CERTFin

27 maggio 2025

Sviluppare strategie innovative per fronteggiare le minacce cyber: il valore della resilienza e della collaborazione e il ruolo dell'intelligenza artificiale

Romano Stasi

Direttore Operativo

Alcune evidenze dal Report 2025 del CERTFin

CERTFin

- La **percentuale media di budget dedicato** da ogni banca **alla sicurezza IT**, rispetto al totale delle spese generali sostenute per l'IT, si è attestata al **7%**. **77% delle banche ha un budget crescente**, nessuna banca in diminuzioner.
- Di tale budget, la quota destinata ad interventi per la **prevenzione e il contrasto delle frodi** corrisponde al **12%**.

- Del totale degli importi economici associati ai tentativi di frode, l'**84%** viene bloccato.

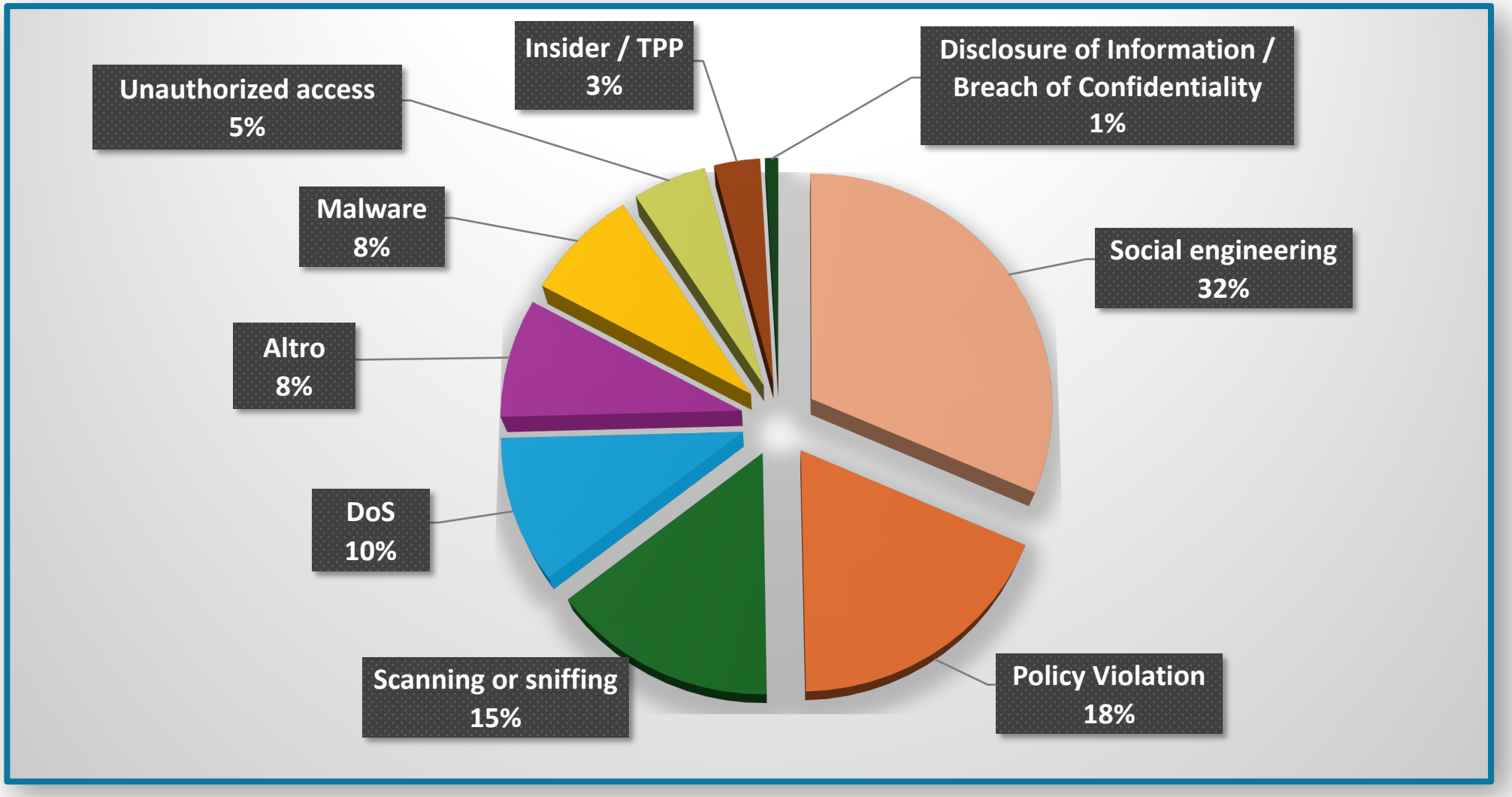
- Le transazioni fraudolente effettive operate **direttamente dal cliente** legittimo sono **l'82%** del totale.
- **Oltre il 60%** delle frodi effettive sono realizzate sfruttando come punto di contatto iniziale le **chiamate telefoniche e/o gli SMS.**

- Il **27%** delle soluzioni impiegate per il **monitoraggio e la rilevazione degli attacchi** rivolti alla clientela è basata su **tecnologie di AI.**
- Si osserva un **aumento del 125%** di conti correnti aperti mediante **furto d'identità**.

- Il **35%** dei PSP dichiara di aver rilevato almeno un **data breach indiretto** (28 CASI ad es., compromissione fornitore terzo o supply-chain).
- **Diminuiscono gli attacchi DDOS** e restano circa costanti le infezioni ransomware.

Distribuzione degli Incidenti di Sicurezza informatica

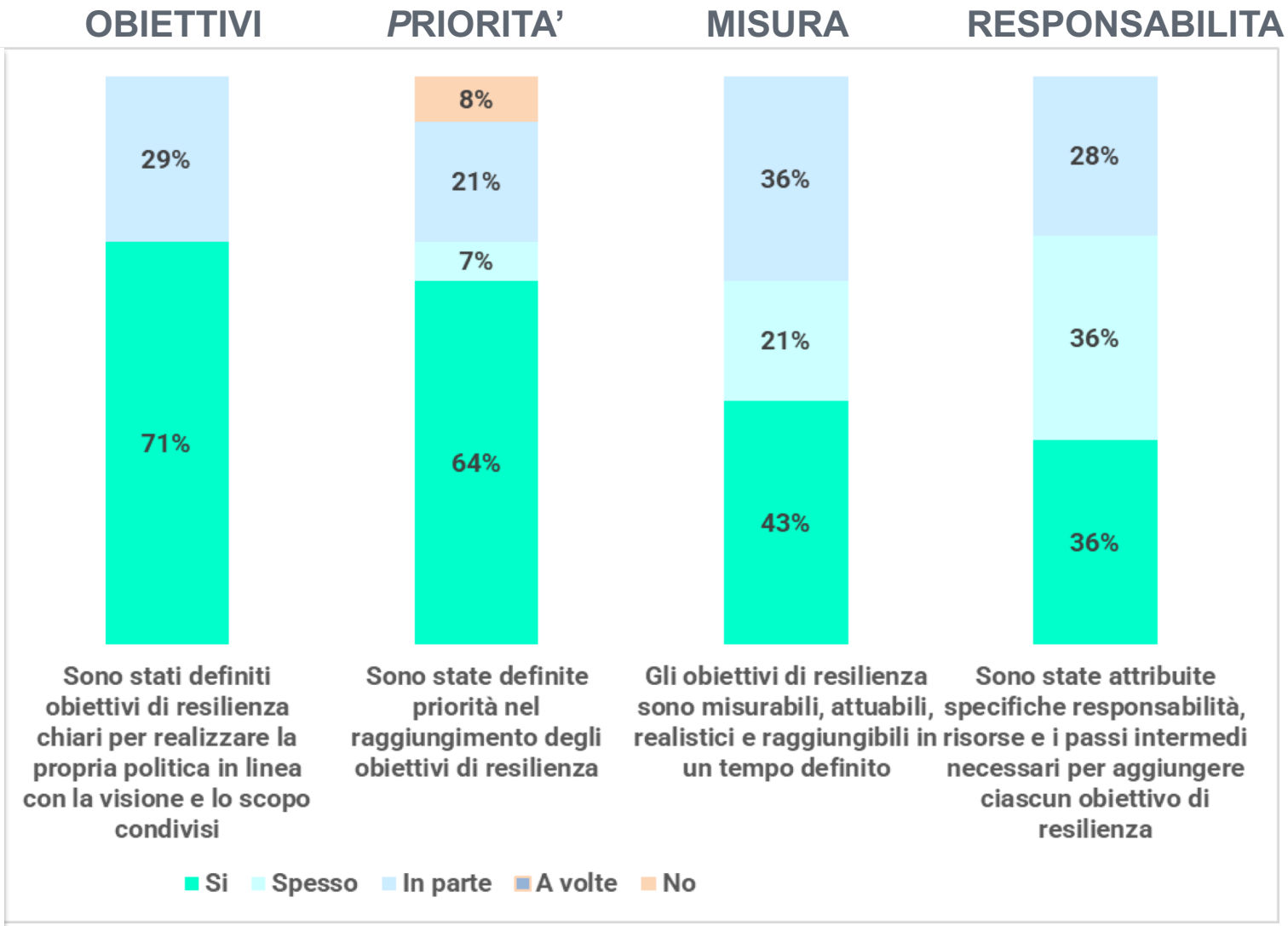
CERTFin



Fonte: Report Sicurezza e frodi informatiche in banca, 2025

«Obiettivi» di Resilienza

Si è impostato un **percorso strategico di resilienza**, con obiettivi misurabili e monitorati.



Tutte le organizzazioni hanno definito, del tutto o in parte, obiettivi di resilienza chiari e misurabili, attribuendone le relative responsabilità.

Fonte: Survey 2025 Osservatorio DORA Continuity & Resilience

Vulnerabilità sistemiche della catena della frode

CERTFin

È di primaria importanza che **tutti gli stakeholders siano coinvolti** per fronteggiare vulnerabilità sistemiche. Le istituzioni spingono per una integrazione dell'ecosistema digitale ma è necessario al contempo **una chiara distribuzione delle responsabilità per affrontare in modo integrato e collaborativo vulnerabilità e attacchi.**

1. ***Canale*** → Le banche non hanno modo di garantire **la sicurezza delle comunicazioni del canale mobile di interazione** con i clienti, canale remoto primario informativo e dispositivo. Gli operatori telefonici possono fare molto per incrementare la sicurezza nei servizi digitali.

2. ***Identità*** → I truffatori sfruttano la crescente *disintermediazione* e *frammentazione* nella gestione dell'identità digitale ormai elemento fondante non solo nell'attivazione dei servizi ma anche nell'operatività quotidiana dei clienti. **Identity providers e Identity wallets possono aggiungere sicurezza** nell'integrare servizi finanziari.

3. ***Business*** → Anche per le **truffe e il commercio elettronico fraudolento**, i clienti si rivolgono ai PSP per coprire le proprie perdite. Serve di **associare la corretta responsabilità** tra cliente, banche, operatori di TLC e piattaforme Social ognuno per quanto di competenza di impatto nella catena della frode.

4. ***Meccanismo di blocco*** → Non esiste un meccanismo internazionale efficace che consenta alle banche di **bloccare o recuperare le transazioni fraudolente**. Il settore bancario può avere regole piu' robuste per collaborare operativamente.

CERTFin

Grazie!