



EL NUEVO PERÍMETRO DE LA SEGURIDAD ATM

Conocer las amenazas es el primer paso para construir un ecosistema más seguro.



EL CONTEXTO

El fraude ATM va más allá del ataque físico.

3.500

incidentes relacionados con ATM registrados en Europa en el primer semestre de 2026.



Prácticamente el **100%** fueron clasificados como fraude.



Las amenazas pueden afectar a la tarjeta, al efectivo, a los datos, al software, a las comunicaciones y a los sistemas conectados.

¿CÓMO SE MANIFIESTA EL FRAUDE?



TARJETA · EFECTIVO · DATOS

Tres modalidades concentran los incidentes registrados:



60%

Card trapping

La tarjeta queda retenida deliberadamente en el lector para ser recuperada posteriormente por el atacante.



29,5%

Cash trapping

El efectivo queda retenido mediante un dispositivo interno o externo y puede ser recuperado después por el delincuente.

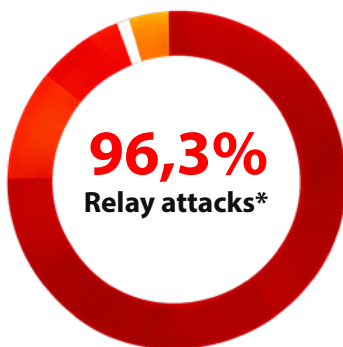


10,5%

Skimming y compromiso de datos

El objetivo es obtener o interceptar los datos sin necesidad de sustraer físicamente la tarjeta.

DEL ATAQUE FÍSICO AL DIGITAL



Entre los incidentes europeos de skimming y compromiso de datos clasificados por método, el **96,3%** correspondió a relay attacks.



¿Qué es un relay attack?

El atacante intercepta y retransmite en tiempo real la comunicación de una transacción legítima para hacerla válida fraudulentamente en otro punto remoto



La superficie de ataque ya no termina en el cajero: también incluye las comunicaciones y los sistemas conectados.

*No significa que el 96,3% de todos los ataques ATM sean relay attacks.

PROTEGER TODO EL ECOSISTEMA ATM

Un ATM forma parte de un ecosistema compuesto por:



HARDWARE



SOFTWARE



COMUNICACIONES



DATOS Y TRANSACCIONES



SISTEMAS CENTRALES



La **seguridad debe empezar antes del arranque** y mantenerse durante todo el ciclo operativo

Antes del sistema operativo

- Gestión de BIOS
- Cifrado de Disco
- Protección frente a manipulaciones físicas

Durante la operación

- Integridad y hardening
- Control de software y hardware
- Control de comunicaciones
- Monitorización remota
- Gestión remota centralizada



Garantizar el cumplimiento normativo: AI Act, DORA y CRA

DEL DISPOSITIVO AL PROCESO OPERATIVO

El objetivo ya no es únicamente proteger el cajero, sino proteger de extremo a extremo los procesos necesarios para:



DESPLEGAR

Distribuir de forma segura los dispositivos



ACTUALIZAR

Mantener sistemas y software actualizados



MANTENER

Garantizar la continuidad y la integridad operativa



OPERAR

Gestionar y supervisar de forma segura



ENFOQUE DE CERO CONFIANZA

El enfoque Zero Trust reduce la confianza implícita y controla qué puede ejecutarse, conectarse, modificarse y comunicarse.



VERIFICAR CONTINUAMENTE



PRIVILEGIOS MINIMOS



MONITORIZAR Y CONTROLAR

lookwise
DEVICE MANAGER

Protección Zero Trust para ATM y otros dispositivos OT críticos.

No se trata solo de proteger el cajero. Se trata de proteger de extremo a extremo los procesos operativos críticos y reducir la superficie de ataque antes de que una amenaza se convierta en un incidente.

[Descubre LDM](#)

