos

FUJITSU

shaping tomorrow with you

CONTENIDO

Capítulo 1

Antecedentes y situación del sector

Desde que el primer cajero empezó a operar en 1967, su incorporación ha sido exponencial, llegando a la cifra actual de más de 3 millones de cajeros instalados en todo el mundo. Durante todo este tiempo, se han convertido en el punto de contacto más cercano del banco con sus clientes, tanto por la posibilidad de expedir efectivo, como los múltiples nuevos servicios que pueden realizarse desde estos terminales. Por todo ello, se han convertido en **el principal foco** de los delincuentes para el **ataque a las entidades financieras**.

Los ataques a cajeros automáticos van aumentando año a año en todas las regiones, y no solo los ataques físicos más tradicionales (gases explosivos, lanzas térmicas, levantamiento de cajeros,...) sino en los ataques lógicos y de fraude, que cada vez son más sofisticados, llegando a ser orquestados desde el exterior y ejecutándose al mismo tiempo desde diferentes localizaciones, provocando la **pérdida de enormes cantidades de efectivo** en pocos minutos.

Cibercrimen en Europa

El año 2016 ha sido el año en el que más ataques a cajeros se han producido, solo **en Europa se han incrementado un 30%** respecto a años anteriores, y la cifra va en aumento. Esto, unido a la transformación que está viviendo el sector financiero hacia el entorno digital, nacen nuevos riesgos, que dan lugar a nuevas necesidades en materia de seguridad. Aplicar exhaustivos y avanzados controles permitirá reducir los riesgos, manteniendo seguros a las propias entidades y a sus usuarios.

European ATM Crime Statistics - Summary

ATM Related Fraud Attacks	H1 2012	H1 2013	H1 2014	H1 2015	H1 2016	% +/- 15/16
Total reported Incidents	9,595	12,676	7,345	8,421	10,820	+28%
Total reported losses	€131m	€124m	€132m	€156m	€174m	+12%
ATM Related Physical Attacks	**H1 2012**	**H1 2013**	**H1 2014**	**H1 2015**	**H1 2016**	**% +/- 15/16**
Total reported Incidents	968	1,007	1,032	1,232	1,604	+30%
Total reported losses	€8m	€10m	€13m	€26m	€27m	+3%

Estadística de ataques a cajeros en Europa

Cibercrimen en América Latina

Según cifras publicadas, **el cibercrimen costó el año pasado a América Latina $ 90 mil millones** del total de $ 575 mil millones globales, el 0,5% del GDP mundial (PIB). El impacto en México asciende hasta los $ 5 mil millones al año, solo superado por los $ 8 mil millones de Brasil. Se estima un crecimiento del impacto del cibercrimen en todo el mundo de hasta $ 6 billones en 2021.

Un estudio de la Council of the Americas cita que el 50% de las empresas en América Latina sufrieron ataques Malware en 2013. Creciendo a más del 87% en 2016 en brechas de seguridad.

Se estima que el 31% de los usuarios no se sienten seguros utilizando los ATMs. En 2013 fue detectado el Malware Ploutus en México. Desde entonces se estima que la banca mundial ha perdido en torno a los $ 450 millones con esta infección. Cada ataque dirigido a un ATM ocasiona de media una pérdida de $ 50,000.

Tras el ataque por parte del grupo criminal **Cobalt** en verano de 2016 en Tailandia, en el que mediante Malware transmitido a través de la red bancaria interna se sustrajeron $ 3 millones, la seguridad para los cajeros se debe extender a la propia red de la sucursal y a las redes corporativas, además de nuevas políticas de seguridad para aplicar a los puestos de trabajo y a los propios empleados. En este ataque, y para evitar mayores pérdidas, debió dejarse sin servicio la mitad del parque de ATMs y se tardó más de dos semanas en aplicar una solución definitiva, con el consiguiente impacto económico. Este ha sido el mayor ataque en la historia de los cajeros automáticos, ya que se ha saltado al siguiente nivel de complejidad para poder atacar un gran número de máquinas de forma simultánea y remota. Meses más tarde volvió a repetirse en varios países de Europa. Se prevé que no será el último de este tipo y envergadura.

Fujitsu y la seguridad de los ATMs

Este White Paper se fundamenta en la base de conocimiento de **Fujitsu** en materia de seguridad de ATMs y pretende ser una guía de las mejores prácticas en dicha materia. En él se describen los principales vectores de ataque que se concentran en las siguientes tres categorías:

- **Fraude:** Ataques destinados a la suplantación del usuario mediante el robo de datos.
- **Ataques físicos:** Ataques que tienen como objetivo robar el efectivo disponible en el cajero.
- **Ataques lógicos:** Ataques para hacerse con el control del cajero o interceptar información del usuario.

Es imprescindible el conocimiento de los mismos para establecer mecanismos y respuestas de actuación ante las diferentes amenazas de seguridad existentes.

Los productos y servicios de Fujitsu, asociados a una metodología de análisis, favorecen los controles que permiten reducir y mitigar el riesgo asociado y disponer de alta capacidad de resiliencia y continuidad del negocio.

Capítulo 2

Fraude

Se refieren a ataques destinados a la **suplantación del usuario**, mediante la obtención fraudulenta de los datos, de su tarjeta bancaria y sus claves personales.

Observación del PIN de seguridad antes de la sustracción de la tarjeta

Vectores principales del ataque

Los ataques conocidos como "**skimming**" son los más comunes, su finalidad es clonar o reproducir los datos de la tarjeta de crédito y suelen ir acompañados por la captura del PIN del usuario mediante mecanismos de espía, cámaras, etc.

A continuación se exponen brevemente los vectores más extendidos de este ataque:

- **Copiado de los datos de la tarjeta bancaria de usuario**:
  - Lectura fraudulenta y copia de los datos de la banda magnética o skimming:
    - **Falsa embocadura**. Sustitución o recubrimiento de la embocadura real del lector de tarjeta en el frontal por una imitación que incluye en su interior los mecanismos de lectura y grabación de los datos de las tarjetas de usuario.
    - **Lector externo** en miniatura superpuesto en la zona de paso de la banda magnética de la tarjeta, bien en el frontal sobre la embocadura exterior, o bien en la misma boca de entrada del propio lector.
    - **Falso lector interno** o "Deep Skimming". En este caso el falso lector se ubica en el interior de la unidad, en algún punto del recorrido de la banda dentro de la misma, evitando que sean efectivas las medidas de detección externas.
    - **Differential Skimming** (o Stereo Skimming): Dos skimmers o lectores de banda sobre una falsa boca superpuesta para neutralizar la eficacia de embocaduras antiskimming que utilizan el jamming o señal inhibidora.
  - Pinchado de los datos leídos por unidad de tarjeta o "**Eavesdropping**", es decir, interceptar los datos recibidos por la lectora legítima. Esta lectura se puede producir de dos formas:
    - Destructiva: Copiado de banda mediante acceso a la unidad a través de ventana practicada en el frontal, e intercepción de los mismos en algún punto interno del lector.

  - No destructiva: Implica el acceso al interior del cajero y a la conectividad de la unidad lectora de tarjeta donde son interceptados los datos.
- Captura de los datos intercambiados entre el lector de chip y la tarjeta o "**Shimming**":
  - Falso lector intercalado entre la tarjeta y el lector de chip. Colocación de un dispositivo fraudulento en el interior del lector de tarjeta, en concreto ubicado en la zona de lectura del chip, que intercepta el flujo de información entre lector de chip y la tarjeta, almacenando los datos intercambiados.

■ **Captura de la tarjeta de usuario**.
- "Card trapping o card fishing".
  - Estas técnicas, representadas entre otras por el denominado "**lazo libanés**", persiguen atrapar la tarjeta que es introducida por el usuario en el lector de tarjeta, haciendo imposible su recuperación por el mismo. Una vez que el usuario se marcha del cajero, el ladrón consigue extraer la tarjeta del lector, procediendo a su duplicado o uso fraudulento de la misma.

■ **Obtención de las claves de usuario**.

Todas las técnicas anteriores, no serían completamente útiles sin la obtención del PIN, "Personal Identification Number", asociado a la tarjeta de usuario.

Las técnicas más habituales usadas para ello son las siguientes:
- Colocación de una micro-cámara oculta orientada al teclado de usuario.
  - Técnicas de añadido o sustitución de algún elemento del frontal, embellecedor, panel luminoso, etc. por otro equivalente, que integra mecanismos de grabación y/o transmisión.
- Observación distraída por terceras personas del PIN del usuario
- Colocación de un falso teclado superpuesto al actual.

Contramedidas contra el fraude

Tanto los fabricantes como el mercado evolucionan al compás de la aparición de nuevas técnicas de fraude.

A continuación se enumeran las medidas contra el fraude más extendidas en el mercado:

■ **Protección contra el copiado de los datos de la tarjeta de usuario.**
- **Medidas pasivas**:
  - Embocaduras con diseños especiales, que limitan la colocación de skimmers, sin afectar a la capacidad del usuario de introducción o recogida de la tarjeta.
  - Aquí también podrían encajar soluciones en las que se cambia el modo en el que el usuario introduce la tarjeta en la unidad, ayudado en la mayoría de los casos por una guía externa.
  - En este grupo se incluirían también pequeñas placas diseñadas para minimizar la ubicación de skimmers en el interior de la unidad, en zonas de recorrido de banda. Esta solución también es eficaz contra los ataques tipo "shimming", aunque en este sentido la mejor recomendación es la certificación EMV de los lectores.
- **Medidas pasivas con reporting**:
  - Embocaduras dotadas de barreras que limitan la colocación de skimmers, siendo requerido su vandalismo para ser sobrepasadas, lo que implica informar y/o bloquear el lector para impedir la entrada de tarjetas.
  - Sensores de perforación, vibración, etc., capaces de detectar y reportar ataques físicos contra el frontal en la zona ligada al lector de tarjetas, eficaces contra el eavesdropping.
- **Medidas activas sin reporting**: Son capaces de interferir en la capacidad de grabación de lectores externos fraudulentos.
  - Dispositivos inhibidores o "jamming".
  - "**Jitter**" o movimiento aleatorio de avance y retroceso de la tarjeta durante la entrada y salida en la unidad lectora del cajero.
- **Medidas activas con detección y reporting**, ligadas a la colocación alrededor de la embocadura o por la parte posterior del frontal de elementos que son capaces de detectar cambios temporales en las condiciones de la misma que pueden resultar sospechosos.

■ **Medidas contra la captura de la tarjeta de usuario**.
- **Medidas físicas**.
  - Exteriores a la unidad lectora, como embocaduras diseñadas para limitar las posibilidades de introducción en el lector de objetos para bloqueo de la tarjeta de usuario.
  - Interiores a la unidad lectora, como el disparo controlado por la unidad de una barrera que retiene la tarjeta en la unidad ante la detección de comportamiento sospechoso de la tarjeta en su interior.
- **Medidas lógicas**.
  - Encaminadas a la realización de movimientos preventivos de la tarjeta dentro de la unidad, y a evitar que el usuario pueda introducir su PIN en caso de detección de elementos extraños en la misma.
  - Ligadas a la gestión de la información que la unidad es capaz de reportar, previo y durante el movimiento de una tarjeta dentro de la unidad.

■ **Contramedidas contra la obtención de las claves de usuario**.
- El uso de teclados, conforme a las certificaciones PCI, para evitar acceso a la información almacenada en el teclado.
- Barreras de protección a la observación de la entrada del PIN en el teclado -"Pin Shield"-.
- Pantallas con filtro de privacidad que limiten la visibilidad de la información en pantalla a terceros.
- Integraciones especiales de los teclados en el frontal que limiten la posibilidad de superposición de teclados falsos.
- Sensores de detección de retirada de teclado o mesa del cajero.
- Colocación de espejos o videocámara a modo espejo que permita al usuario la detección a su alrededor de situaciones anómalas o de observación por terceros.
- Uso de soluciones de biometría, como las soluciones **PalmSecure de Fujitsu**.

Capítulo 3

Nivel Lógico

Los ataques lógicos se están convirtiendo en la actualidad en el método más preocupante y creciente, con el potencial de causar pérdidas de grandes cantidades. En este tipo de ataque se hace uso de dispositivos electrónicos externos o software malicioso. Las herramientas se utilizan para tomar el control lógico del dispensador automático y así conseguir retirar elevadas cantidades de dinero, lo que en el mundo del ATM se conoce como "**cash-out**" o "**jackpotting**".

Todos estos nuevos métodos argumentan la necesidad de proteger el entorno de los ATMs frente a ciberataques.

Los ataques más peligrosos se ejecutan de forma remota

Principales vectores de ataque

Las tres áreas principales para mantener la seguridad lógica de un cajero son:

- Seguridad a nivel de red.
- Seguridad a nivel de sistema operativo (memoria, procesos, registro, recursos).
- Seguridad a nivel de aplicaciones que realizan la comunicación entre el host y los dispositivos del cajero.
  - **Red:**
    - Comunicación entre los dispositivos del cajero y el host del cajero.
    - Dispositivos de red como routers y switches pueden ser objetivos de un ataque.
  - **Sistema operativo:**
    - Vulnerabilidades zero day (desconocidas por la comunidad y los fabricantes).
    - Vulnerabilidades conocidas en sistemas operativos que no tienen soporte (Windows XP).
  - **Software:**
    - Software de control de módulos de cajero automático.
    - Software utilizado para interactuar con el usuario (ya sea cliente o el operador de ATM).
    - Software utilizado para la comunicación con el centro de proceso de datos y realizar la transacción.
    - XFS (eXtensions for Financial Services) es un estándar que proporciona una arquitectura cliente-servidor para la comunicación de aplicaciones financieras con los dispositivos de cajeros automáticos en la plataforma Windows.

Contramedidas de seguridad lógica

Las medidas para mantener la seguridad lógica, los sistemas o herramientas propuestos por Fujitsu son:

- **Sistemas de seguridad de punto final (End Points)**: Los nuevos sistemas de protección para puntos finales son clave en la prevención, detección y remediación de ciberataques en nuestros sistemas. Pueden incluir todas estas opciones y herramientas:
  - **Firewall:** Controla el tráfico de red y bloquea posible malware antes de que se expanda a nuestros sistemas.
  - **Antivirus**: Analiza y erradica el malware que llega a los sistemas.
  - **Sistemas de análisis de comportamientos**: Bloquea archivos que demuestran un comportamiento sospechoso de ser malicioso.
  - **Sistemas de eliminación de malware:** Remediación/ eliminación persistente de infecciones complejas de eliminar.
  - **Control de aplicaciones**: Herramientas de monitorización y control de comportamientos de procesos y aplicaciones con sistemas de bloqueo automático usando listas blancas y negras.
  - **Control de dispositivos**: Bloqueo de infecciones de dispositivos externos (por ejemplo USB) previniendo infecciones y la sustracción o alteración de datos.
  - **Control de integridad de sistemas**: Facilidad para detectar modificaciones no autorizadas sobre archivos.
  - **Machine Learning** (aprendizaje automático): Técnicas de detección previa a la ejecución de posibles amenazas desconocidas o variantes/mutaciones de amenazas conocidas. Eficaz sobre amenazas de zero day, es decir, nuevas amenazas.
  - **Técnicas de emulación**: Técnicas anti evasión para la detección de amenazas ocultas, emulando comportamientos para facilitar la toma de decisión.
- **Firewall a nivel de host:** además de los firewalls perimetrales para el entorno de cajeros, es muy recomendable instalar firewall integrado a nivel de host (en los propios cajeros) para monitorizar, analizar y bloquear/permitir las comunicaciones desde o hacia el cajero.
- **Control de aplicaciones**: utilizar un software de bastionado, con funciones IDS e IPS, que monitorice y solo permita la ejecución de aplicaciones conocidas (lista blanca), y bloquee el resto de aplicaciones no autorizadas (lista negra) para proteger:
  - Procesos o aplicaciones activos en el sistema.
  - Accesos y modificaciones sobre ficheros de los sistemas.
  - Accesos hacia/desde diferentes redes internas o externas del banco.
  - Utilización y accesos a las zonas de memoria de otras aplicaciones o procesos.
  - Utilización de dispositivos externos.
  - Eventos registrados del sistema operativo.
- **Sistemas de Sanboxing**: sistemas de "sandboxing" o entornos de ejecución aislados, de tal forma que todo proceso que se ejecuta en el sistema es aislado en un entorno de ejecución donde se limita el acceso al sistema (acceso a infraestructura de comunicaciones, ficheros de sistema, zonas de memoria de otras aplicaciones, dispositivos conectados al sistema) y se analiza su comportamiento.
- **Sistemas de VirtualPatching**: Sistemas que permiten, en tiempos muy cortos, el parcheo virtual del sistema operativo y aplicaciones. Esta característica permite:
  - Reducir la necesidad de actualizar a nivel de parches de seguridad, en las aplicaciones o en el sistema operativo. Estas aplicaciones suelen ejecutarse en un entorno aislado. Aun siendo vulneradas, no podrán salir de su entorno de ejecución.
  - Aumentar los intervalos de mantenimiento.
  - Minimizar el riesgo de los sistemas legacy que ya no disponen de mantenimiento y soporte del fabricante (ejemplo: WindowsXP).
- **Sistemas de Encriptado del disco duro**: algunos ataques lógicos evitan la protección de seguridad, arrancando el cajero por algún medio alternativo como puede ser una unidad de dispositivos USB o CD-ROM. Esta solución evitaría la amenaza de acceder al disco duro e infectarlo con software malicioso.
- **IAM o gestión de identidades**: Los sistemas IAM permiten la gestión para iniciar, capturar, registrar y gestionar identidades de los usuarios y sus privilegios de acceso de forma automatizada. Garantizan que los privilegios de acceso se conceden de acuerdo con una política de control de acceso para que los usuarios y los servicios estén debidamente autenticados, autorizados y auditados. Estos sistemas ayudan a mitigar las amenazas procedentes de los técnicos de cajeros, personal de oficinas y empresas de transporte de fondos, lo que robustece los despliegues, tanto de infraestructuras de los cajeros como de cambios en los desarrollos propios del banco al registrar todos los accesos y acciones llevados a cabo.
- **SIEM**: Sistema para facilitar la recolección, almacenamiento, correlación y análisis de la información de multitud de registros de una gama de sistemas de seguridad. Estas herramientas proporcionan componentes básicos para la prevención, detección y remediación de incidentes de seguridad, así como análisis retrospectivos para apoyar investigaciones de seguridad y análisis forenses. Estos sistemas también ayudan al cumplimiento de la regulación de seguridad (incluyendo PCI DSS y Guía de Buenas Prácticas de la CESG 13).

Capítulo 4

Nivel Físico

Este tipo de ataques afectan a la **integridad física** del cajero, llegando incluso a provocar daños importantes en las infraestructuras donde está ubicado, así como a las personas.

El enfoque tradicional de protección se centra en evitar el acceso indebido a los elementos que almacenan el efectivo, pero el aumento de los ataques de tipo lógico requieren una mayor protección de acceso a la zona "no segura" del cajero.

Apertura de ATM mediante fuerza bruta

Vectores principales del ataque

- **Utilización de la violencia o fuerza extrema para el acceso al efectivo de la caja fuerte**.
  - Intento violento de acceso mediante el uso de herramientas estándar.
  - Ataques orientados a reventar la caja fuerte mediante explosivo o gas.
  - Levantamiento o arranque del cajero de su lugar de fijación.
- **Ocultación o manipulación desde el exterior de los módulos de dispensación**.
  - Colocación de falsas bocas en el dispensador de efectivo.
  - Apertura fraudulenta del shutter para colocación de elementos que atrapen el efectivo en el interior de la unidad.
- **Acceso no autorizado a las unidades de efectivo o cajetines de dispensación**.
  - Apertura no autorizada de la puerta de la caja fuerte.
  - Acceso no autorizado al efectivo.
- **Acceso a la zona no segura del cajero**.
  - Apertura fraudulenta, violenta, u olvido intencionado del bloqueo del frontal del cajero.
  - Perdida, robo o copiado de llave de la puerta de acceso a la zona no segura.
  - Interceptación de las comunicaciones del dispensador con el controlador del cajero. **Black Box**.
    - Tras acceder al interior del cajero, se conecta un elemento electrónico ("caja negra") que envía comandos al dispensador para que entregue dinero, liberándose de la necesidad de una tarjeta o autorización para la transacción.

- En este tipo de ataque, interceptan comúnmente las interfaces USB o RS232 de la lectora de tarjetas, pinpad o la dispensadora de dinero, utilizando un sniffer de hardware. Los bits capturados desde/hacia la dispensadora son replicados para así obtener el dinero.

Estrategias de defensa

- **Utilización de la violencia o fuerza extrema para el acceso al efectivo de la caja fuerte**.
  - Contra el intento violento de acceso con utilización de herramientas estándar.
    - Uso de cajas fuertes con grados de resistencia conforme a los estándares que lo regulan (Ej. EN-1143-1), certificadas por los laboratorios autorizados no solo a nivel de ensayo, sino también de control de la producción.
    - Inclusión de cerraduras de combinación electrónica y llave, conformes al grado de seguridad requerido.
    - Utilización de detectores de vibración en el interior de las cajas para la detección de esta serie de situaciones.
    - Sistemas anticuña, para evitar el desmontaje de la puerta de la caja fuerte.
    - Bulones de diámetro y longitud adecuados al grado de seguridad requerido.
  - Ataques orientados a reventar la caja fuerte mediante explosivo o gas.
    - Contramedidas para la detección del gas y en su caso a la neutralización o disuasión (humo, sirenas).
    - **Sistemas de entintado de billetes**, que inhabilitan los mismos para su uso.
    - Barreras que impiden la extracción de la unidad de billetes, aunque se tenga acceso al interior de la caja fuerte.
    - Detección de superación del nivel de temperatura en el interior de la caja para ataques con lanza térmica.
  - Levantamiento del cajero de su lugar de fijación.
    - Puntos de anclaje, adecuados en resistencia, número y ubicación.
    - Peanas certificadas conforme a la normativa exigible.
    - Mecanismos de detección de intento de levantamiento de cajero.

- **Ocultación o manipulación desde el exterior de los módulos de dispensación**.
  - Colocación de falsas bocas en el dispensador de efectivo.
    - Diseño de mecanismos asociados al frontal que impidan la colocación de falsas bocas.
    - Modificación de las embocaduras o trampillas de protección de acceso a las unidades de dispensación, que interfieran durante su apertura con los "cepos" y eviten que prosiga la emisión del efectivo hacia el usuario.
  - Apertura fraudulenta del shutter para colocación de elementos que atrapen el efectivo en el interior de la unidad.
    - Utilización de sensores que detecten la apertura de las trampillas de protección de acceso a las unidades de dispensación fuera de tiempo.

- **Acceso no autorizado a las unidades de efectivo o cajetines de dispensación**.
  - Apertura no autorizada de la puerta de la caja fuerte.
    - Cerraduras con ventanas programación variables.
    - Dispositivos de detección de apertura y cierre de la puerta de la caja fuerte.
    - Detección de bloqueo del cierre de la puerta de la caja fuerte.
    - Control de acceso al interior de la caja de mecanismos de la puerta de apertura la caja fuerte.
  - Acceso no autorizado al efectivo.
    - Cámaras de seguridad integradas en cajero y/o en el habitáculo, orientadas hacia las unidades de efectivo.
    - Detección de extracción de la unidad de su zona de reposo.
    - Detección de apertura de módulos del dispensador.
    - Detección de retirada del cajetín de efectivo.
    - Control de apertura del cajetín de efectivo.

- **Acceso a la zona no segura del cajero**.
  - Apertura fraudulenta, violenta, u olvido intencionado del bloqueo del frontal del cajero.
    - Sensores de detección de apertura/cierre frontal y puertas del cajero.
    - Sensores de frontal y puerta bloqueada.
    - Sensores de vibración o rotura asociados al frontal ante ataque violento.
  - Perdida, robo o copiado de llave de la puerta de acceso a la zona no segura.
    - Cerraduras con llave de seguridad.
    - Cerraduras electrónicas con gestión de claves.
  - Interceptación de las comunicaciones del dispensador con el controlador del cajero. Black Box.
    - Comunicaciones encriptadas entre dispensador y controlador.
    - Autenticación entre dispensador y controlador.
    - Añadir distintos niveles de seguridad de cara a modificar dicha autenticación.

Como medidas complementarias a todas las anteriores, está la integración de micro-cámaras en distintas partes del frontal del ATM, (teniendo en consideración las restricciones ligadas a la protección de datos personales), que permitan no solo identificar al usuario, sino reconocer el modus operandi seguido en la manipulación de los equipos.

Capítulo 5

Fujitsu y la seguridad de ATMs

Fujitsu es la compañía japonesa líder en Tecnologías de la Información y Comunicaciones (TIC), con una gama completa de productos, soluciones y servicios tecnológicos para satisfacer la demanda de sus clientes en 170 países de los cinco continentes.

Una de sus principales líneas de negocio es el canal de autoservicio para la banca, proporcionando una solución completa y única que abarca desde la fabricación del propio ATM, el desarrollo de software o los servicios más avanzados como la gestión integral de la infraestructura completa de ATMs o servicios de Business Analytics, poniendo principal foco en la seguridad de los mismos.

FUJITSU ATM Serie 100

Soluciones en Terminales de Autoservicio

Fujitsu dispone de un amplio abanico de soluciones orientadas a cubrir los distintos vectores de ataque, tanto en lo relacionado con el fraude, como a nivel físico y nivel lógico.

Con relación a la seguridad de copia, captura de la tarjeta o claves de usuario, Fujitsu ofrece:

- Lectores de tarjeta certificados EMV, así como teclados pin-pad de usuario con certificación PCI PTS (incluyendo mecanismos de carga remota de claves RKL).
- Embocaduras anti-skimming pasivas y con capacidad de reportar vandalismos que limitan la colocación de dispositivos de copia en el exterior, como su introducción en la unidad de tarjeta. También minimizan la entrada de elementos fraudulentos orientados al robo de la tarjeta de usuario.
- Funcionalidades de "Jamming", "Jitter" y disparo de "antifishing" físico en los lectores de tarjeta.
- Soluciones de Pin Shield para la privacidad de la entrada del pin de usuario, y teclados con teclas integrados a través de la mesa que dificultan la colocación de falsos teclados.
- Lector de las venas de la mano o de la huella dactilar como soluciones de biometría para completar los mecanismos de identificación del usuario ante el cajero.

Respecto a la protección de acceso al efectivo del cajero, Fujitsu dispone de:

- Cajas fuertes con distintos grados de resistencia (CEN-IV, CEN-III, etc.), conforme a la normativa de seguridad EN-1143-1.
- Cerraduras de combinación electrónica estándar y con conectividad IP, certificadas con nivel de seguridad VDS-Clase 2, y la capacidad de realizar integraciones de soluciones específicas a requerimientos de nuestros clientes.

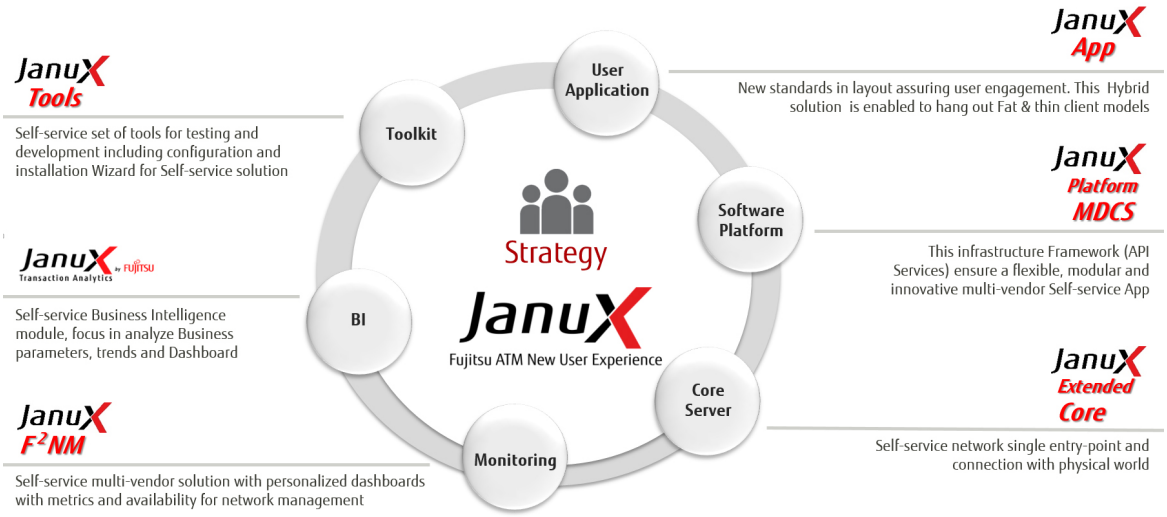
- Mecanismos de seguridad de serie en nuestras cajas fuertes como sistemas anti-cuña, bulones en los cuatros laterales de la puerta de la caja fuerte.
- Sensores sísmicos de grado 3 de seguridad con tester remoto y sensor de temperatura para detección de ataques con lanza térmica.
- Sistema de detección de presencia de gas que tienden a la neutralización del mismo, con objeto de evitar o minimizar la posibilidad de explosión, y que puede ser combinado con soluciones también disponibles de entintado para las unidades de dispensación y aceptación de efectivo.
- Soluciones de barrera (Protection Barrier) con llave de seguridad y anclaje a la caja fuerte, que son capaces de resistir la explosión y la desaparición de la puerta de la caja, impidiendo el acceso a la unidad de billetes.
- Las cajas fuertes de los cajeros Fujitsu incluyen 4 puntos de anclaje al suelo o anclaje a peanas certificadas con grado IV de seguridad clase IV.
- Sensores de levantamiento del cajero "Ram Raid" que pueden ser incorporados a la base de la caja fuerte, con capacidad de detectar y reportar tanto el sabotaje del sistema, como el desprendimiento del cajero.
- Embocaduras anticepo en el dispensador de efectivo y detección de apertura fraudulenta del shutter del frontal.
- Las comunicaciones entre dispensador y controlador se realizan en modo encriptado y con requerimientos de autenticación muy exigentes a nivel físico.
- Sensores de detección de apertura/cierre y bloqueo de la puerta de la caja fuerte para reportar tanto a la aplicación, como a la regleta de alarmas de la oficina.
- Precinto anti-manipulación de detección de acceso a la caja de mecanismos del interior de la puerta de la caja fuerte.
- Detección de retirada de la unidad dispensadora, de cajetín y de protección de acceso al mismo mediante cerraduras de llave y de activación del sistema de entintado ante manipulación del mismo.

En cuanto a la protección de acceso a la zona no segura del cajero, Fujitsu incorpora a sus equipos:

- Mecanismos de bloqueo de frontal son sensores de detección de apertura, tanto magnéticos grado 3, como mecánicos, para reportar tanto a la centralita de alarmas como a la aplicación.
- Cerradura de seguridad para acceso al interior del cabinet.
- Elementos de protección de acceso a los puertos delcontrolador del cajero.

Fujitsu dispone de una suite completa de aplicaciones y soluciones de gestión y monitorización de cajeros, que cubre toda la torre de software instalada en los ATMs.

- **JanuX** F²NM: módulo de monitorización para múltiples proveedores con diferentes paneles de control personalizables que muestran en tiempo real todas las alertas y métricas de la infraestructura completa. La generación de alertas en base a patrones predefinidos permiten la identificación de un posible ataque de forma inmediata.
- **JanuX Analytics**: Módulos de Business Intelligence con foco en analizar las tendencias del canal de autoservicio y realización de predicciones. Este módulo previene la detección de diferentes ataques y fraudes no detectados por las monitorizaciones tradicionales.
- **JanuX Tools**: Conjunto de herramientas para facilitar y mejorar la gestión de las fases de desarrollo y pruebas.
- **JanuX App**: Aplicación de usuario, con nuevos estándares de diseño que garantizan la participación de los mismos. Esta solución híbrida está habilitada para su utilización en múltiples dispositivos.
- **JanuX Platform MDCS**: Es una Plataforma de Software. Este Framework de infraestructura (API Services) garantiza una aplicación de autoservicio de múltiples proveedores flexible, modular e innovadora.
- **JanuX Extended Core**: Que proporciona un framework adicional de servicios, incluyendo un portal de autoservicio.



Gestión de Redes de Autoservicio

Todos los elementos de seguridad instalados en los cajeros pierden efectividad si no se implementa un servicio efectivo de monitorización, que recopile todos los datos en tiempo real y notifique las alertas para poder proporcionar una rápida respuesta ante cualquier ataque y frustrarlo.

Desde su Centro de Excelencia de Autoservicio, Fujitsu ofrece sus servicios de gestión y monitorización, que en conjunción con una sólida metodología y una dilatada experiencia, permiten aumentar notablemente la disponibilidad y seguridad de la red de ATMs. Fujitsu es una de las primeras compañías en prestar servicio de monitorización de cajeros.

En colaboración con los Servicios de Seguridad de las entidades financieras, los servicios de Fujitsu proporcionan seguimiento continuado del ciclo completo, y permiten a las Entidades Financieras tener la mínima exposición frente a amenazas.

El objetivo es asegurar los datos y los activos lógicos de Fujitsu y de sus clientes mediante el despliegue de servicios de seguridad gestionados del Centro de Operaciones de Seguridad (SOC) y servicios profesionales expertos.

El portafolio de Servicios de Seguridad comprende una amplia gama de servicios gestionados de seguridad (MSS) y servicios profesionales expertos. Las Ofertas MSS incluyen servicios que pueden proporcionar soluciones de defensa en profundidad, que van desde tecnologías de protección de red como firewalls, seguridad web y sistemas de detección de intrusiones, hasta servicios de encriptación y servicios de protección de punto final (por ejemplo, anti-malware).

- **Consultoría de seguridad:** Un análisis completo del estado de situación y que elabora un informe de exposición de la entidad frente amenazas.
- **Servicios de Monitorización Activa** que alertan de posibles ataques con respuesta de actuación en primer nivel en un entorno 24x7x365. Monitorización de las diferentes redes de autoservicio en tiempo real con interacción directa con los cajeros automáticos, personal de oficinas, empresas de transporte de fondos y con los servicios centrales de la entidad (Departamentos de Tecnología, Operaciones, Seguridad,...).
- **Servicios de Análisis y Predicción:** mediante herramientas de Business Intelligence de la suite **JanuX**, y apoyados en la bases de conocimiento internas, detectan patrones de comportamiento y se establecen recomendaciones de actuación, control y seguimiento de los cambios que se van introduciendo en la red de autoservicio.

Fujitsu Security Operations Center (SOC)

Nuestro SOC tiene como objetivo asegurar los datos de nuestros clientes y sus activos, mediante el despliegue de servicios de seguridad (gestionados por los diferentes SOC de Fujitsu distribuidos geográficamente) y servicios profesionales expertos.

Estos centros gestionan la seguridad de información para gran parte de las empresas más importantes del mundo y organizaciones del sector público. Garantizan que las amenazas cibernéticas sean identificadas y eliminadas, además de proponer mejoras sobre las medidas de seguridad implantadas.

Algunos de los servicios que se prestan en los diferentes SOC son:

- Colaboración en la implantación de herramientas y soluciones.
  - Antifraude.
  - Anti malware.
  - Control de acceso y autenticación.
  - Fugas de información.
  - Protección de comunicaciones.
- Auditoría técnica.
- Certificación normativa.
- Gestión de contingencia y continuidad de operaciones de negocio.
- Colaboración para facilitar el cumplimiento legal y normativo.
- Diseño y ejecución de planes de formación y concienciación.
- Gestión de incidentes de seguridad.
- Inteligencia de seguridad.
- Monitorización y **Protección en Tiempo Real** de la infraestructura completa del cliente (redes, redes perimetrales, centros de datos, puesto de trabajo, **cajeros automáticos, TPVs**, etc.).
- Seguridad de la nube.
- Integración con Sistemas SIEM para correlación de datos obtenidos de las diferentes herramientas de seguridad para facilitar la toma de decisiones y una respuesta temprana ante amenazas.

En resumen

La seguridad en los entornos de autoservicio no es una alternativa que se deba analizar. En un entorno cada vez más digital, los ataques e intentos de explotar vulnerabilidades están creciendo y evolucionando constantemente.

Las consecuencias de una elevada exposición, escasas medidas de seguridad o una estrategia no alineada, tendrán una importante afectación en términos económicos y de reputación.

Fujitsu puede ayudarle a desarrollar su estrategia de seguridad tanto en el entorno de autoservicio como en cualquier otro entorno de su entidad.

Contacto
FUJITSU Technology Solutions
Camino Cerro de los Gamos, 1
28224, Pozuelo de Alarcón (Madrid)
Tfno.: +34 91 784 9000
Website: www.fujitsu.com/es