CERTFin

ABI Lab

SICUREZZA E FRODI INFORMATICHE IN BANCA

Come prevenire e contrastare attacchi informatici e frodi su Internet e Mobile Banking

CERTFin

SICUREZZA E FRODI INFORMATICHE IN BANCA
Come prevenire e contrastare attacchi informatici e frodi su Internet e Mobile Banking

Osservatorio Cyber Knowledge and Security Awareness

TLP GREEN maggio 2021

CERTFin

SOMMARIO

EXECUTIVE SUMMARY

Chi lavora nel mondo della cybersecurity, e in particolare chi opera all'interno del settore finanziario, è abituato al necessario e continuo aggiornamento su tutti gli aspetti inerenti l'evoluzione delle minacce e dei fenomeni di frode, sia sul fronte tecnico che su quello organizzativo.

Tuttavia, questa tradizionale evoluzione è stata, quanto mai prima d'ora, accentuata ed accelerata dallo sconvolgimento dello scenario, causa pandemia covid-19, in cui ci siamo visti calare, nostro malgrado, nel 2020.

I modelli di attacco si sono adattati con repentina efficacia al nuovo contesto, alle nuove modalità di lavoro, al forzato distanziamento banca-cliente, costringendo chi difende a dover tener conto anche di fattori trascurati fino al giorno prima.

Questo si riflette inevitabilmente su alcuni dei dati raccolti: ad esempio, malgrado una grande disomogeneità dei dati, si rileva che, rispetto all'anno precedente, la quota degli investimenti destinata ad incrementare la sicurezza dei servizi è cresciuta, in alcuni casi anche di venti punti percentuali.

Come consuetudine, il nostro Report ha l'obiettivo di analizzare ad ampio spettro la fenomenologia del mondo delle frodi nel settore bancario italiano, così da essere uno strumento di supporto per gli operatori del settore.

I dati raccolti consentono un'analisi neutra e ragionata sullo stato delle minacce cyber nel settore finanziario, ma è evidente che, al termine di un anno così particolare, operare un confronto con i dati rilevati negli anni precedenti va fatto con cautela.

In alcuni casi i principali trend delle frodi hanno subìto delle discontinuità e, conseguentemente, i task sui quali può essere utile indirizzare maggiormente le risorse per migliorare i processi difensivi devono essere identificati a valle di attente riflessioni.

La nostra analisi si basa sull'attenta valutazione, e interpretazione, di tutte le informazioni raccolte attraverso la survey annuale compilata su base volontaria dalle organizzazioni aderenti al CERTFin, nell'ambito dell'Osservatorio Cyber Knowledge

and Security Awareness, volutamente impostata con un taglio essenziale, senza approfondire troppo gli aspetti prettamente tecnici, in modo da risultare fruibile al maggior numero possibile di lettori.

Le statistiche e i commenti presentati si riferiscono a un campione di rispondenti che, per il settore bancario, raggiunge un'elevata rappresentatività in termini di dipendenti (78%) e pertanto possono essere considerati ragionevolmente significativi. Anticipando alcune delle conclusioni che seguono, possiamo affermare che il 2020 è stato un anno in cui il numero complessivo di attacchi andati a buon fine è aumentato, seppur di poco. Sul totale delle transazioni anomale, la percentuale di frodi effettive è stata infatti pari al 17%, contro il 14,5% dello scorso anno. Tale incremento è imputabile, tra gli altri, alla cospicua quota di bonifici istantanei fraudolenti e al significativo peso delle frodi effettive sulle ricariche di carte prepagate, passate, per il settore Retail, dal 5% del 2019 al 25% del 2020 e per il settore Corporate addirittura dallo 0% a circa il 20%. Più nello specifico, si conferma il trend che vede la clientela Retail tradizionalmente quella più colpita, tanto da risultare come target in 4 casi su 5.

Nonostante il brusco cambio di scenario e l'ulteriore sofisticazione di alcuni pattern di frode a cui abbiamo assistito, pur con una leggera flessione, la percentuale di transazioni fraudolente bloccate/recuperate si mantiene a livelli elevati: in media l'83%.

Sul fronte dei vettori d'attacco, appare opportuno evidenziare come ormai le tecniche miste (ad esempio social engineering combinato con malware) siano assolutamente prevalenti rispetto alle altre, arrivando a rappresentare il 65% degli attacchi, toccando ben l'80% se ci riferiamo alla clientela retail.

Diversamente, sul fronte degli attacchi alle infrastrutture, il 2020 fa registrare un picco di attacchi RDDoS, concentrati in 3 grandi ondate, con il 57% degli istituti che dichiara di averne subìto almeno uno. Considerato l'intensificarsi del fenomeno, si manifesta, a livello di settore, l'esigenza di focalizzarsi sulla revisione e il potenziamento delle soluzioni esterne anti-DDoS.

Tra i principali fenomeni che negli ultimi anni hanno maggiormente insidiato il settore vi è sicuramente lo schema di frode noto come "SIM Swap", che, ricordiamolo, avviene sempre a posteriori di un furto di credenziali. Dai dati rilevati emerge distintamente come il fenomeno abbia accusato una significativa contrazione. Il ridimensionamento di questa tipologia di frode è

senz'altro riconducibile allo sforzo prodotto dal tavolo di lavoro congiunto tra settore bancario, rappresentato dal CERTFin, e operatori telefonici, tavolo attivo già dalla fine del 2019.

Sebbene la sperimentazione condotta dal tavolo di lavoro sia ancora in corso, è indubbio che le contromisure tecniche identificate si sono dimostrate efficaci e che, di conseguenza, se adeguatamente diffuse, consentiranno di rendere il fenomeno marginale.

Riguardo alle modalità utilizzate per autorizzare le transazioni, grazie anche agli investimenti precedentemente citati, si evidenzia, in maniera del tutto positiva, come il settore nell'ultimo anno abbia diversificato significativamente le modalità di autenticazione del cliente, il tutto a beneficio di una maggiore sicurezza della clientela stessa.

Infine, si segnala che il Report 2021 dedica, all'interno dell'appendice, alcuni approfondimenti verticali a tematiche particolarmente attuali in ambito bancario, a firma di esperti autorevoli che afferiscono a player nazionali ed internazionali con forti competenze di cybersecurity e che supportano le attività del CERTFin in qualità di Cyber Advisor.

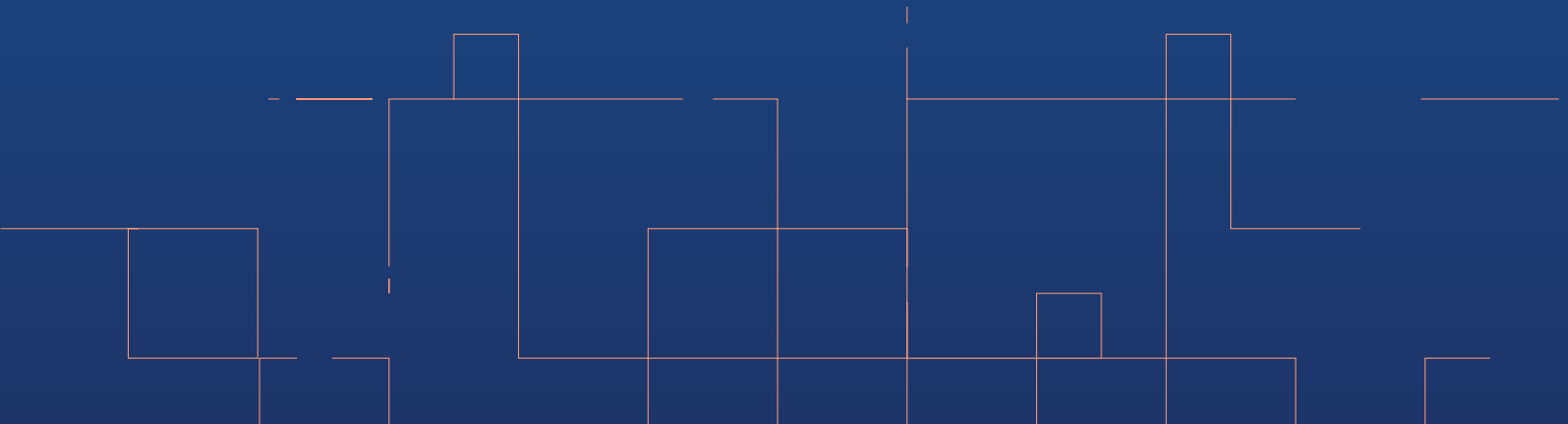
Tutte le attività legate all'impostazione, all'elaborazione dei dati della survey e alla redazione del Report sono state condotte da: Romano Stasi, Mario Trinchera, Roberto Tordi, Maria Ferrucci, Piero Piperno, Simone Coltellese, Gabriele Gamberi.

Si desidera inoltre ringraziare:

- le banche e gli outsourcer interbancari che hanno partecipato alla rilevazione
  Banca Carige, Banca IFIS, Banca Mediolanum, Banca Passadore, Banca Popolare di Sondrio, Banca Reale, Banca Sella, Banco BPM, Banco di Desio e della Brianza, BNL, BPER Banca, Cassa di Risparmio di Asti, Cedacri, Credito Emiliano, Credito Valtellinese, FinecoBank, illimity, Intesa Sanpaolo, Monte dei Paschi di Siena, Poste Italiane, UBI Banca, UniCredit, Volksbank
- i Cyber Advisor per la redazione dei contributi riportati in appendice del Report
  Accenture, Cleafy, Exprivia, Kaleyra, KPMG, Lutech, Reply, TIM.

CERTFin

STRUTTURE DI CYBERSECURITY E INVESTIMENTI



1. STRUTTURE DI CYBERSECURITY E INVESTIMENTI

In linea con l'impostazione già adottata nella scorsa edizione del Report, si è scelto di iniziare l'analisi dei dati dedicati alla conformazione delle strutture di cybersecurity interne alle banche con il tracciamento delle figure tecniche poste alla guida delle attività svolte, per poi procedere con la rilevazione degli strumenti adottati a supporto delle attività di contrasto e prevenzione delle frodi e successivamente con la rappresentazione dei livelli di maturità percepita dal personale interno su alcuni processi di sicurezza.

Successivamente, saranno analizzate le previsioni di spesa dedicata alla sicurezza dei canali Internet e Mobile e alle attività di contrasto e prevenzione delle frodi per l'anno in corso.

A tal proposito, si segnala che a causa di una importante disomogeneità dei dati rilevati, in parte attribuibile alla necessità di provvedere ad investimenti straordinari, non inizialmente inseriti all'interno del budget 2020 di diverse banche rispondenti, non è stato possibile rappresentare in maniera attendibile i dati relativi al rapporto tra spese totali dedicate al contrasto e prevenzioni delle frodi, spese totali relative alla sicurezza e spese totali dedicate all'IT.

Ad ogni modo, nel complesso l'insieme delle analisi svolte all'interno del presente capitolo sembra evidenziare un percorso evolutivo in atto caratterizzato da un orientamento generale volto ad introdurre, anche in una prospettiva di breve-medio periodo, strumenti evoluti per il contrasto delle frodi sui canali remoti e a consolidare le attività focalizzate sulla gestione preventiva di minacce ed eventi cyber.

1.1. Le strutture di Cybersecurity interne alla banca

Analizzando il grafico 1.1, costruito su un campione di 22 banche rispondenti, si può evincere come nella maggior parte dei casi (il 54%) le attività di cybersecurity interne risultino essere in capo ad un CISO (Chief Information Security Officer); a seguire è stata indicata la figura del CIO (Chief Information Officer) nel 14% dei casi e il Chief Risk Manager nel 5% dei casi.

Il 27% dei rispondenti, invece, segnala che le attività oggetto dell'analisi sono gestite da una figura diversa rispetto a quelle proposte ma, ad ogni modo, nella maggior parte dei casi, risulta essere assimilabile a profili professionali affini a quelli citati oppure che rientrano nell'ambito dell'ICT management interno alla banca.

Alcune realtà, inoltre, hanno segnalato una gestione delle attività di cybersecurity condivisa da più figure tecniche di riferimento. Ad ogni modo, anche in considerazione dei dati pubblicati negli anni scorsi, sembra concretizzarsi un trend generale volto al rafforzamento del ruolo dei CISO.

Per quanto riguarda, invece, le **funzioni coinvolte nei processi di gestione delle frodi**, la figura 1.2, costruita su un campione di 22 rispondenti, evidenzia che:

- le funzioni di governance e operations sono coinvolte nell'82% dei casi;
- la funzione di sicurezza applicativa nel 64 % dei casi;
- la funzione di gestione dell'infrastruttura IT nel 59% dei casi.

Un cospicuo numero di rispondenti ha segnalato, inoltre, il coinvolgimento di altri tipi di strutture interne (*Legale, Commerciale, Compliance, Contact Center, Canali Digitali*); in diverse realtà, infine, è stata segnalata la presenza di una struttura dedicata al "*fraud management*".

In relazione, invece, al numero di risorse assegnate a ciascuna funzione, si segnala che le operations e la governance risultano avere, in media, un numero maggiore di risorse dedicate, rispettivamente con 7 e 8 addetti.

Al fine di offrire una panoramica completa di come evolvono le strutture di cybersecurity si è ritenuto opportuno anche analizzare le **tecnologie e gli strumenti utilizzati nell'ambito delle attività finalizzate alla prevenzione e al contrasto delle frodi**. La figura 1.3, costruita su un campione di 22 rispondenti, dimostra che nella maggior parte dei casi sono stati già introdotti strumenti di advanced data analytics (59%), di intelligenza artificiale (55%) o strumenti di identificazione biometrica (50% dei casi).

Di particolare interesse risulta essere quanto emerge in relazione alle **soluzioni tecnologiche** che le banche intendono acquisire in prospettiva, nell'arco del breve-medio periodo. A tal proposito, il 59% delle banche rispondenti prevede di introdurre strumenti SOAR (Security Orchestration, Automation and Response), il 45% strumenti di Robotic Process Automation e il 41% strumenti anti-SIM Swap.

In considerazione dei dati rappresentati, dunque, per il prossimo futuro è ipotizzabile un'evoluzione delle strutture di cybersecurity, che potranno essere più orientate a dotarsi di strumenti automatizzati in grado di garantire un corretto presidio dei task "ripetitivi", con ricadute positive sul lavoro svolto dai security analyst, che potranno focalizzarsi maggiormente sull'analisi e la mitigazione delle minacce più sofisticate.

L'analisi sulla conformazione delle strutture di cybersecurity si conclude con la valutazione del **livello di maturità** percepito all'interno di ogni organizzazione in relazione ai processi e ai diversi ambiti di competenza delle strutture di cybersecurity.

La figura 1.4 rappresenta un livello di maturità percepito grossomodo conforme su tutti i processi presi in considerazione (campione di 22 rispondenti). Il livello più alto, 4,18, su una scala da 1 (minore) a 5 (massimo), è attribuito al "monitoraggio della rete ai fini dell'intrusion detection".

Inoltre, il processo di "*monitoraggio degli end point ai fini di sicurezza*", già di per se particolarmente rilevante e ancor di più nel contesto pandemico in atto, laddove il ricorso intensivo al lavoro agile ha moltiplicato il numero degli endpoint messi in rete, viene percepito con un livello di maturità soddisfacente, con un valore di 4.05 su 5.

Per quanto riguarda, invece, i diversi ambiti che afferiscono alla cybersecurity, la figura 1.5, costruita su un campione di 22 rispondenti evidenzia che la **cyber threat intelligence** risulta avere acquisito il maggior livello di maturità percepita, con un punteggio di 4,58 su 5. Rispetto allo scorso anno, tra tutti gli ambiti analizzati, quest'ultimo risulta aver avuto il maggior incremento (nel 2020 il livello era di 3.58).

Si tratta di un dato di rilievo, che dimostra come la cyber threat intelligence sia ormai largamente diffusa all'interno delle banche italiane e sia in grado di abilitare un cambio di paradigma all'interno delle strategie di cybersecurity, sempre più orientate

a prevenire, ove possibile, gli eventi cyber attraverso la gestione precoce delle minacce segnalate.

Tra gli ambiti con un maggior livello di maturità percepito rientra anche l'**awareness interna** che, in ogni caso, può essere ulteriormente migliorata, anche in considerazione delle numerose campagne di phishing registrate nel 2020 e nel primo quadrimestre del 2021, spesso perpetrate sfruttando tematiche connesse con la pandemia da COVD-19 ancora in atto.

1.2 Evoluzioni di spesa per la sicurezza dei canali remoti.

La particolare attenzione delle banche italiane sulla sicurezza dei canali remoti risulta essere confermata anche dall'evoluzione degli investimenti dedicati in questo ambito (figura 1.6).

La maggior parte dei rispondenti, per il 2021, ha indicato un aumento della spesa destinata alla sicurezza dei canali remoti, con iniziative sia verso il cliente, nell'80% dei casi, sia internamente verso l'organizzazione, nel 90% dei casi, considerando una scala di valori che va da lieve a rilevante.

È opportuno evidenziare che gli aumenti di investimento "rilevanti" (ovvero superiori al 15% rispetto all'anno precedente), previsti per il 2021 e dichiarati dal 10% dei rispondenti, saranno tutti destinati ai servizi per la clientela.

1.3 Budget per il contrasto e prevenzione delle frodi.

Per avere un quadro di dettaglio sul piano di budget 2021 delle banche italiane dedicato alla prevenzione e al contrasto delle frodi informatiche, è interessante comprendere le esigenze alla base di costi e investimenti stanziati.

Su un campione di 19 rispondenti, il 48% ha indicato gli interventi per incrementare i livelli di sicurezza dei servizi come principale driver di spesa. Tra le motivazioni che spingono le banche italiane in questa direzione, probabilmente, vi è anche la necessità di assicurare adeguati livelli di sicurezza a fronte di una superficie di attacco potenziale che si è ampliata in maniera

considerevole anche a seguito dell'introduzione intensiva del lavoro agile, registrata nel corso del 2020.

Seguono poi, senza differenze considerevoli, gli investimenti dedicati ai progetti di evoluzione del servizio alla clientela anche in ottica di business (26%) e quelli dedicati all'adeguamento alle normative di settore (25%).

Figura 1.1 **Figure interne responsabili dei processi di Cybersecurity**

(22 rispondenti)

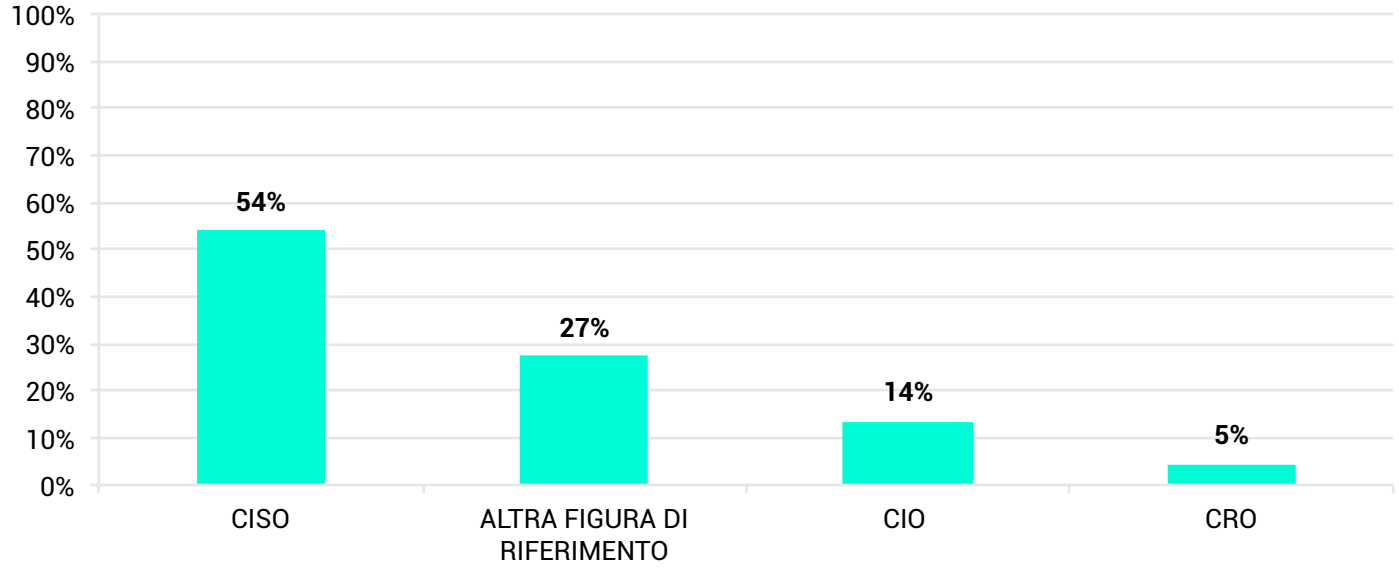
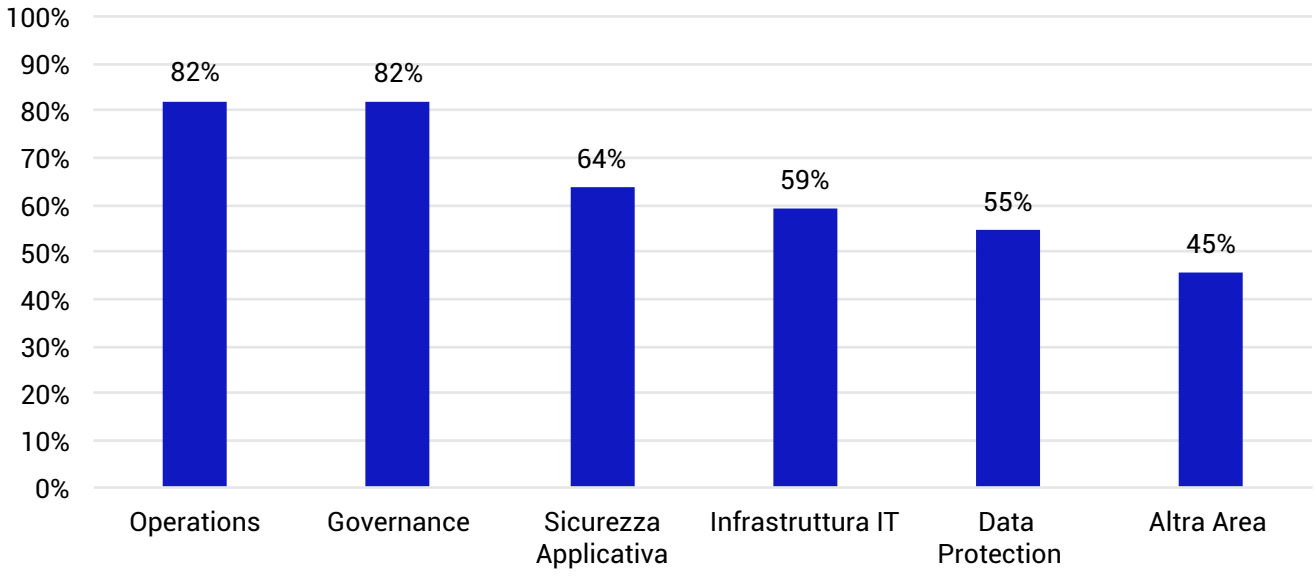


Figura 1.2 **Funzioni e numero di risorse coinvolte nei processi di gestione delle frodi all'interno dell'organizzazione**

(22 rispondenti)



NUMERO DI RISORSE IMPIEGATE IN MEDIA	**7**	**6**	**5**	**4**	**5**

Figura 1.3 **Tecnologie a supporto delle attività finalizzate al contrasto delle frodi**

(22 rispondenti)

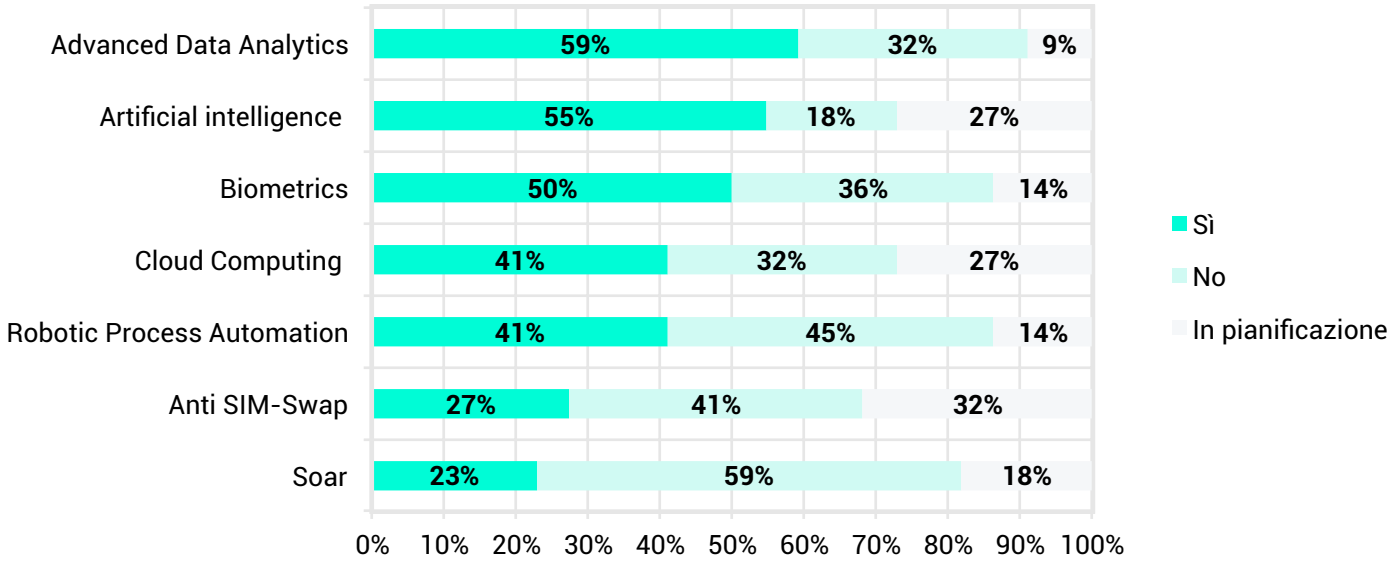


Figura 1.4 **Livello di maturità percepito in relazione ai diversi processi di cybersecurity della banca su una scala di valori dove 1= livello di maturità minimo, 2=basso, 3=medio, 4=elevato, 5=massimo**

(22 rispondenti)

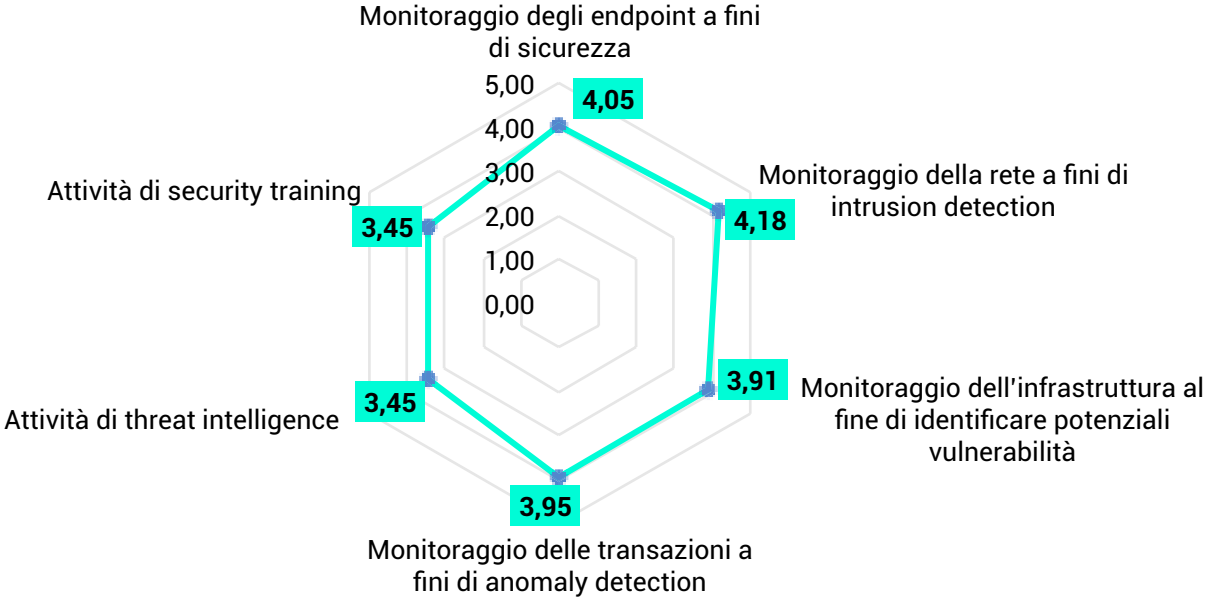


Figura 1.5 **Livello di maturità percepito in relazione ai diversi ambiti di cybersecurity della banca su una scala di valori dove 1= livello di maturità minimo, 2=basso, 3=medio, 4=elevato, 5=massimo**

(22 rispondenti)

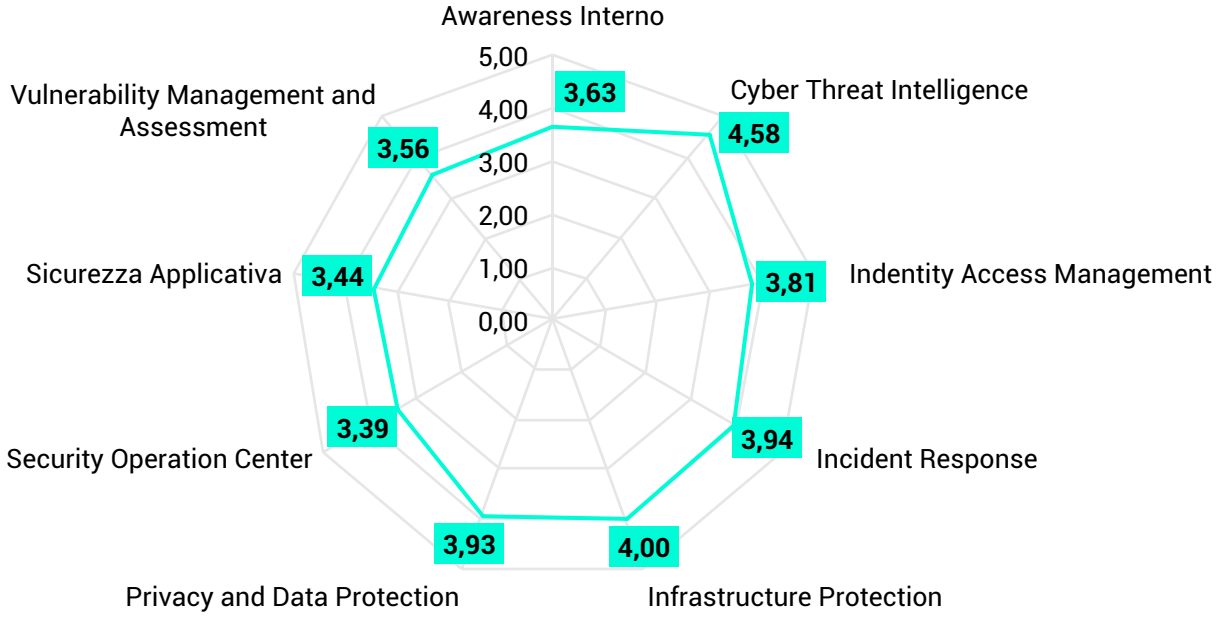


Figura 1.6 **Previsioni livello medio di spesa dedicata alla sicurezza dei canali Internet/Mobile nel 2021**

(20 rispondenti)

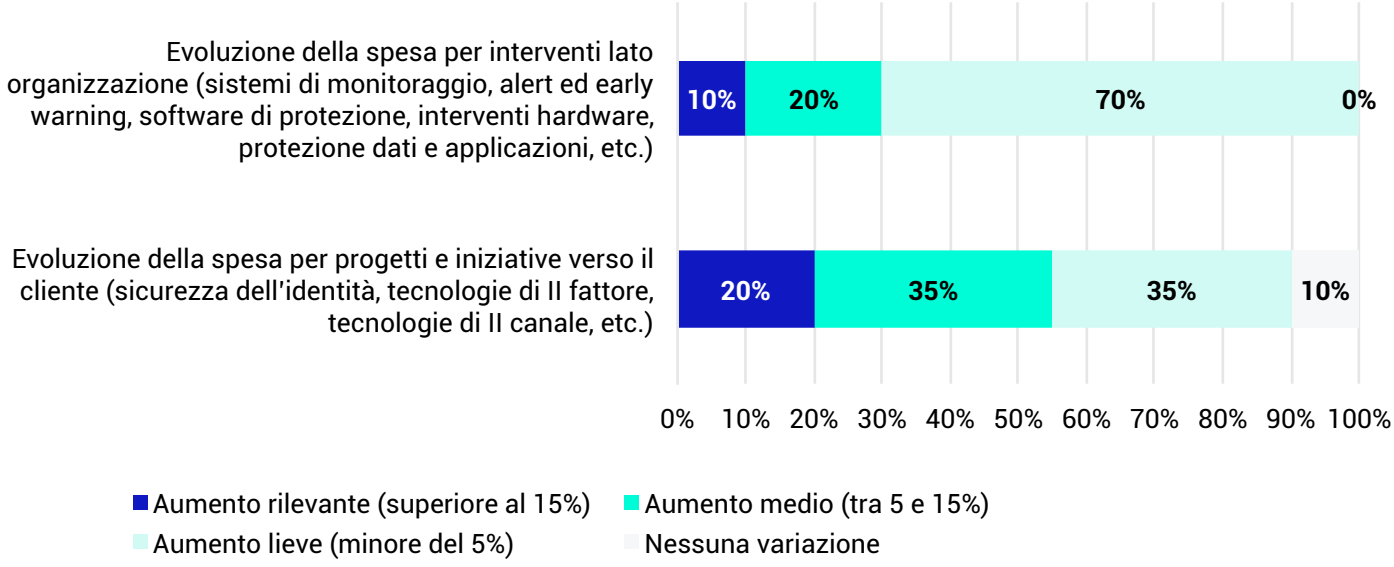
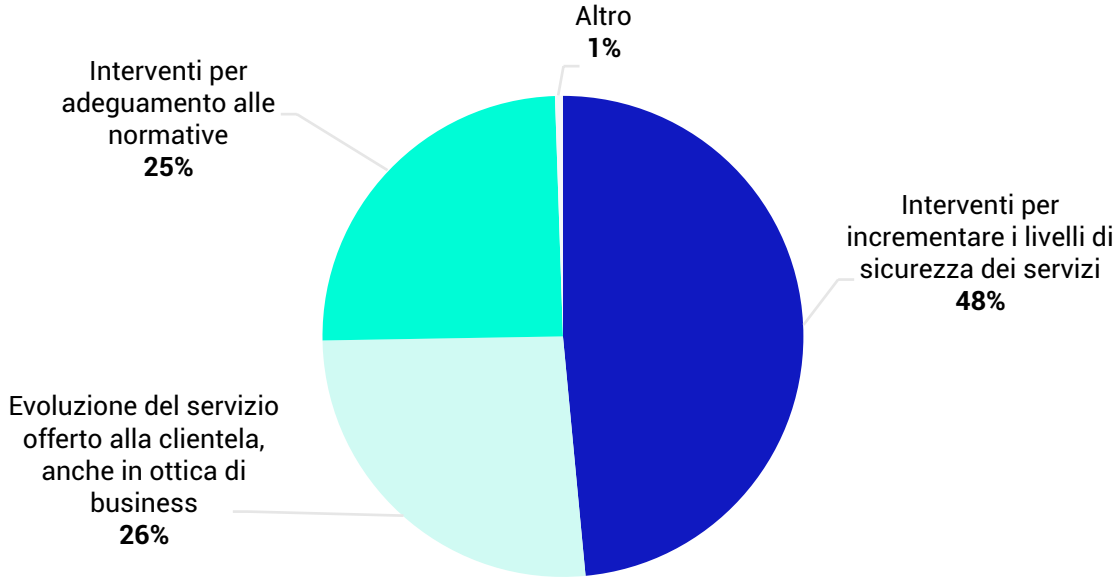


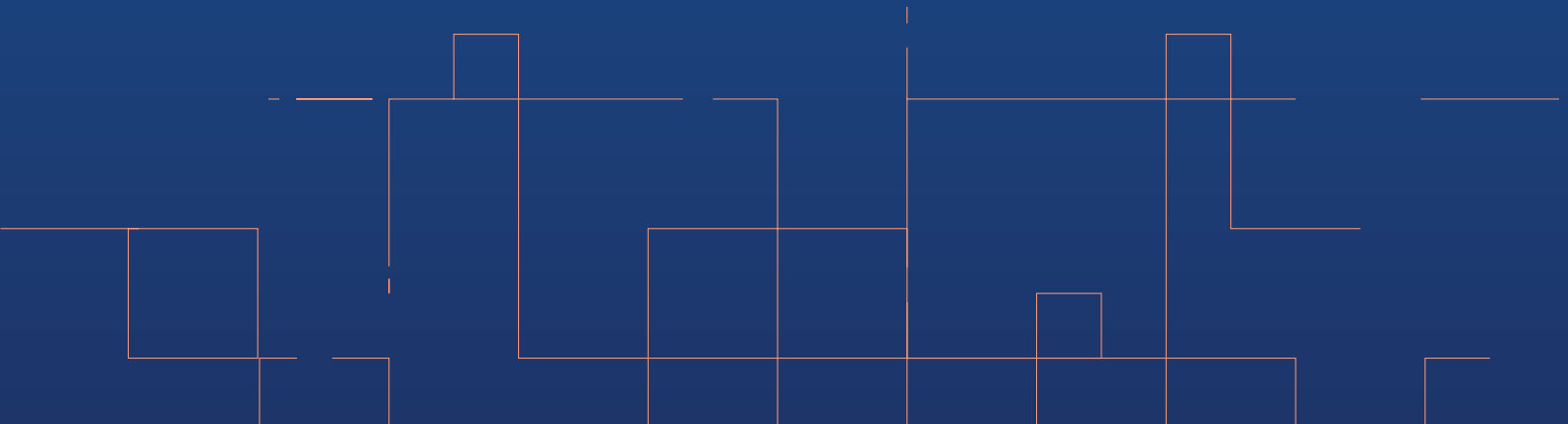
Figura 1.7 **Ripartizione percentuale del budget destinato a progetti/interventi legati al contrasto e alla prevenzione delle frodi informatiche nell'anno 2021**

(19 rispondenti)



CERTFin

IL DIMENSIONAMENTO DELLE FRODI INFORMATICHE INTERNET/ MOBILE



2. IL DIMENSIONAMENTO DELLE FRODI INFORMATICHE INTERNET/ MOBILE

Introduzione

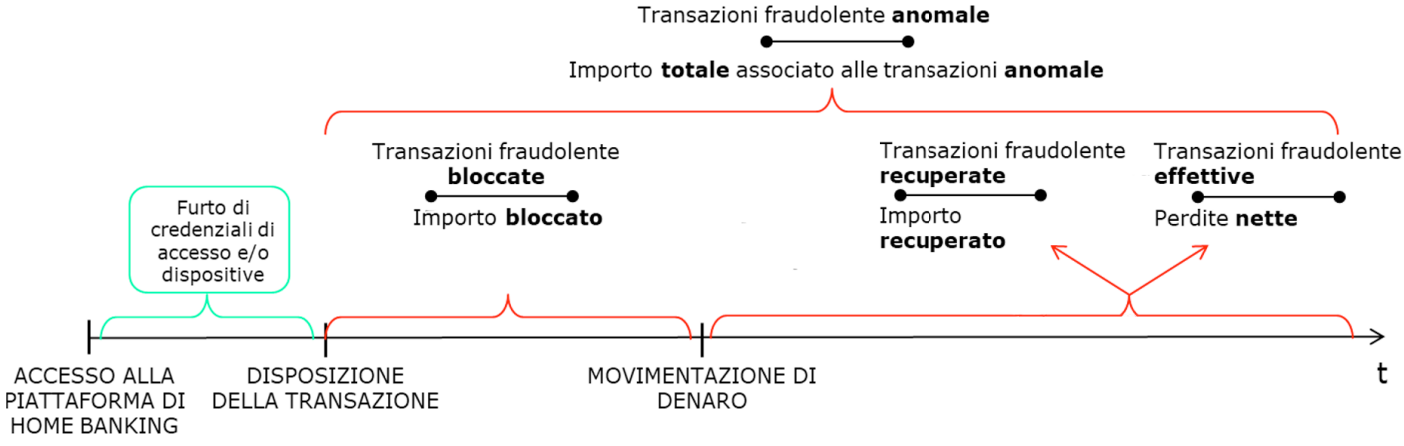
Come di consueto, la presente sezione del Report si sofferma sul dimensionamento delle frodi perpetrate verso i segmenti Retail e Corporate attraverso i canali Internet e Mobile Banking. La panoramica descritta nel capitolo è molto significativa, soprattutto se si tiene conto della mole di accessi ai servizi digitali: 20 organizzazioni hanno segnalato oltre 5,5 miliardi di accessi contro i 2,2 dell'anno precedente registrato da 14 istituti.

Il campione rispondenti di 23 organizzazioni ha indicato i dati rilevati nel periodo compreso tra il 1° gennaio e il 31 dicembre 2020, rispondendo ad un elenco di domande lievemente aggiornato rispetto allo scorso anno. In particolare, è stato inserito un quesito volto ad indagare eventuali transazioni fraudolente che hanno riguardato il servizio CBI e si è chiesto di indicare la distribuzione percentuale dell'età delle vittime degli attacchi.

In analogia con quanto già fatto lo scorso anno, sono state inoltre aggiornate le tipologie di operazioni di pagamento per cui si è chiesto di indicare le transazioni anomale registrate (secondo lo schema rappresentato in figura 2.1 e descritto nella pagina seguente), con l'obiettivo di rappresentare in maniera quanto più fedele il quadro attuale dei pagamenti digitali (nello specifico, sono state aggiunte le categorie bollettino postale e ricarica telefonica).

Figura 2.1 **Rappresentazione schematica del percorso di attuazione di una transazione fraudolenta**

(20 rispondenti)



- *transazioni fraudolente bloccate*: frodi che sono state rilevate e bloccate prima che abbiano avuto un impatto economico sul conto corrente della vittima (ad esempio perché bloccate e/o rilevate dai sistemi di alert e fraud detection della banca). Non sono ricompresi in tale definizione i tentativi di sottrazione delle credenziali di accesso;
- *transazioni fraudolente recuperate*: frodi che hanno comportato una movimentazione di denaro dal conto corrente della vittima ma per le quali è stato possibile recuperare l'intero importo transato;
- *transazioni fraudolente effettive*: frodi "andate a buon fine", per le quali il cliente ha subito un danno economico, anche parziale, indipendentemente dai rimborsi ottenuti dall'istituto.

Perdita di credenziali

La prima parte della sezione sul dimensionamento indaga l'andamento del furto di credenziali di accesso e/o dispositive per l'utilizzo di canali Internet e Mobile. Nel 2020 si registra un'inversione di tendenza rispetto a quanto emerso l'anno scorso, con un peggioramento per il segmento Retail e un miglioramento per il segmento delle imprese.

Andando nel dettaglio dei dati segnalati, su un campione di 22 rispondenti la percentuale di clienti attivi (ovvero coloro che nel corso dell'anno hanno effettuato almeno un accesso, anche semplicemente per fini informativi, all'Internet Banking) del segmento **Retail** che ha subito una sottrazione di credenziali è stata pari allo 0,35% (lo scorso anno tale percentuale era stata dello 0,25% su un campione di 18 rispondenti). L'analisi a campione costante, funzionale ad una rappresentazione ancora più fedele del fenomeno, di 9 istituti tra il 2018 e il 2020 conferma tale trend (figura 2.2), passando da poco meno dello 0,3% (0,286%) a quasi lo 0,6% (0,579%).

Con riferimento al segmento **Corporate**, come sopra accennato, si assiste ad un decremento della percentuale di clienti attivi a cui sono state rubate le credenziali (passando da 2,63% a 1,63% tra il 2019 e il 2020, media rispettivamente calcolata su 13 e 20 rispondenti). Come per il segmento Retail, anche per il comparto imprese l'analisi a campione costante mostra tale andamento (2,714% nel 2019 e 1,641% nel 2020).

Vale la pena ricordare, tuttavia, che i dati molto negativi dell'anno scorso erano imputabili per gran parte ad un caso particolarmente grave di data breach.

Figura 2.2

Percentuale clienti attivi Retail che hanno subito un furto di credenziali
Trend 2018-2020

(campione costante 9 rispondenti)

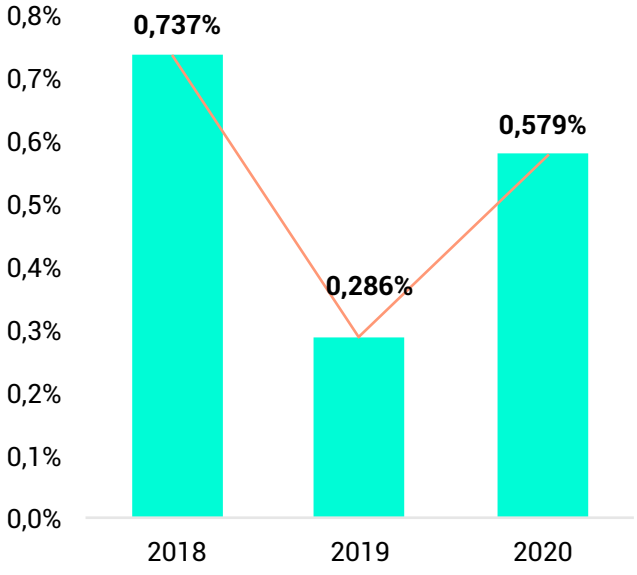
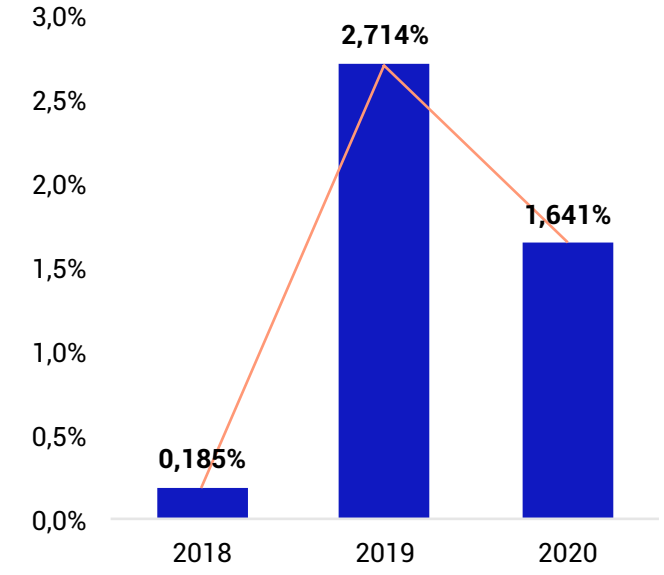


Figura 2.3

Percentuale clienti attivi Corporate che hanno subito un furto di credenziali
Trend 2018-2020

(campione costante 9 rispondenti)



Le transazioni fraudolente bloccate, recuperate ed effettive - analisi su Clientela Retail

La sezione che segue vuole indagare le operazioni di pagamento attraverso cui gli attaccanti tentano di sottrarre denaro. A tal fine, per ciascuna operazione di pagamento al campione rispondenti è stato chiesto di indicare la quantità di transazioni anomale suddividendole tra bloccate, recuperate ed effettive. Indirettamente, il capitolo indaga quindi anche la capacità di reazione e risposta degli istituti.

Per facilitare la lettura dei fenomeni rilevati nel corso del 2020, sono riportati nelle pagine a seguire le seguenti rappresentazioni, riferite alla numerosità degli accadimenti:

- ripartizione percentuale delle tipologie di transazioni fraudolente bloccate e recuperate;
- ripartizione percentuale delle tipologie di transazioni fraudolente effettive;
- ripartizione percentuale tra transazioni bloccate/recuperate ed effettive;
- ripartizione percentuale tra tipologie di transazioni anomale (bloccate, recuperate ed effettive).

La prima parte del capitolo riporta le evidenze emerse per il segmento Retail.

Focalizzando l'attenzione sul primo grafico (figura 2.4), emerge che sul totale delle transazioni anomale bloccate e recuperate, la quota prevalente è rappresentata dai bonifici istantanei con oltre il 50%, seguiti dai bonifici ordinari (nazionali e esteri all'interno dello Spazio Economico Europeo) e dalle ricariche di carte prepagate (figura 2.3).

Anche tra le **frodi effettive** i bonifici istantanei cubano la percentuale più alta, con il 46,5%. Tra le transazioni fraudolente "andate a buon fine", come anticipato nell'Executive Summary, è da evidenziare il forte incremento delle ricariche di carte prepagate (non operate tramite bonifico) - nella maggior parte dei casi appartenenti a "money mule" - rispetto allo scorso anno, dal 4% al 25% (figura 2.5). Vale la pena sottolineare che tale fenomeno è limitato ad alcune realtà, che hanno evidenziato tuttavia importanti volumi. Da non trascurare la percentuale di frodi sulle ricariche telefoniche, che nell'anno della loro introduzione tra le operazioni di pagamento approfondite dalla survey raggiungono poco meno del 5%.

Lo strumento della carta prepagata è inoltre quello per cui più elevata risulta l'efficacia dell'attacco, con circa 1/3 dei tentativi che sfociano in perdite effettive di denaro (figura 2.6). Stesso rapporto si registra anche per le ricariche telefoniche, seppure su tale strumento la numerosità delle transazioni anomale (asse delle ascisse) è molto ridotta rispetto ad altri. Aumenta, seppur di poco, la percentuale di efficacia degli attacchi sui bonifici istantanei, arrivando al 17%.

La figura 2.7, infine, mostra la ripartizione percentuale tra tipologie di transazioni anomale, suddividendole tra bloccate/recuperate ed effettive: come accennato nell'introduzione del Report, **nel 2020 cresce l'efficacia degli attacchi**, con una quota di transazioni anomale effettive passata dal 14,5% al 18%.

La sezione dedicata al comparto Retail si conclude con una novità della survey di quest'anno, ovvero la **distribuzione dell'età delle vittime** in relazione alle frodi tentate o effettive (figura 2.8) . Ai partecipanti è stato chiesto di indicare la distribuzione percentuale tra le seguenti quattro fasce d'età: under 30, tra i 30 e i 45 anni, tra i 45 e i 60 anni e over 60. Dall'analisi dei dati emerge che la fascia più colpita è quella tra i 30 e i 45 anni, con il 35% delle risposte, seguita non lontano dalla fascia 45-60 anni (28%). A pari merito le fasce restanti (under 30 e over 60), con il 19% e il 18% rispettivamente.

Vale la pena evidenziare, tuttavia, che tale rappresentazione non tiene conto del volume del transato (le fasce più colpite, cioè, sono quelle caratterizzate - con molta probabilità - da una maggiore numerosità di transazioni). Sarà possibile valutare, nella rilevazione 2022, l'introduzione di questo parametro, per consentire una rappresentazione ancora più fedele della distribuzione dell'età delle vittime di frodi.

Figura 2.4

Ripartizione percentuale delle tipologie di transazioni fraudolente bloccate e recuperate - analisi sul numero di accadimenti* (segmento Retail)

*Ripartizione percentuale sul totale di transazioni fraudolente effettive fornite da 21 rispondenti

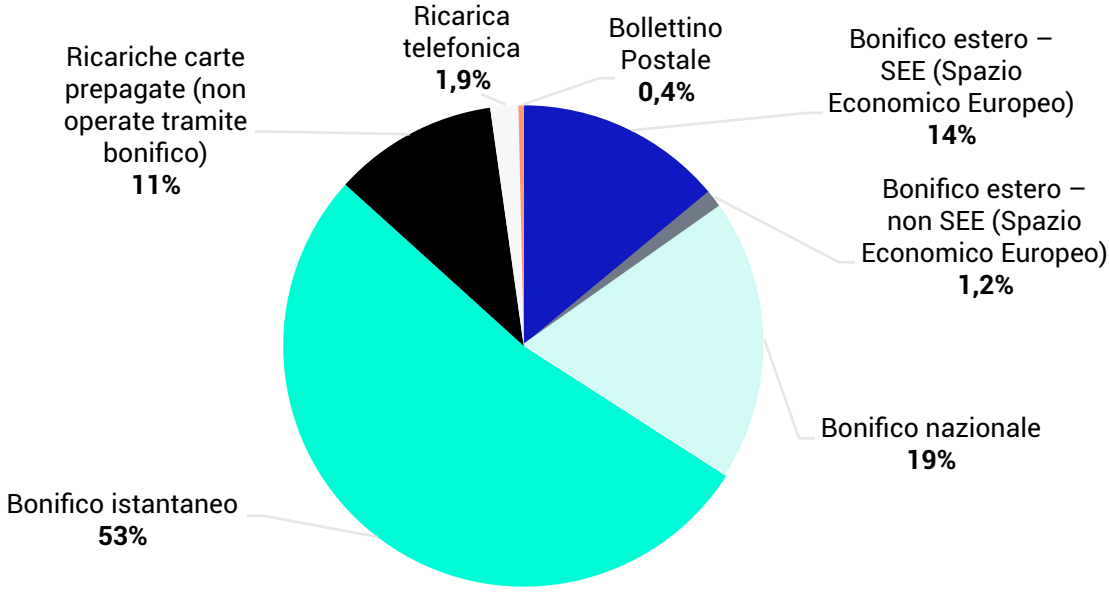


Figura 2.5 **Ripartizione percentuale delle tipologie di transazioni fraudolente effettive - analisi sul numero di accadimenti* (segmento Retail)**

*Ripartizione percentuale sul totale di transazioni fraudolente effettive fornite da 21 rispondenti

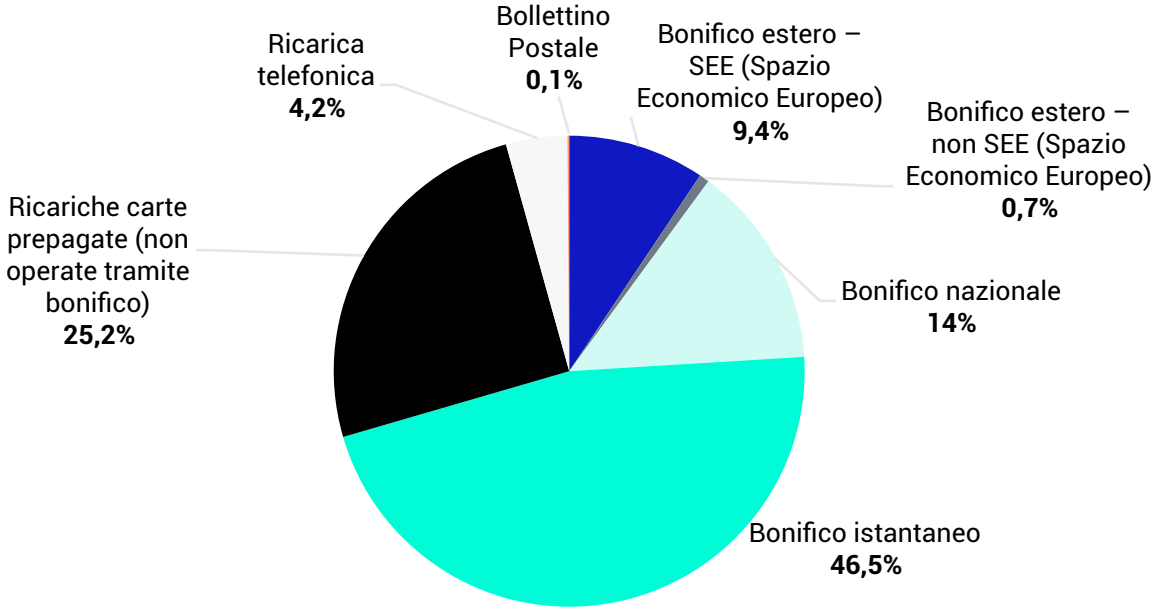


Figura 2.6 **Dimensionamento numero accadimenti per tipologia di transazione* - Ripartizione tra transazioni bloccate/ recuperate ed effettive (segmento Retail)**

*Elaborazione sul totale di transazioni anomale rilevate da 21 rispondenti

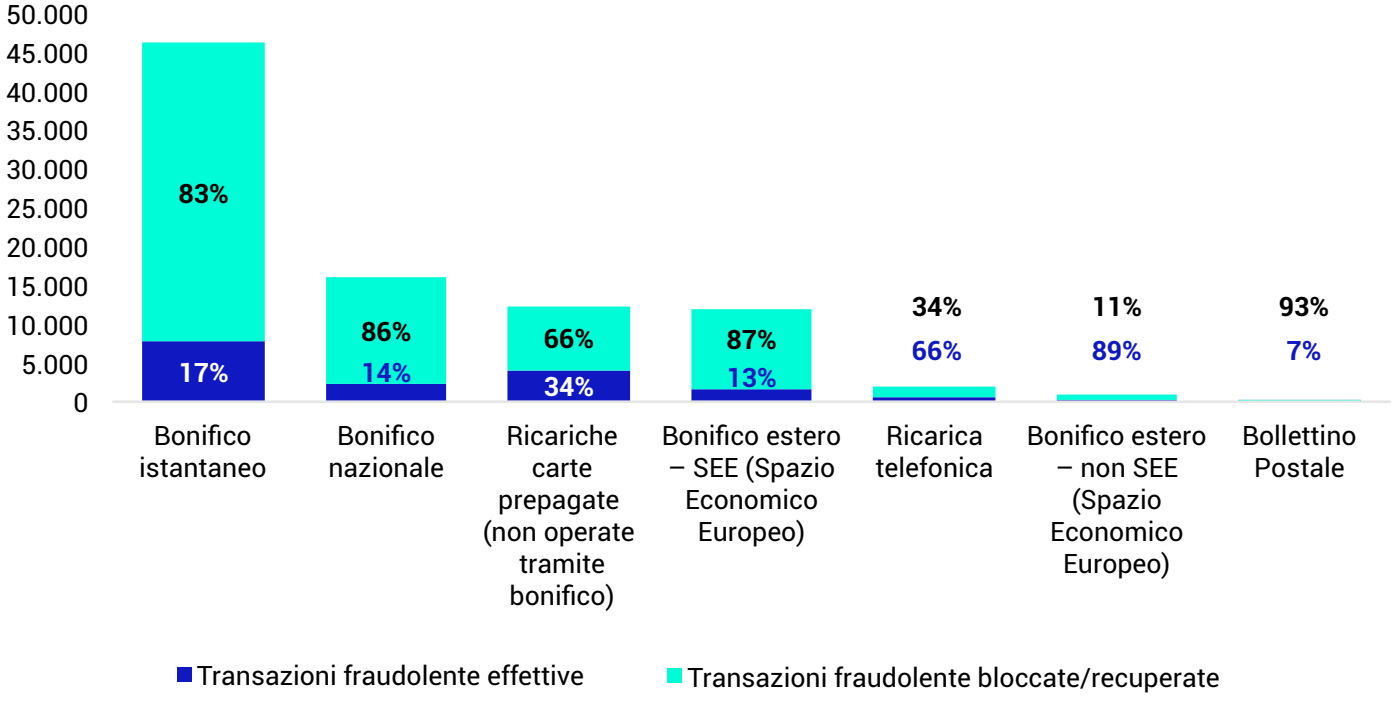


Figura 2.7

Ripartizione percentuale tra tipologie di transazioni anomale (bloccate, recuperate ed effettive) - analisi sul numero di accadimenti* (segmento Retail)

*Ripartizione percentuale sul totale di transazioni fraudolente effettive fornite da 21 rispondenti

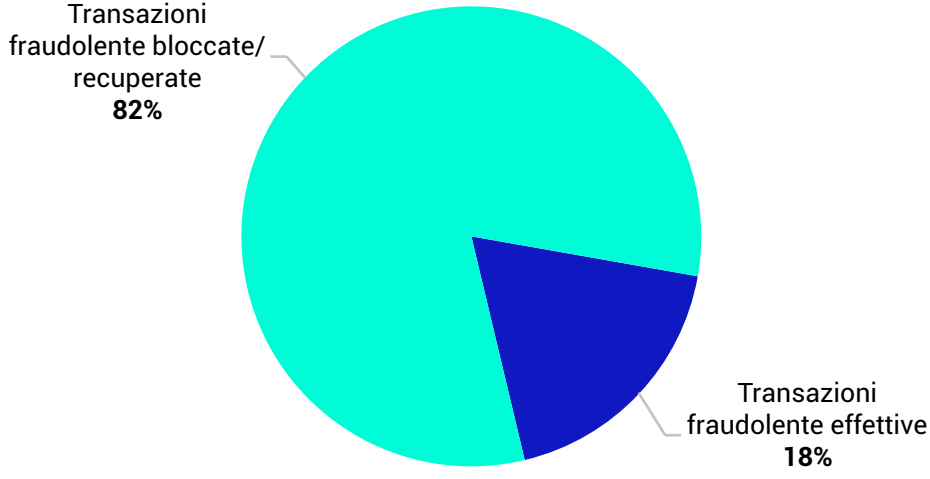
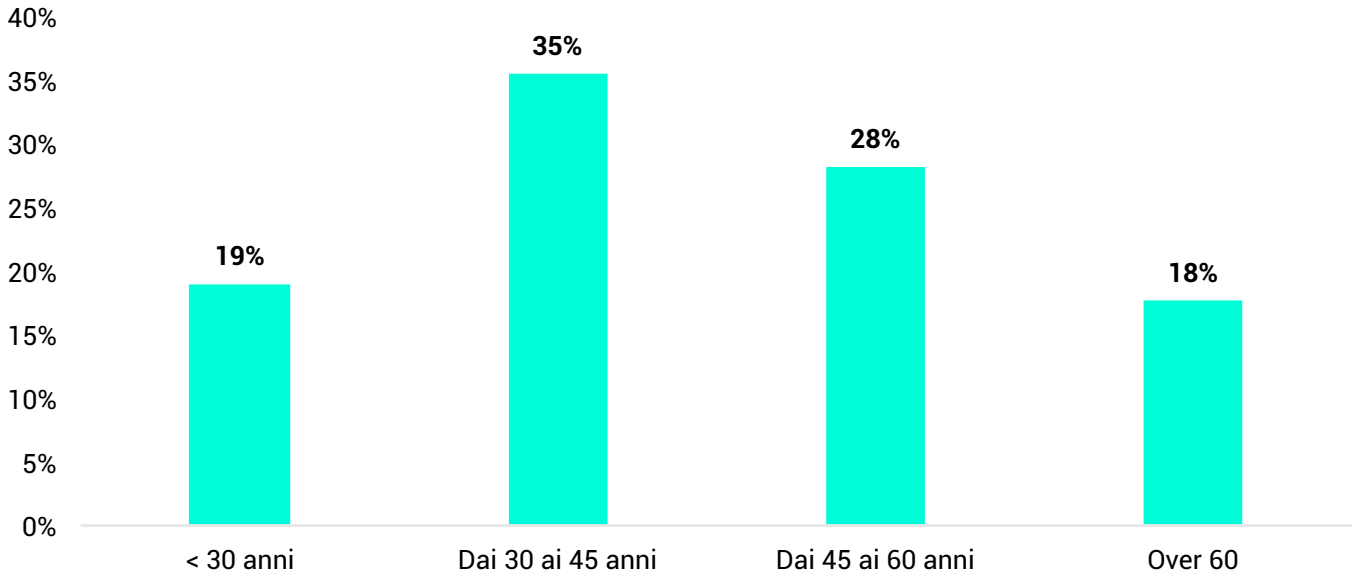


Figura 2.8 **Distribuzione percentuale dell'età delle vittime di transazioni anomale* (segmento Retail)**

*Ripartizione percentuale sul totale di transazioni fraudolente effettive fornite da 10 rispondenti



Le transazioni fraudolente bloccate, recuperate ed effettive - analisi su Clientela Corporate

Passando all'analisi del segmento delle imprese, il **bonifico nazionale** continua ad essere lo strumento prevalente nell'esecuzione dell'attacco (figure 2.9 e 2.10, rispettivamente rappresentanti la ripartizione percentuale delle tipologie di transazioni fraudolente bloccate/recuperate e la ripartizione percentuale delle tipologie di transazioni fraudolente effettive).

Soffermando l'attenzione sulle transazioni bloccate e recuperate, il bonifico istantaneo diminuisce notevolmente, passando da circa il 20% al 5% del totale, mentre risultano invariati i bonifici esteri.

Sul campione di 21 istituti rispondenti, l'analisi delle transazioni fraudolente effettive evidenzia che anche per tale comparto la voce **ricariche di carte prepagate** è particolarmente elevata (20,2%, da sottolineare che frodi con tale strumento nel 2019 non erano state segnalate da nessun istituto). Rispetto allo scorso anno va anche notato un aumento della quota di frodi su bonifici istantanei (passati da circa il 7% a oltre il 20%). In sostanza, si assiste a una mutata composizione delle frodi effettive: mentre nel 2019 oltre 4/5 delle frodi effettive era stata registrata sui bonifici nazionali, quest'anno l'efficacia dell'azione degli attaccanti si è rivelata su una **maggiore varietà di strumenti**.

La criticità delle frodi sui bonifici istantanei, già rilevata sul fronte Retail, viene confermata anche dalla figura 2.11 (si ricorda per una migliore lettura che l'altezza dei singoli istogrammi rappresenta il totale dei casi rilevati per ogni tipologia di strumento): su 100 transazioni anomale, si registrano i 2/3 di frodi effettive (nel 2019 l'efficacia delle frodi sullo strumento era stata mediamente del 10%). Migliora invece la situazione per i bonifici nazionali (5% vs 33% del 2019).

Sempre dalla lettura della figura 2.11 si conferma inoltre la criticità emergente dello strumento ricarica di carta prepagata, con un'efficacia degli attacchi anche maggiore (55%) rispetto al comparto Retail.

Il panorama della ripartizione delle transazioni fraudolente tra bloccate, recuperate ed effettive si conclude con la figura 2.12, che evidenzia sul totale delle transazioni anomale quante sono andate a buon fine e quante invece sono state bloccate ex ante o recuperate ex post. Le percentuali che emergono evidenziano che il segmento Corporate soffre meno del Retail, con il 10% dei tentativi di frode sfociati in un danno economico per la vittima.

Figura 2.9

Ripartizione percentuale delle tipologie di transazioni fraudolente bloccate e recuperate - analisi sul numero di accadimenti* (segmento Corporate)

*Ripartizione percentuale sul totale di transazioni fraudolente effettive fornite da 21 rispondenti

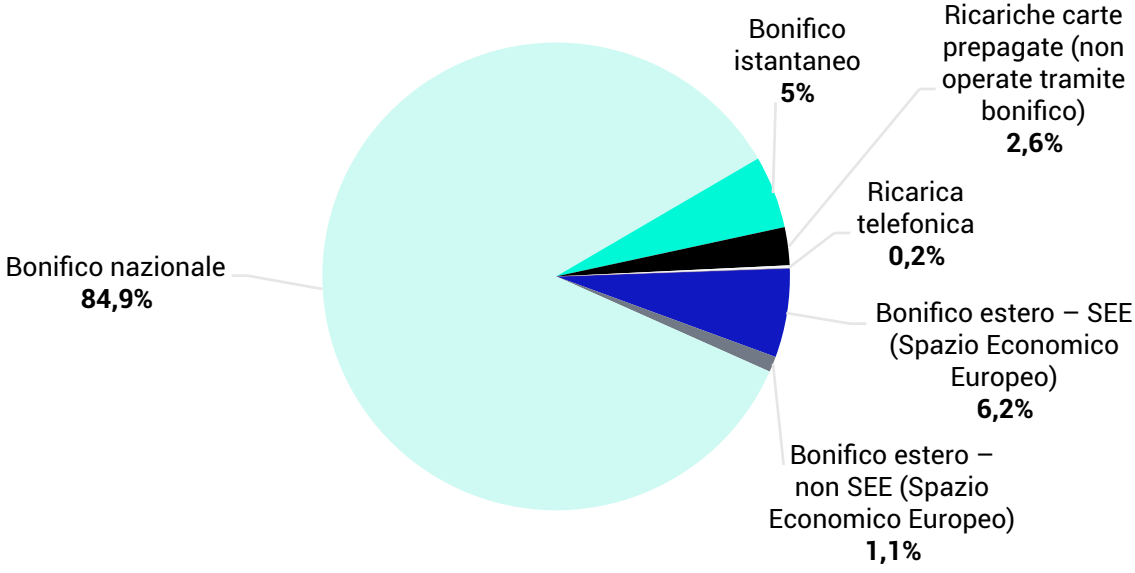


Figura 2.10 **Ripartizione percentuale delle tipologie di transazioni fraudolente effettive - analisi sul numero di accadimenti* (segmento Corporate)**

*Ripartizione percentuale sul totale di transazioni fraudolente effettive fornite da 21 rispondenti

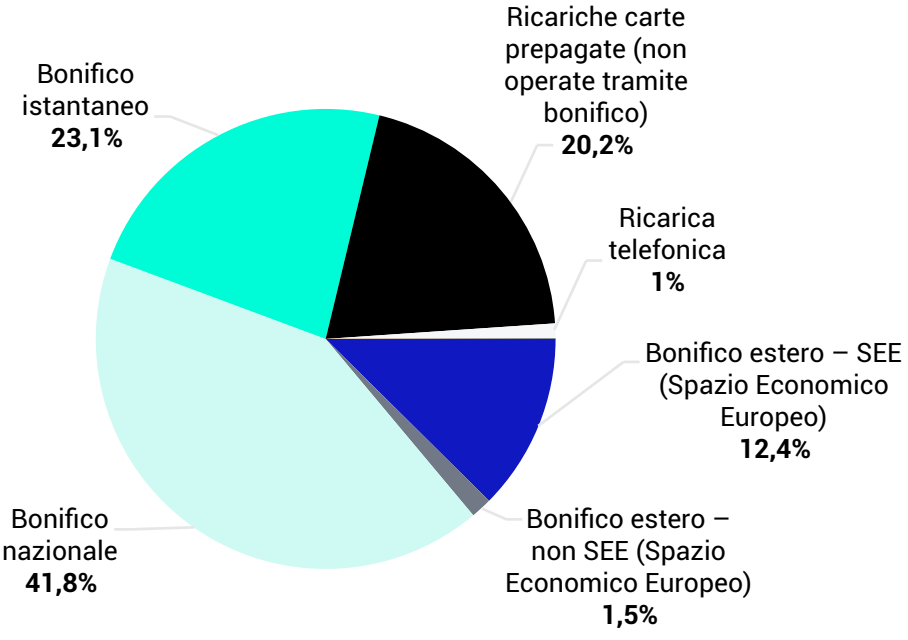


Figura 2.11 **Dimensionamento numero accadimenti per tipologia di transazione* - Ripartizione tra transazioni bloccate/recuperate ed effettive (segmento Corporate)**

*Ripartizione percentuale sul totale di transazioni fraudolente effettive fornite da 21 rispondenti

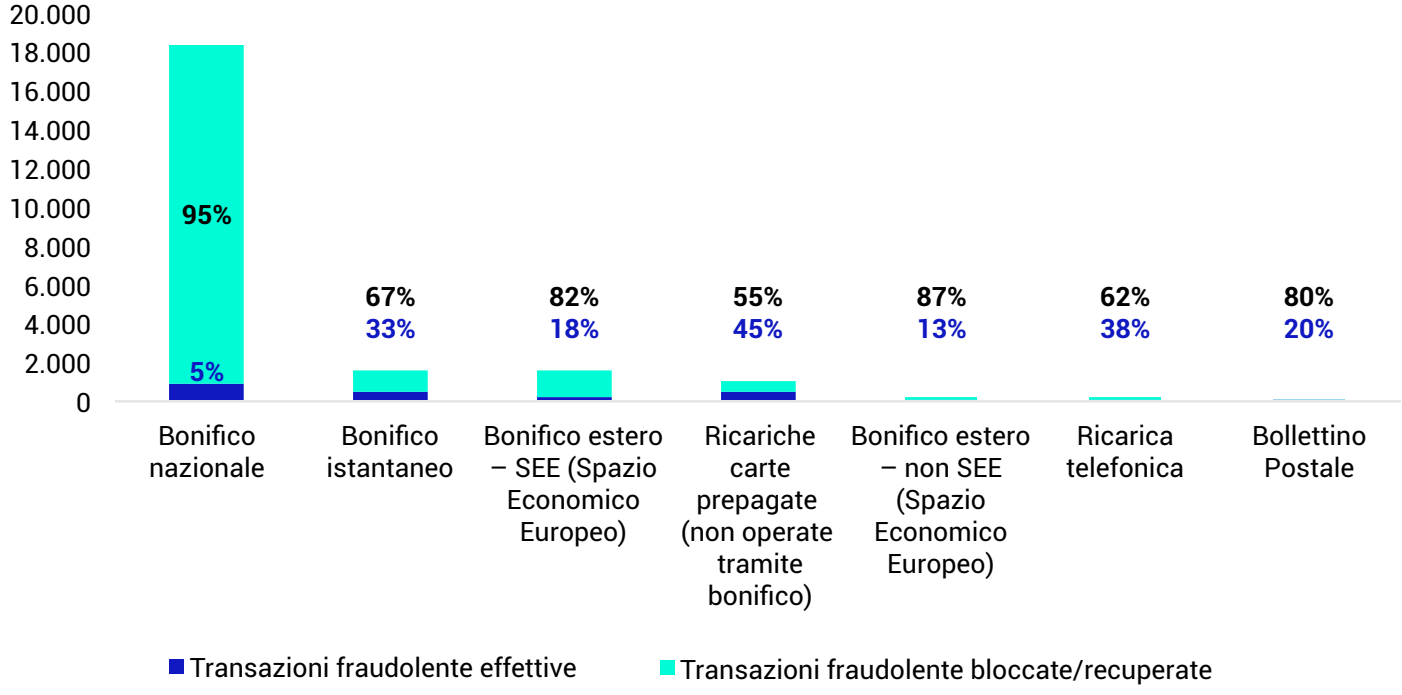
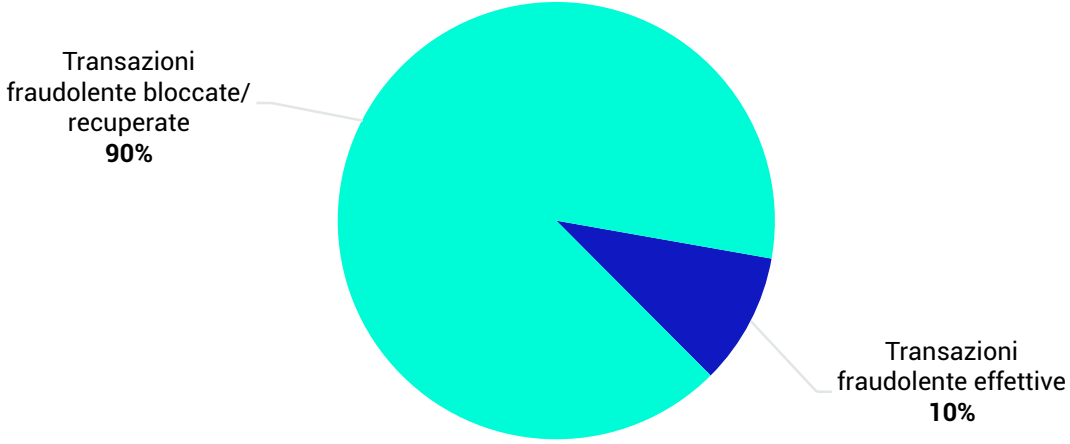


Figura 2.12 **Ripartizione percentuale tra tipologie di transazioni anomale (bloccate, recuperate ed effettive) - analisi sul numero di accadimenti* (segmento Corporate)**

*Ripartizione percentuale sul totale di transazioni fraudolente effettive fornite da 21 rispondenti



Le transazioni fraudolente bloccate, recuperate ed effettive - analisi su Clientela R&C

Comparando le risultanze emerse per i due segmenti, nel seguente paragrafo si illustrano:

- la ripartizione delle transazioni anomale registrata nel 2019 tra il comparto Retail e quello Corporate;
- la ripartizione tra transazioni fraudolente bloccate/recuperate ed effettive, aggregando i dati dei due segmenti.

Il primo grafico (2.13) conferma il trend registrato anche negli scorsi anni: il segmento Retail è il "preferito" dai frodatori, con circa i 4/5 delle transazioni anomale.

Le considerazioni emerse nei paragrafi precedenti sul rapporto tra transazioni fraudolente bloccate/recuperate ed effettive sono confermate invece dal grafico 2.14, dove le seconde cubano il 17% delle anomale totali.

Da segnalare, comunque, che **la capacità degli istituti di contrastare il fenomeno delle frodi informatiche resta buona, con oltre 4 tentativi su 5 che vengono tempestivamente bloccati o recuperati in seguito alla movimentazione di denaro dal conto corrente della vittima**.

Figura 2.13 **Totale transazioni anomale (bloccate, recuperate ed effettive)* - ripartizione numero accadimenti tra Retail e Corporate**

*Ripartizione percentuale sul totale di transazioni fraudolente effettive fornite da 21 rispondenti

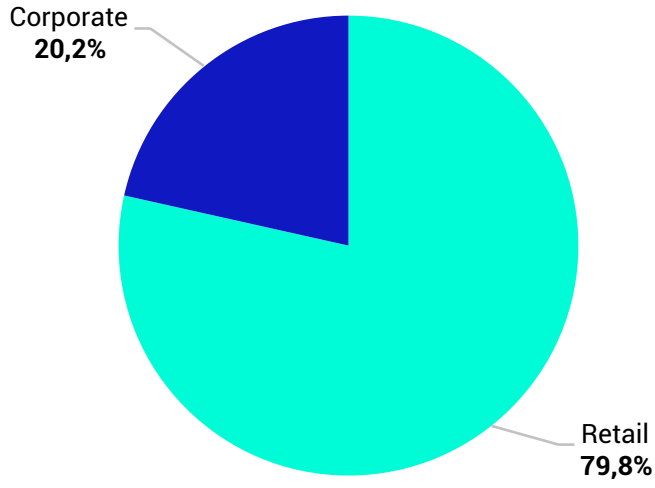
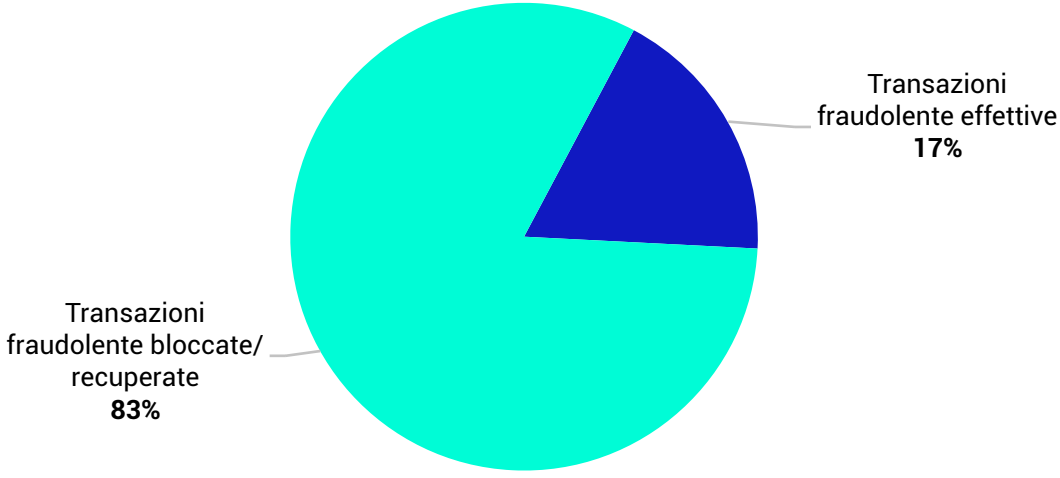


Figura 2.14 **Ripartizione percentuale delle tipologie di transazioni anomale (bloccate, recuperate ed effettive)* - analisi sul numero di accadimenti (complessivo Retail e Corporate)**

*Ripartizione percentuale sul totale di transazioni fraudolente effettive fornite da 21 rispondenti



Distribuzione geografica delle frodi - Analisi su tutta la clientela

Anche quest'anno la survey ha chiesto di indicare verso quali Paesi sono indirizzate prevalentemente le transazioni fraudolente. La figura 2.15, che sulle ascisse riporta quante volte un Paese è stato segnalato come destinatario di tentativi di frode ("Paese 1" se principale destinazione o "altro", se secondaria) e sulle ordinate il suo peso specifico in termini di criticità, evidenzia che la **Germania** è il Paese preferito dai frodatori, seguita dalla Spagna. Rispetto al 2019, si segnala un netto aumento della loro incidenza sul fenomeno per la Lituania e il Belgio, che rispettivamente passano dall'ultima alla terza posizione e dalla settima alla quarta, mentre migliora la situazione per Francia e Portogallo.

A differenza del 2019, diversi sono stati i rispondenti che hanno segnalato **transazioni verso Paesi non appartenenti allo Spazio Economico Europeo - SEE** (figura 2.16). Tra questi, la prima posizione è occupata dalla Gran Bretagna, segnalata dal 57% dei rispondenti. Al secondo posto troviamo la Turchia, seguita da Ucraina, Benin, Svizzera e Andorra.

Tale quadro evidenzia che i tentativi di frode non sono più concentrati soltanto verso Paesi "classici", ma si stanno muovendo verso destinazioni diverse, anche al di fuori dei confini dell'Unione Europea.

È anche per questo che si rivela sempre più importante rafforzare anche le collaborazioni extra europee, finalizzate ad una diffusa condivisione non soltanto di informazioni tecniche ma anche di pattern di attacco, così da poter definire meccanismi di prevenzione e difesa efficaci.

Figura 2.15 **Paesi destinatari di bonifici fraudolenti all'interno dello SEE - vista complessiva per Paese - segmenti R&C**

(17 rispondenti, 41 occorrenze)

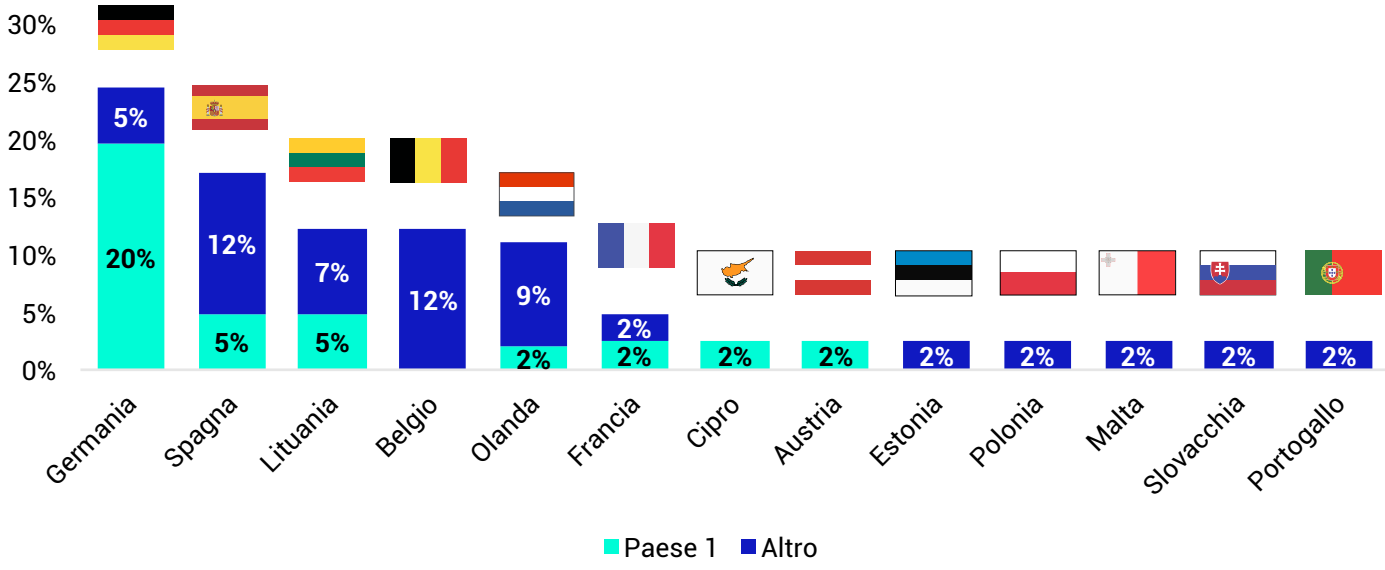
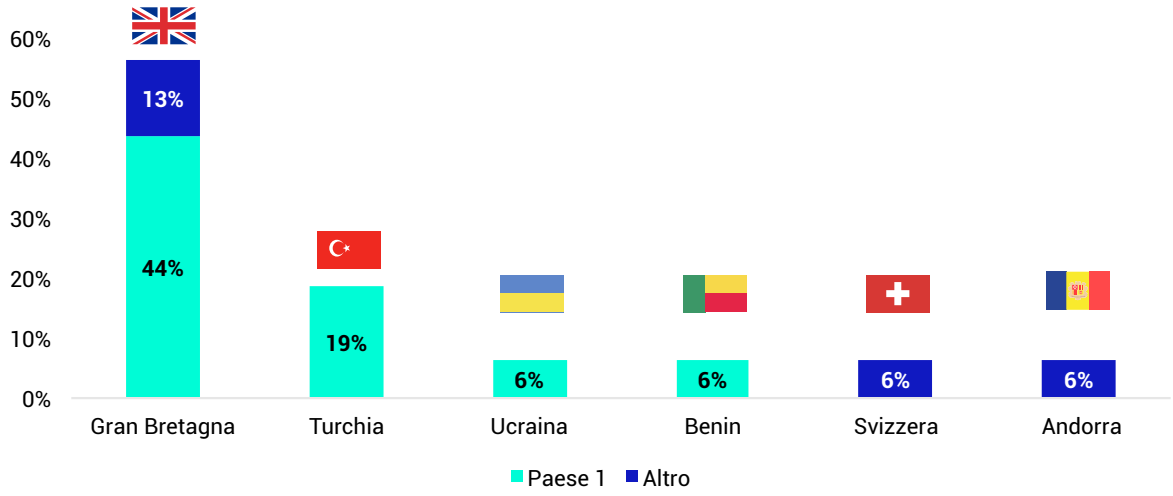


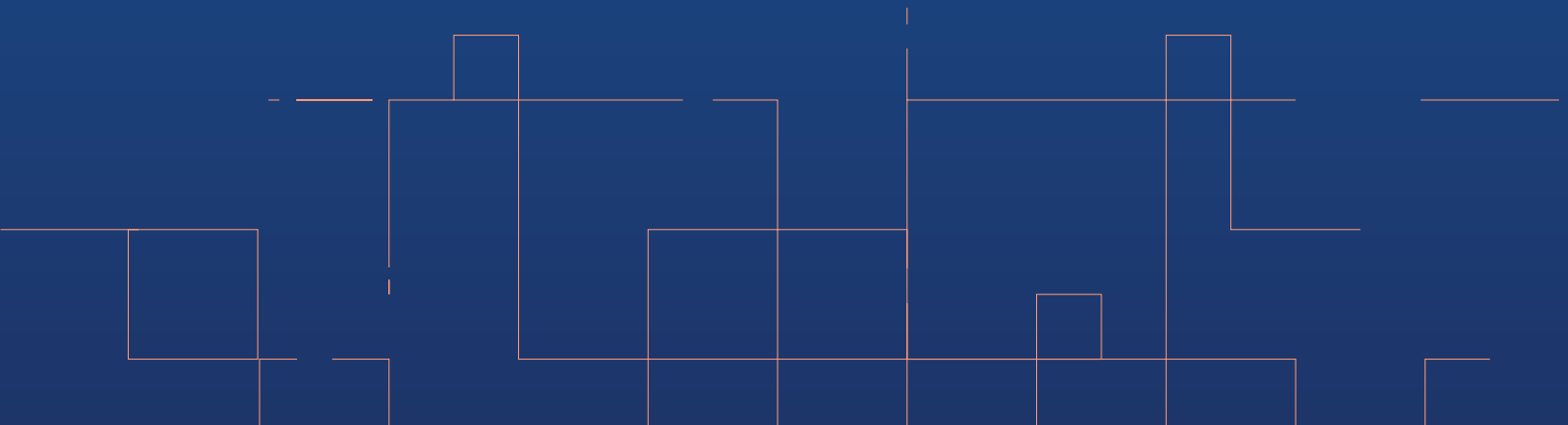
Figura 2.16 **Paesi destinatari di bonifici fraudolenti all'esterno dello SEE - vista complessiva per Paese - segmenti R&C**

(9 rispondenti, 16 occorrenze)



CERTFin

MODALITÀ DI ATTACCO



3. MODALITÀ DI ATTACCO

Lo scoppio della pandemia di Covid-19 ha stravolto le normali vite delle persone in tutto il mondo ed ha avuto un chiaro impatto anche sulle attività illecite, offrendo ai criminali informatici nuove possibilità per trarre in inganno le proprie vittime. Infatti, nel corso del 2020 abbiamo assistito ad un incremento esponenziale della creazione di siti clone, così come della diffusione di campagne di phishing e di malspam aventi come target l'utente finale. Cyber criminali di tutto il mondo hanno sfruttato a loro vantaggio il tema Covid-19, utilizzandolo come esca per distribuire trojan bancari e manipolare utenti al fine di ottenere profitti illeciti.

Con tale premessa è quindi di fondamentale importanza per gli istituti bancari conoscere i trend e le modalità di attacco utilizzati da utenti malintenzionati al fine di rafforzare i propri sistemi antifrode e indirizzare al meglio i propri sforzi al contrasto dei vari fenomeni osservati.

Come nella survey condotta lo scorso anno, la presente sezione del documento vuole approfondire le modalità di attacco finalizzate alla realizzazione di frodi. Frodi che fondamentalmente possono essere classificate in 3 macrocategorie: emissione di un ordine di pagamento da parte del frodatore, modifica di un ordine di pagamento da parte del frodatore (ad esempio attacchi di tipo MITB) e manipolazione operata dal frodatore a danno del pagatore (es. BEC o Invoice Fraud).

Le domande proposte nella survey hanno come obiettivo quello di rivelare quali sono le tecniche di attacco e pattern utilizzati dai criminali informatici per colpire i clienti degli istituti bancari utilizzando i canali Internet Banking e Mobile. Nella maggior parte dei casi di frode rilevati dai rispondenti è da evidenziare come sia molto forte la componente di social engineering per indurre le vittime a consegnare nelle mani dei frodatori dati sensibili e credenziali bancarie. In particolare, il segmento Retail risulta essere l'obiettivo primario di frodatori che utilizzano tecniche di social engineering, anche in combinazione tra loro, come l'utilizzo di tecniche di Smishing e Vishing, mentre la clientela Corporate risulta essere maggiormente soggetta a frodi perpetrate tramite l'utilizzo di malware, molti dei quali con funzionalità di tipo MITB. Altro dato da non sottovalutare è il maggior numero di casi di frode identificate sul canale Internet Banking rispetto a quello Mobile ai danni della clientela Retail (figura 3.1).

Infine, si è assistito ad una diminuzione del fenomeno noto come SIM SWAP. A tal proposito, il CERTFin, nell'ambito delle proprie attività, sta promuovendo l'adozione di diverse soluzioni tecniche al fine di contrastare il fenomeno. La relativa sperimentazione, tuttora in corso, ha già fornito risultati eccellenti.

Il presente capitolo illustra i principali risultati di tali analisi.

Focus canale Internet banking - analisi Clientela Retail e Corporate

In questa sezione vengono descritte le principali modalità adottate dagli attaccanti al fine di realizzare frodi attraverso il canale Internet Banking ai danni della clientela Retail e Corporate.

Con riferimento alla clientela Retail (figura 3.2), in funzione di un campione di 19 rispondenti, l'utilizzo di **tecniche miste** (50%) risulta essere la principale modalità con cui i frodatori realizzano le proprie attività illecite. Tale dato conferma quanto rilevato lo scorso anno. Entrando nel dettaglio delle tipologie di tecniche usate in combinazione dai criminali, il 32% è volto all'**installazione di codice malevolo sul dispositivo della vittima**. Difatti, durante il corso del 2020 sono state incessanti le campagne di malspam che hanno sfruttato ricorrentemente temi come quello del Covid-19, ma anche continui riferimenti ad aziende di livello nazionale (INPS, ENEL, BRT, etc.), per distribuire diverse famiglie di malware come Ursnif/Gozi, Formbook, Lokibot e Agent Tesla usando allegati armati di macro malevoli. Il restante 18% si riferisce all'utilizzo di tecniche miste di **social engineering**, quali ad esempio l'utilizzo in combinazione delle tecniche di Smishing e Vishing. In questo scenario, sono stati molti i casi segnalati di **ricezione di SMS**, apparentemente inviati dalla propria banca, che invitano la vittima ad accedere a pagine clone, spesso realizzate molto accuratamente, che inducono la vittima a fornire diversi dati quali le proprie credenziali. Una volta che la vittima inserisce le proprie credenziali, la pagina fake mostrerà quindi un messaggio di errore alla vittima informandola che verrà contattata da un operatore di banca. Nella conseguente chiamata, che arriva nel giro di pochi minuti, l'attaccante, impersonando personale di banca, induce la vittima a cedergli informazioni chiave.

La quota di frodi realizzate puramente mediante l'utilizzo di malware si attesta al 4%. Si tratta di malware che sono diffusi utilizzando altre modalità, quali ad esempio tramite l'installazione di freeware, cioè software gratuiti reperibili in rete ma che nascondono una minaccia al loro interno, i cosiddetti trojan.

Da sottolineare anche l'utilizzo della tecnica del **Vishing** (20%) a fini fraudolenti, dove l'attaccante predispone una chiamata verso il numero di telefono della vittima millantando di essere un operatore della banca, come accennato prima. Spesso, le chiamate vengono condotte mediante tecnica nota come CLI Spoofing (Calling Line Identifier Spoofing), comunemente noto come Spoofing, cioè la tecnica che permette di mascherare il numero originatore di una chiamata (su canale fonia) con una numerazione fittizia.

Al 17% si attestano le frodi realizzate mediante la tecnica classica del phishing, cioè comunicazioni a tema banking veicolate tramite e-mail con link che puntano a domini creati ad hoc.

Le frodi realizzate mediante la tecnica del SIM SWAP appaiono in netto calo, raggiungendo appena il 5%. Tale frode, costruita su più fasi, inizialmente vede i frodatori entrare in possesso di informazioni sensibili tramite diverse tecniche di social engineering o acquistando su forum underground interi set di dati messi in vendita a seguito di Data Breach ai danni di organizzazioni di ogni tipo. Nelle successive fasi, i frodatori sfruttano le informazioni personali delle vittime per richiedere la sostituzione della SIM presso il dealer dell'operatore di cui è cliente. Di conseguenza, il provider disattiva la scheda SIM originale e ne consegna una nuova al frodatore. A questo punto il frodatore si ritrova in possesso dello strumento attraverso il quale gli OTPs dispositivi sono inviati alla clientela e può così effettuare transazioni a suo piacimento.

Con riferimento alla clientela Corporate (figura 3.3), in funzione di un campione di 18 rispondenti, con il 52% di casi di frode identificati risulta essere l'installazione di codice malevolo la tecnica maggiormente sfruttata dai frodatori, in linea con quanto osservato lo scorso anno. Da sottolineare che più della metà (55%) di tali malware risultano sfruttare la tecniche del Man in The Browser (MITB). In tale forma di attacco, facente parte della famiglia di attacchi Man in the Middle, il malware viene inoculato direttamente nel sistema operativo e nel browser utilizzato dalla vittima. Inoltre, sono diversi i malware dotati di sofisticate capacità di elusione, anche contro i migliori software antivirus. Quindi una volta che il PC della vittima viene infettato

dal malware, quest'ultimo è in grado di intercettare il traffico passante tra client e server. Quando la vittima esegue un bonifico sul sito di Home Banking della propria banca, il malware modifica opportunamente l'operazione effettuando uno Swap dell'IBAN e dirottando le somme di denaro verso il proprio conto o quello di money mule. Alla luce di quanto sopra esposto, il 40% delle frodi identificate è attribuita all'utilizzo di tecniche miste che hanno come finalità l'installazione di malware.

I casi di Invoice Fraud risultano in diminuzione (5%) rispetto alla rilevazione dello scorso anno; qui il frodatore riesce con l'inganno a sostituirsi a fornitore terzi modificando, a danno del personale preposto dei pagamenti, i nuovi riferimenti bancari da utilizzare per il regolamento delle fatture. Infine, con incidenza minore (1%), è possibile osservare l'utilizzo di tecniche quali SIM SWAP, Phishing e BEC.

Focus canale Mobile - analisi Clientela Retail

In questa sezione vengono descritte le principali modalità adottate dagli attaccanti al fine di realizzare frodi attraverso il canale Mobile ai danni della clientela Retail (la clientela Corporate ha un'incidenza non significativa su questo canale).

In funzione di un campione di 13 rispondenti (figura 3.4), al pari del canale Internet Banking, le **tecniche miste** risultano essere la modalità preferita dai frodatori per realizzare attività illecite, ma in percentuale nettamente superiore (81%). Il 57% di frodi realizzate mediante tecniche miste impiegano una **combinazione di tecniche di social engineering** come l'utilizzo di smishing e vishing. Invece, con il restante 24% si attestano le **tecniche miste volte all'installazione di applicazioni malevole sul device mobile delle vittime**. Difatti, nel corso del 2020 sono stati in crescita i trend che hanno visto la distribuzione di noti trojan bancari per piattaforme Android come Cerberus, Alien e Anubis il cui obiettivo primario è quello di ottenere il controllo completo dei dispositivi infetti per sottrarre SMS, credenziali bancarie o altre informazioni sensibili. Tuttavia, si è assistito ad un incremento di applicazioni malevole, sviluppate in tempi molto brevi e quindi meno sofisticate, distribuite tramite campagne di phishing e aventi il solo scopo di esfiltrare SMS per acquisire i codici OTP.

Rispettivamente, con il 10% e 7%, figurano le tecniche del vishing e phishing utilizzate per realizzate transazioni fraudolente su canale Mobile. Con incidenza minore (1%) si riportano rispettivamente l'utilizzo di malware installato tramite altre tecniche e l'utilizzo della sola tecnica dello smishing per indurre la vittima ad inserire credenziali in siti fraudolenti.

Infine, a differenza della scorsa rilevazione, non sono stati indicati numeri significativi in merito all'utilizzo della tecnica del SIM Swap per realizzare frodi tramite il canale Mobile, registrata invece sul canale di Internet Banking.

Figura 3.1 **Confronto tra frodi realizzate sui canali Internet Banking e Mobile su numero di frodi identificate - Clientela Retail**

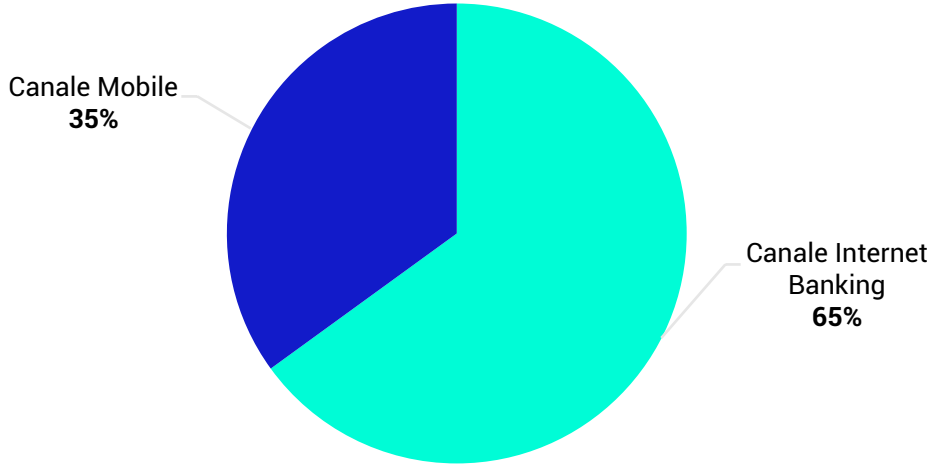


Figura 3.2 **Tipologia e distribuzione tecniche di attacco realizzate sul canale Internet Banking su numero di frodi identificate - Clientela Retail**

(19 rispondenti)

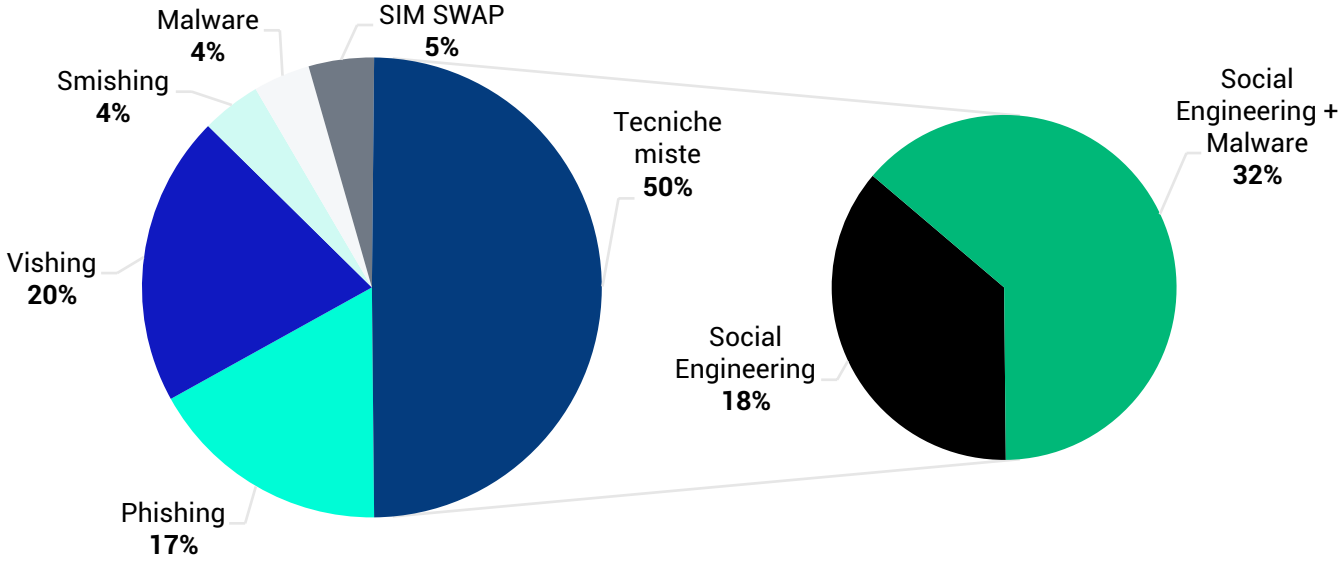


Figura 3.3 **Tipologia e distribuzione tecniche di attacco realizzate sul canale Internet Banking su numero di frodi identificate - Clientela Corporate**

(18 rispondenti)

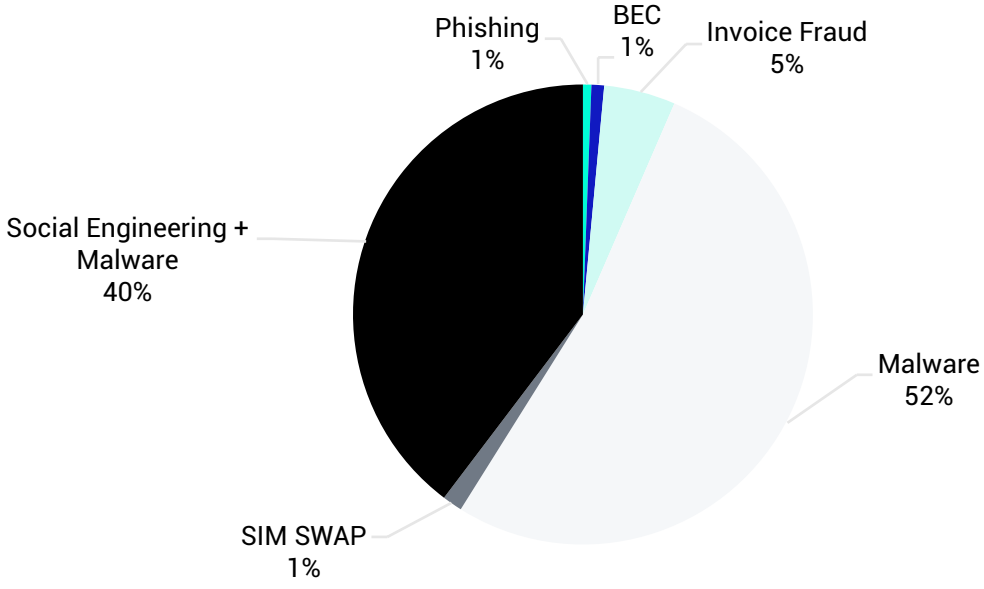
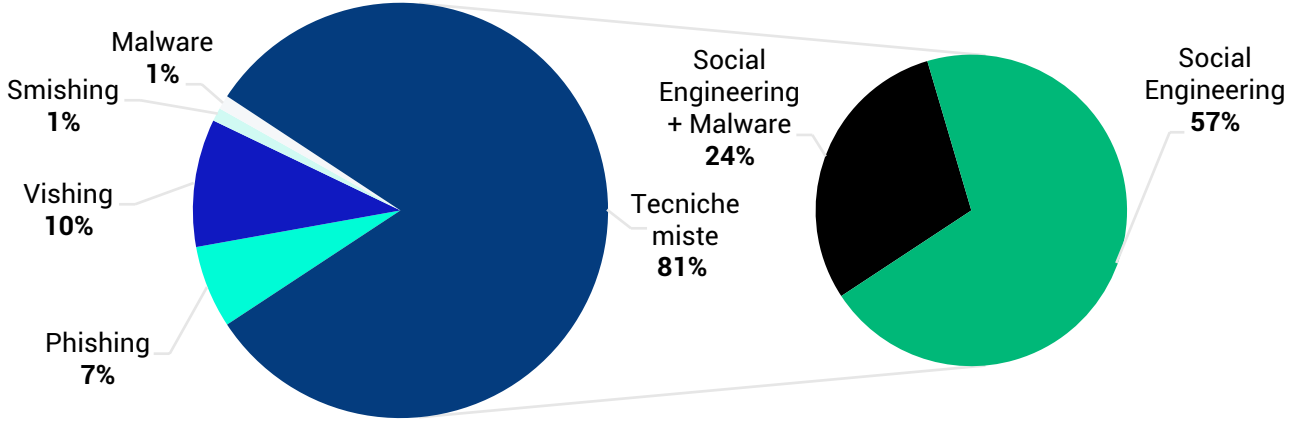


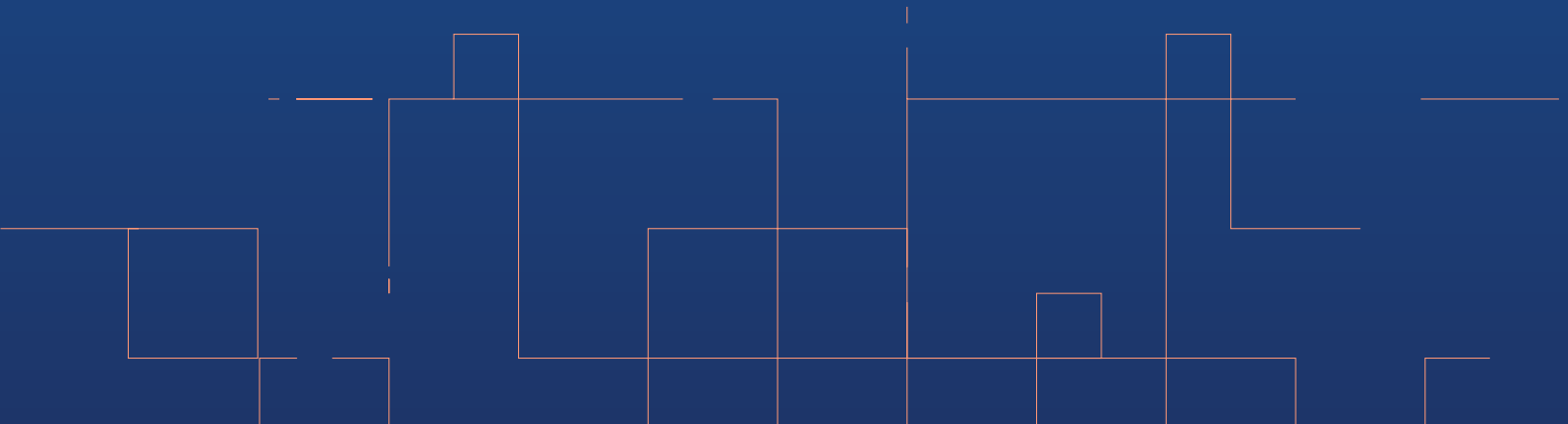
Figura 3.4 **Tipologia e distribuzione tecniche di attacco realizzate sul canale Mobile su numero di frodi identificate - Clientela Retail**

(13 rispondenti)



CERTFin

MECCANISMI DI RILEVAZIONE



4. MECCANISMI DI RILEVAZIONE

Rilevazione e segnalazione della frode - Analisi su clientela Retail e Corporate

Il monitoraggio delle transazioni operato dalla banca continua a rappresentare la modalità principale con cui vengono rilevate disposizioni di pagamento sospette o fraudolente (65% per la clientela Retail, 52% per la clientela Corporate) - figura 4.1 e figura 4.2.

Andando più in dettaglio, si osserva che l'efficienza del monitoraggio è inversamente proporzionale alla percentuale di disconoscimento del cliente, che resta la seconda modalità di rilevazione (21% nel Retail, 24% nel Corporate).

Continua a diminuire il numero di segnalazioni dovute a strumenti aggiuntivi offerti da fornitori terzi (dal 7% al 6% per il Retail, e all'8% per il Corporate) e impiegati da 1/5 dei rispondenti per la clientela Retail e da 1/6 per la clientela Corporate che però, in alcuni casi, danno luogo alla quasi totalità delle segnalazioni (tra l'85 e il 95%).

Soprattutto sul segmento Corporate acquistano rilievo (13%) segnalazioni provenienti da altre fonti.

Figura 4.1 **Fonti di segnalazione di operazioni fraudolente - segmento Retail**

(Andamento medio su 23 rispondenti)

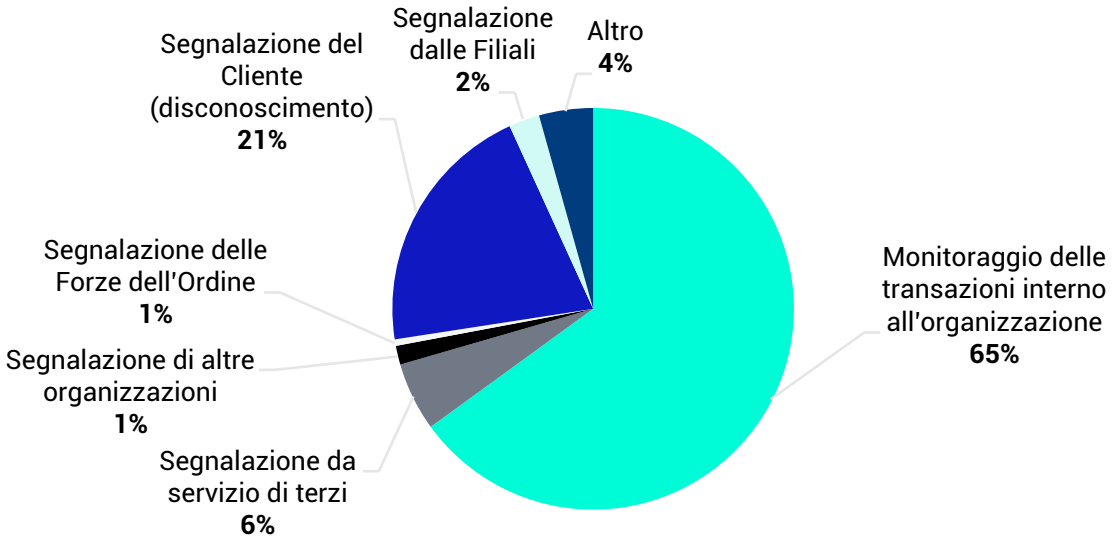
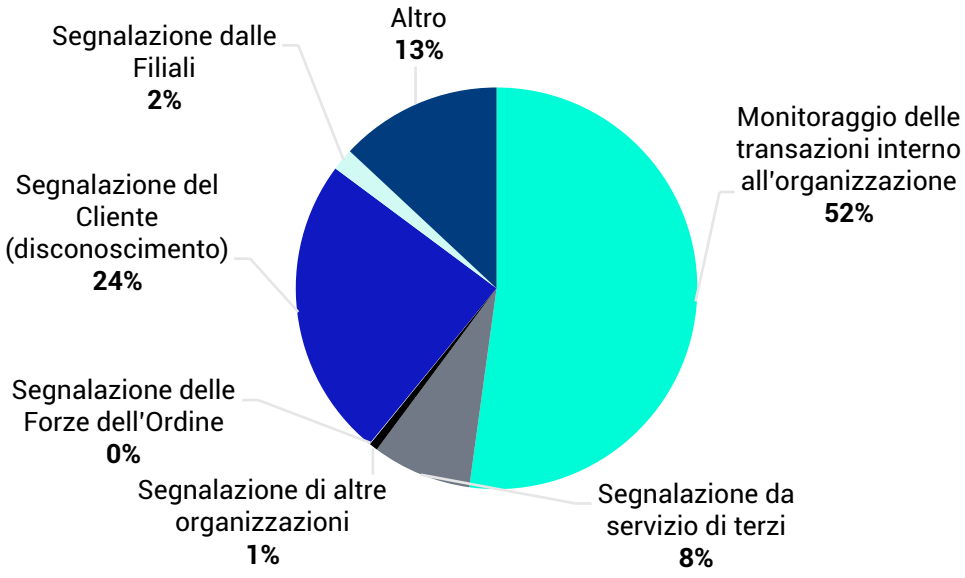


Figura 4.2 **Fonti di segnalazione di operazioni fraudolente - segmento Corporate**

(Andamento medio su 23 rispondenti)



Tecnologie di autenticazione forte

Contromisure tecnologiche di contrasto

Si registrano novità rilevanti riguardo alla distribuzione dell'utilizzo delle tecnologie di autenticazione, che nel 2020 si presentano con un panorama fortemente modificato rispetto a quello del 2019: maggiormente articolato e con una molteplicità di metodi messi a disposizione della clientela.

Tecnologie di autenticazione forte del cliente messe a disposizione in fase di accesso al conto di pagamento on line

Tra le soluzioni prese in esame per l'accesso ai conti correnti on line, le più diffuse nel segmento **Retail** (figura 4.3) sono divenute l'OTP via APP (salito all' 82%), la Push Notification (introdotta dal 74% dei rispondenti), l'OTP via SMS sceso dal primo al terzo posto (61%), il PIN (48%) e sistemi basati su dati biometrici (al 45%). Continua a scendere l'impiego dell'OTP via token (dal 42% al 35% - segnaliamo che era impiegato dall'80% dei rispondenti nel 2018). In coda la secure call (il cui impiego è comunque aumentato dal 5% al 17% dei rispondenti) e l'utilizzo di certificati digitali (4%).

Diversa la distribuzione nel segmento **Corporate** (figura 4.4) dove resiste al primo posto l'impiego dell'OTP via token (scendendo dal 80% al 61% dei rispondenti) seguito da PIN (39%) a parimerito con OTP via App e OTP via SMS, che dal 60% dello scorso anno vengono oggi segnalati dal 39% dei rispondenti. Si segnala infine l'introduzione nel segmento di nuovi metodi quali Dati Biometrici (35%), Push Notification (26%), e Secure call (13%).

Tecnologie di autenticazione forte del cliente messe a disposizione in fase autorizzativa/dispositiva

Per l'autorizzazione di operazioni da parte della clientela **Retail** (figura 4.5), vengono offerte principalmente soluzioni che prevedono l'invio di OTP tramite App (82%) o SMS (61%), fra le quali si è inserita nel 2020 la notifica Push (al 74%). Sale anche l'impiego di PIN (dal 5% al 48%), dati Biometrici (dal 26% al 45%) e OTP via Token (dal 32% al 35%).

Diversa la distribuzione nel segmento **Corporate** (figura 4.6), dove resiste al primo posto l'impiego dell'OTP via token (scen-

dendo dal 73% al 57% dei rispondenti) seguito da OTP via App e SMS che dal 60% dello scorso anno vengono oggi indicati dal 43% dei rispondenti. A questi si affiancano PIN (39%), Push Notification (35%) e dati biometrici (22%). Infine, Secure call e certificati digitali sono resi disponibili dal 17% dei rispondenti.

Figura 4.3 **Tecnologie di autenticazione forte del cliente in fase di accesso al conto di pagamento on line - livello di diffusione***

(segmento Retail, 23 rispondenti)

* Ciascun rispondente può prevedere più soluzioni di autenticazione forte del cliente

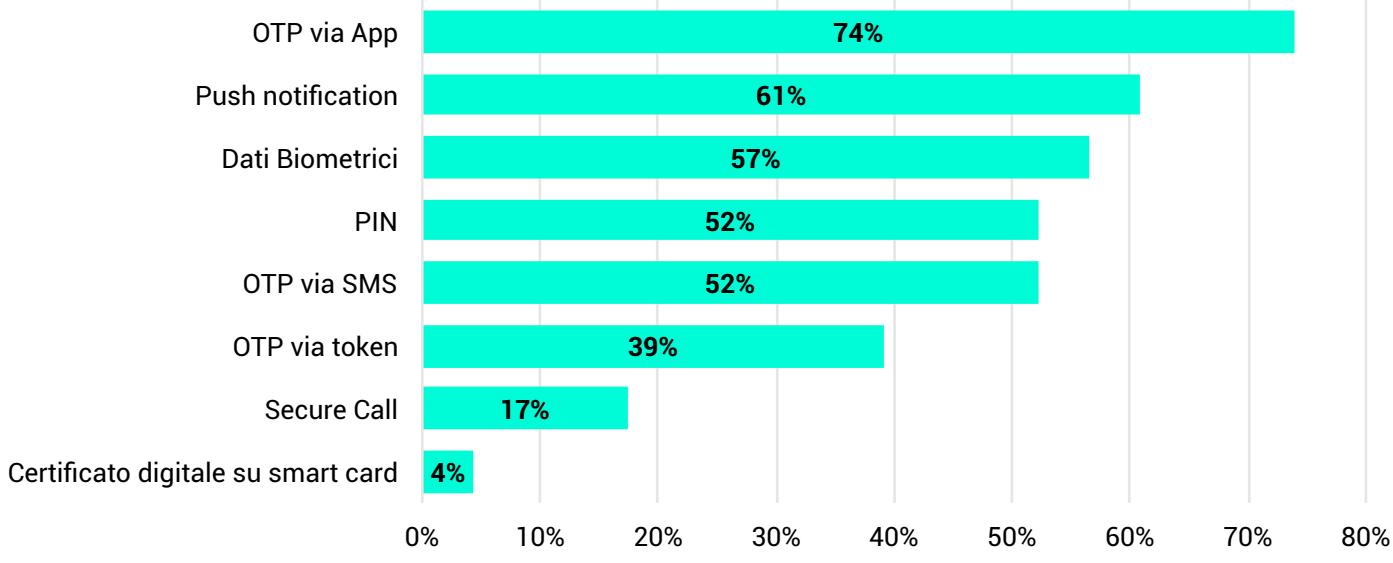


Figura 4.4 **Tecnologie di autenticazione forte del cliente in fase di accesso al conto di pagamento on line - livello di diffusione***

(segmento Corporate, 23 rispondenti)

* Ciascun rispondente può prevedere più soluzioni di autenticazione forte del cliente

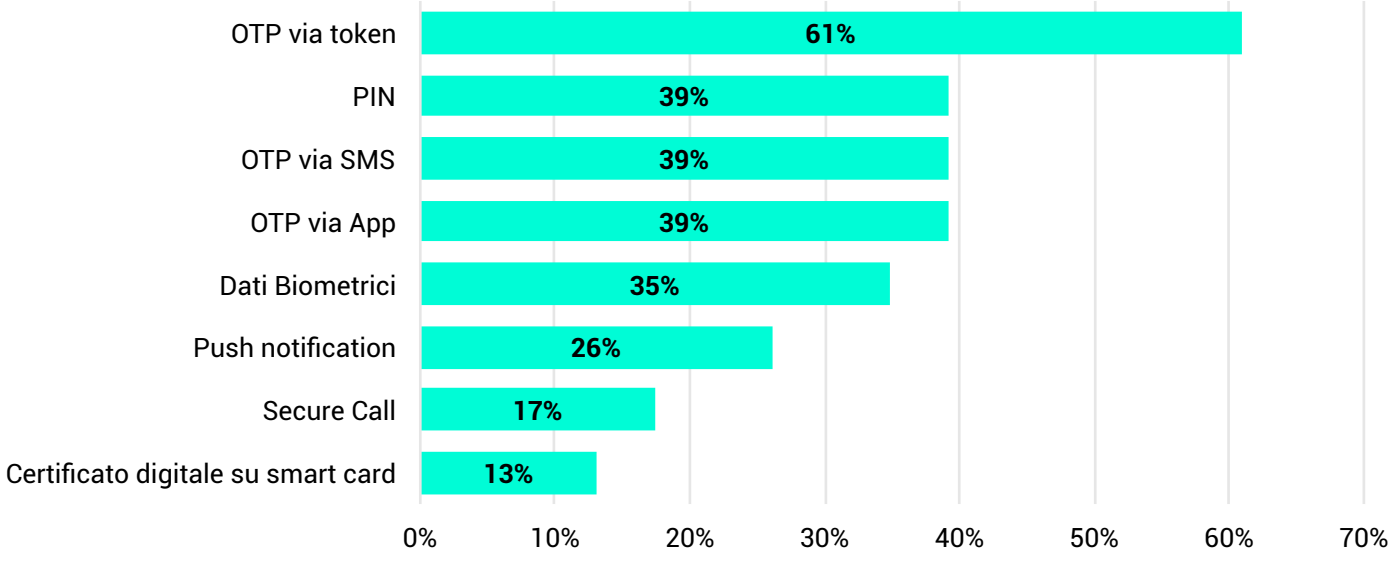


Figura 4.5 **Tecnologie di autenticazione forte del cliente in fase autorizzativa/dispositiva - livello di diffusione***

(segmento Retail, 23 rispondenti)

* Ciascun rispondente può prevedere più soluzioni di autenticazione forte del cliente

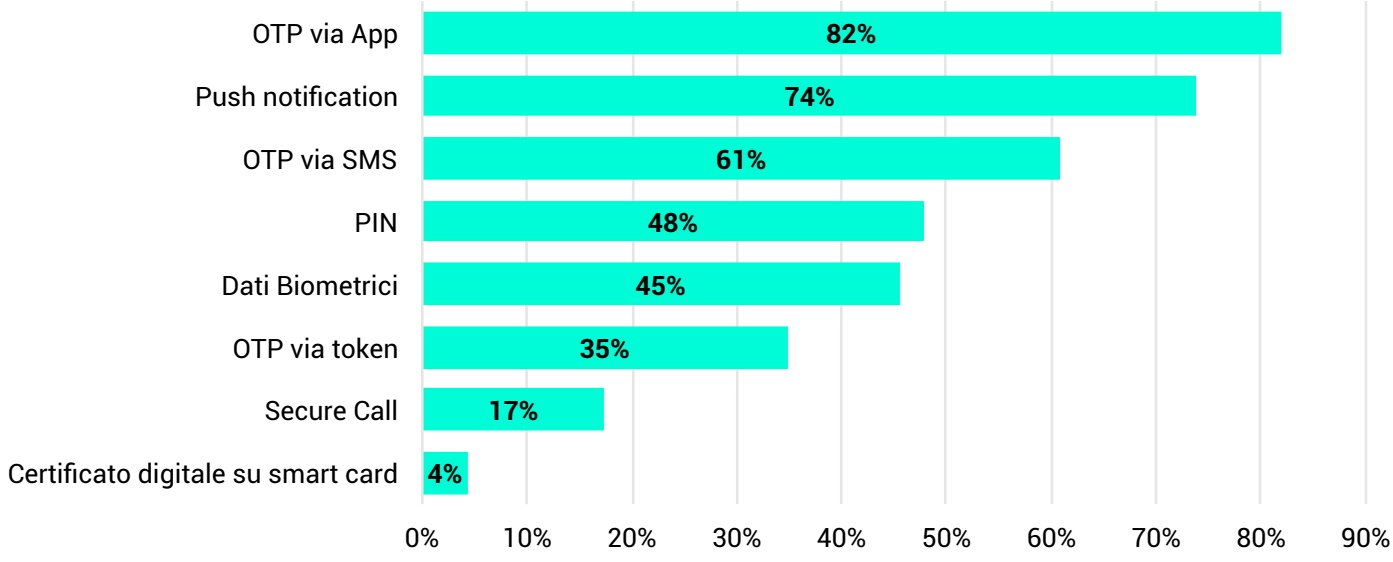
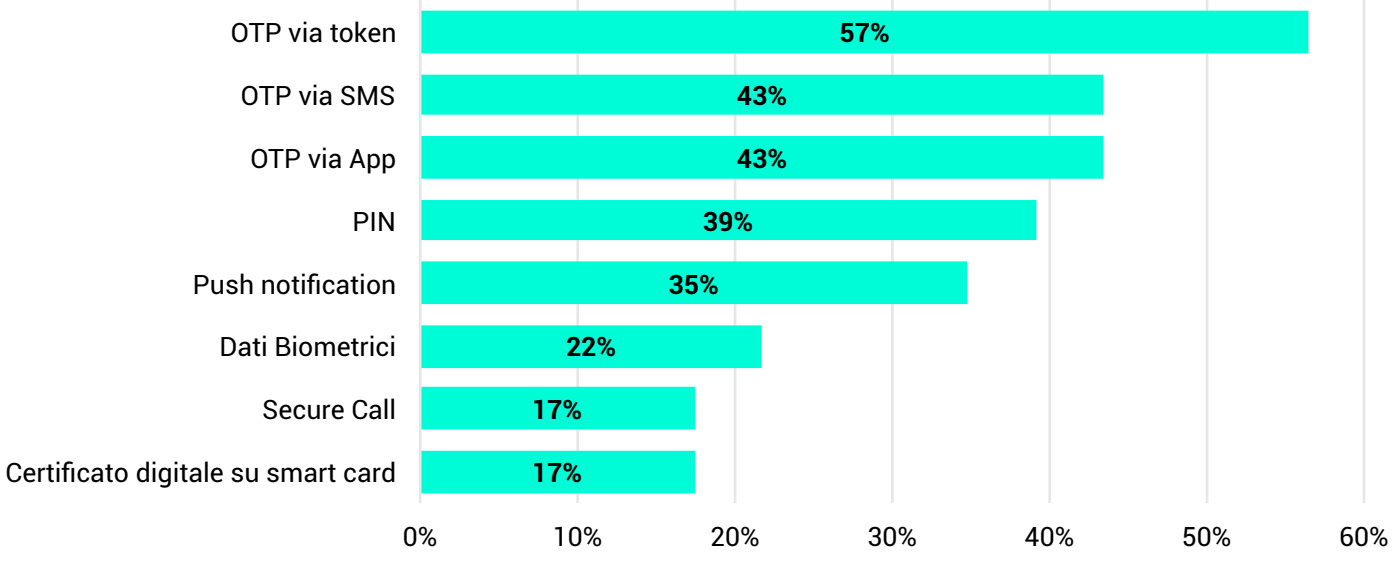


Figura 4.6 **Tecnologie di autenticazione forte del cliente in fase autorizzativa/dispositiva - livello di diffusione***

(segmento Corporate, 23 rispondenti)

* Ciascun rispondente può prevedere più soluzioni di autenticazione forte del cliente



Le azioni verso la clientela - segmento Retail e Corporate

L'uso corretto e consapevole degli strumenti bancari richiede la comunicazione con i propri clienti per condividere aggiornamenti e raccomandazioni su un corretto uso dei device e su buone pratiche di comportamento nella gestione di credenziali e strumenti di pagamento. A tale scopo le banche sfruttano tutti i diversi canali disponibili.

A conferma dell'importanza di tale attività, **tutte le banche rispondenti dichiarano di utilizzare più canali di comunicazione con i propri utenti Retail per i temi cyber** (figura 4.7), prediligendo, nell'ordine, il portale di Internet Banking (91%), l'email (83%), l'informativa su social network (65%), via Mobile app (61%) e presso le filiali (61%). Al 43% si attestano invece le informative contrattualistiche ed altri mezzi di comunicazione (al 22%).

I clienti sono periodicamente informati in merito a diverse tematiche che vanno da un uso corretto dei dispositivi per realizzare operazioni bancarie a distanza a buone pratiche nella gestione di credenziali e password. Tra i vari **argomenti presi in esame** (figura 4.9), i più condivisi con la clientela restano la gestione dell'identità e degli strumenti di sicurezza a protezione dei servizi bancari (83%), la sicurezza nell'utilizzo degli strumenti di pagamento (70%), della posta elettronica (65%), dei dispositivi quando connessi a Internet (57%) e l'utilizzo sicuro dei device mobili (61%). Ulteriori ambiti informativi riguardano i rischi legati all'e-commerce (52%), al money muling (48%) ed ai social network (39%).

Anche per la clientela **Corporate**, le banche rispondenti usano molteplici **canali di comunicazione** (figura 4.8), prediligendo, come per il Retail, il portale di Internet Banking (87%) ed informative via e-mail (cresciute dal 40% al 70%). Parzialmente diminuito il ricorso agli altri canali quali informative presso le filiali (48%), informativa contrattualistica (dal 67% al 43%). Parimenti segnalato dal 43% dei rispondenti l'impiego del social network (era al 33% nel 2019).

Anche per le **tematiche trattate** non si evidenziano particolari differenze circa le azioni di sensibilizzazione e awareness tra Retail e Corporate (figura 4.10): i più discussi sono temi di gestione sicura dell'identità (70%), l'utilizzo sicuro degli strumenti di pagamento (61%), corretto utilizzo della posta elettronica e sicurezza nell'utilizzo dei dispositivi connessi alla rete (entrambi segnalati dal 52% dei rispondenti). Seguono l'utilizzo sicuro dei device mobili (48%), il fenomeno del money muling (39%), i rischi legati all'e-commerce e ai social network (entrambi al 35%).

Figura 4.7 **Canali di di informazione alla clientela Corporate su tematiche di sicurezza cyber e frodi**

(23 rispondenti)

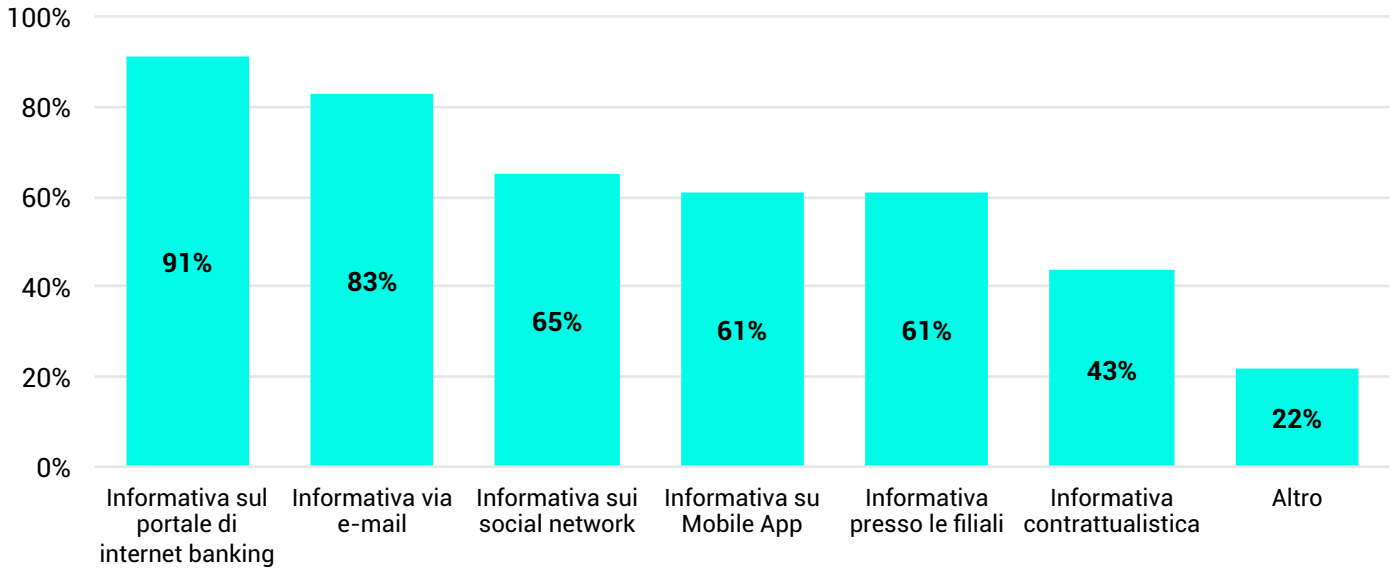


Figura 4.8 **Canali di di informazione alla clientela Corporate su tematiche di sicurezza cyber e frodi**

(23 rispondenti)

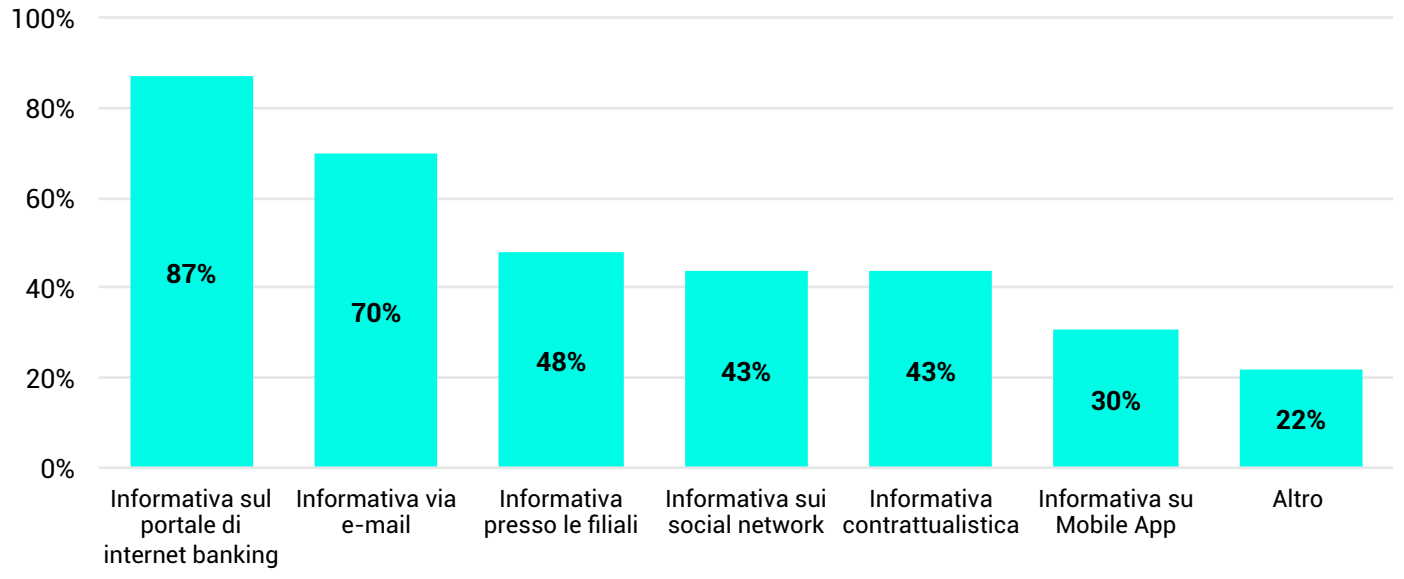


Figura 4.9 **Tematiche di sicurezza cyber e frodi affrontate con la clientela Retail**

(23 rispondenti)

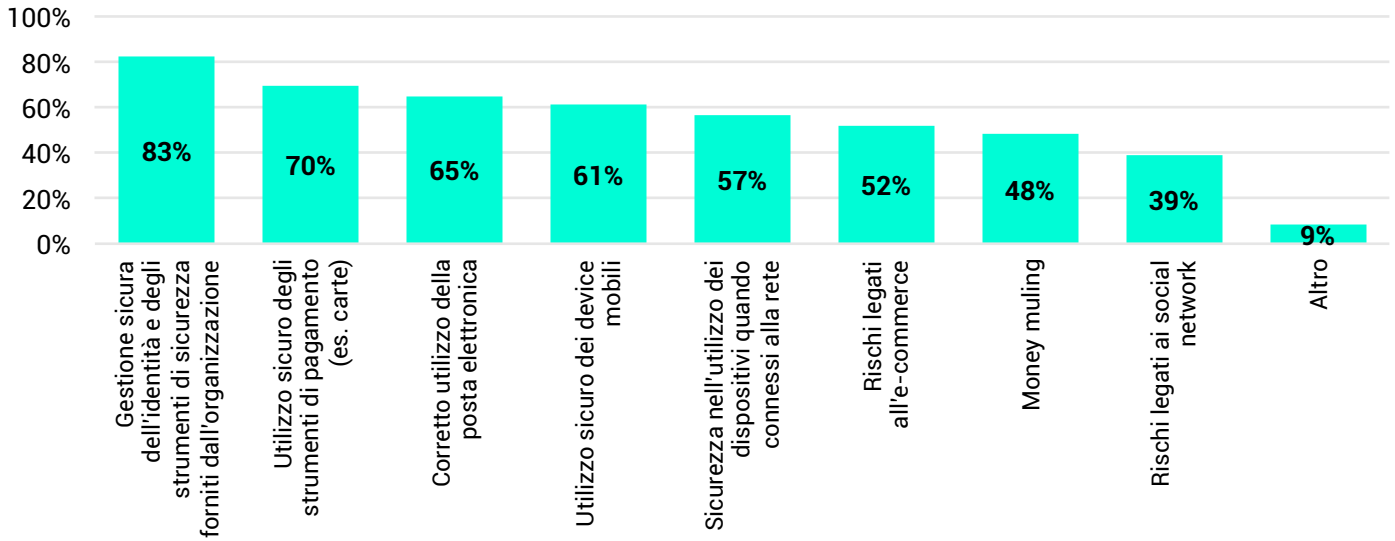
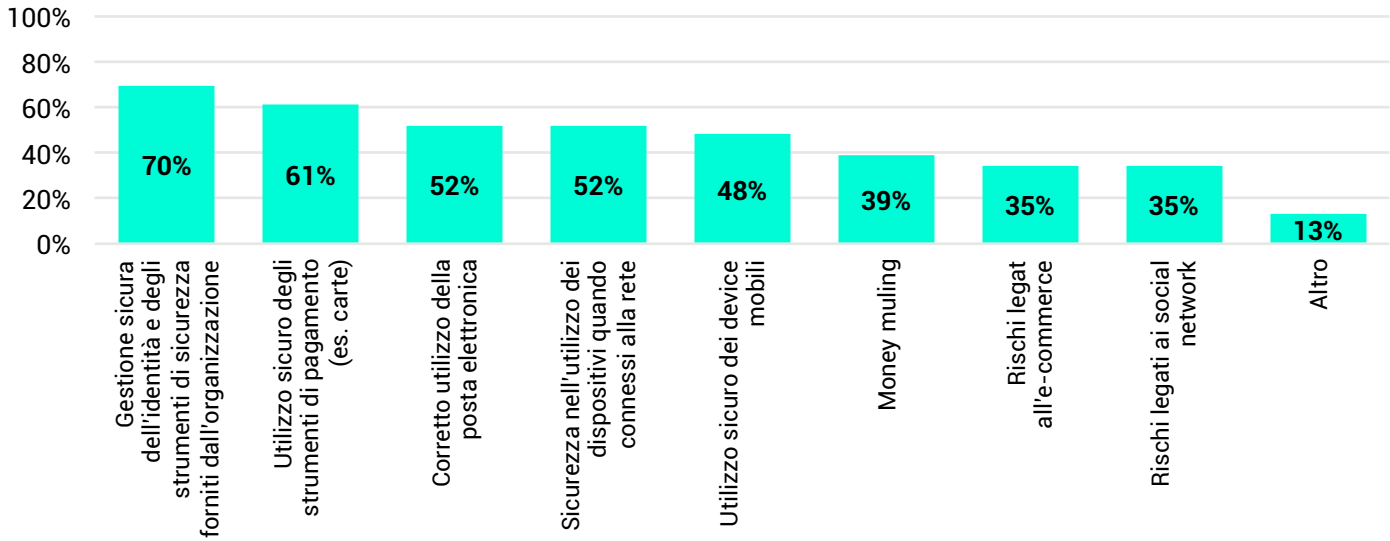


Figura 4.10 **Tematiche di sicurezza cyber e frodi affrontate con la clientela Corporate**

(23 rispondenti)



Le azioni di contrasto interne della banca

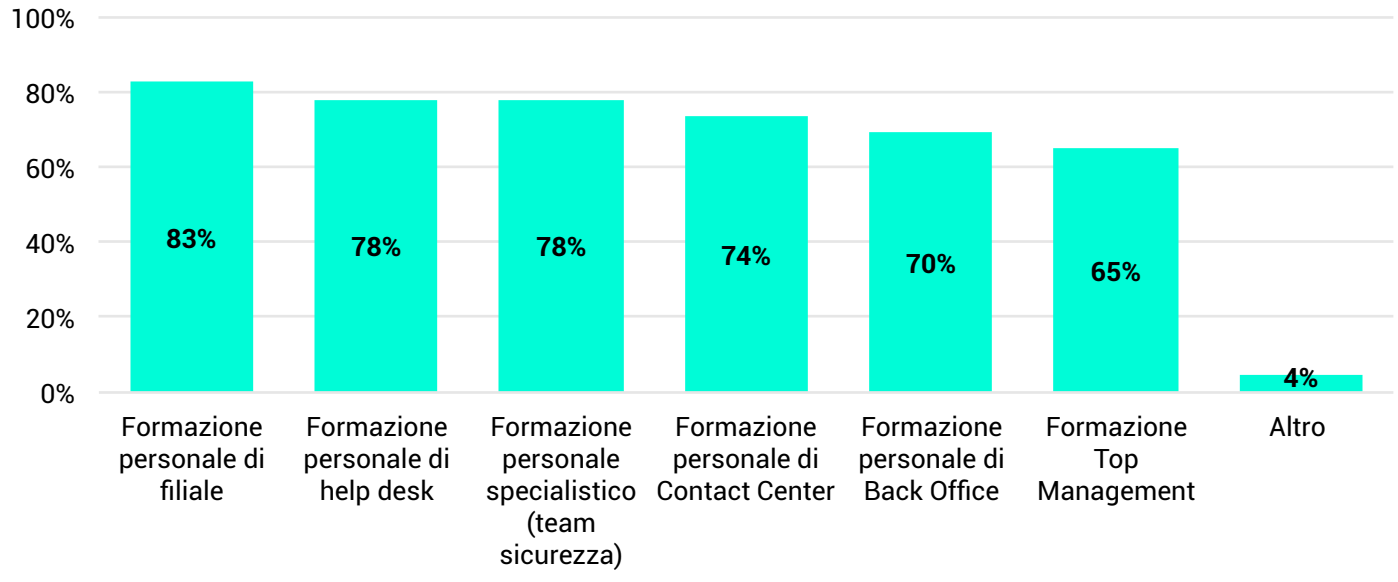
Come già evidenziato nei precedenti capitoli del Report, molti meccanismi di attacco fanno leva sul fattore umano come elemento di vulnerabilità attraverso cui collezionare informazioni utili alla realizzazione di operazioni malevole o di intrusioni nei sistemi informatici, sfruttando procedure sempre più evolute e sofisticate unite a tecniche di social engineering. Per questa ragione risulta fondamentale attuare iniziative di training e awareness per il personale interno. A questo si è aggiunta nel 2020 l'esigenza di potenziare il supporto alla clientela in ragione della difficoltà indotte dalla pandemia.

Le **attività di formazione** (figura 4.11) hanno interessato complessivamente tutte le famiglie professionali. In particolare, nel 2020, le azioni sono state diffuse verso l'intera organizzazione, a partire dal personale di filiale (83%), di help desk e di sicurezza (entrambi citati dal 78% dei rispondenti). La stessa attenzione è stata rivolta anche al personale di Contact Center (74%), back office (70%) e Top Management (65%).

Tra i principali **argomenti affrontati nei corsi di formazione** si segnalano le seguenti tematiche: cybersecurity, contrasto alle frodi, uso corretto degli strumenti aziendali, money muling, phishing ed altre tattiche di attacco. Sono inoltre state riportate come attività formative anche simulazioni Table-Top su eventi cyber.

Figura 4.11 **Attività di formazione interna su tematiche di sicurezza cyber e frodi**

(23 rispondenti)



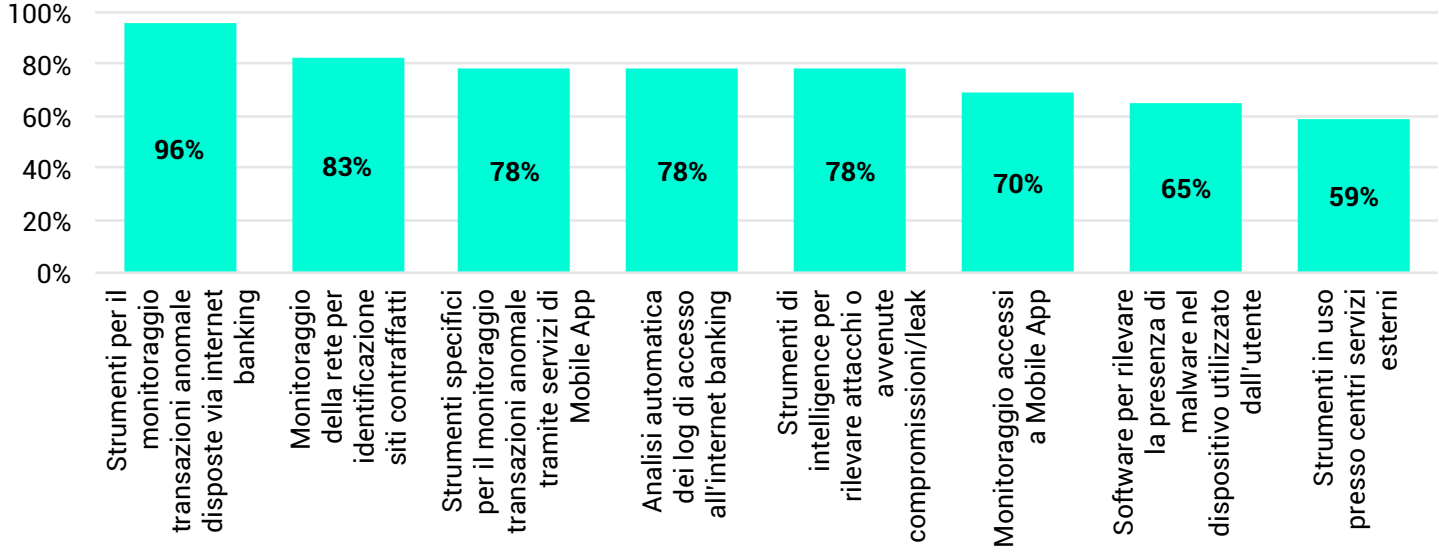
Strumenti tecnologici per il monitoraggio e la rilevazione di attacchi rivolti alla propria clientela

Le attività di monitoraggio e la relativa dotazione tecnologica sono fondamentali per una tempestiva rilevazione di attacchi e frodi. La soluzione più diffusa segnalata da quasi tutti rispondenti (figura 4.12) resta il **monitoraggio di transazioni anomale disposte via Internet banking** (96%). Sale il monitoraggio della rete per l'identificazione di siti contraffatti (dal 74% all'83%). Molto utilizzate (dal 78% dei rispondenti) il monitoraggio di transazioni anomale tramite servizi di Mobile App, l'analisi automatica dei log di accesso all'internet banking e gli strumenti di intelligence impiegati per rilevare attacchi o avvenute compromissioni/leak.

Restano inoltre diffusi il monitoraggio accessi a Mobile APP (70%), i software per rilevare la presenza di malware nel dispositivo utilizzato dall'utente (65%) e l'impiego di strumenti in uso presso centri servizi esterni (che sale dal 47% al 59%).

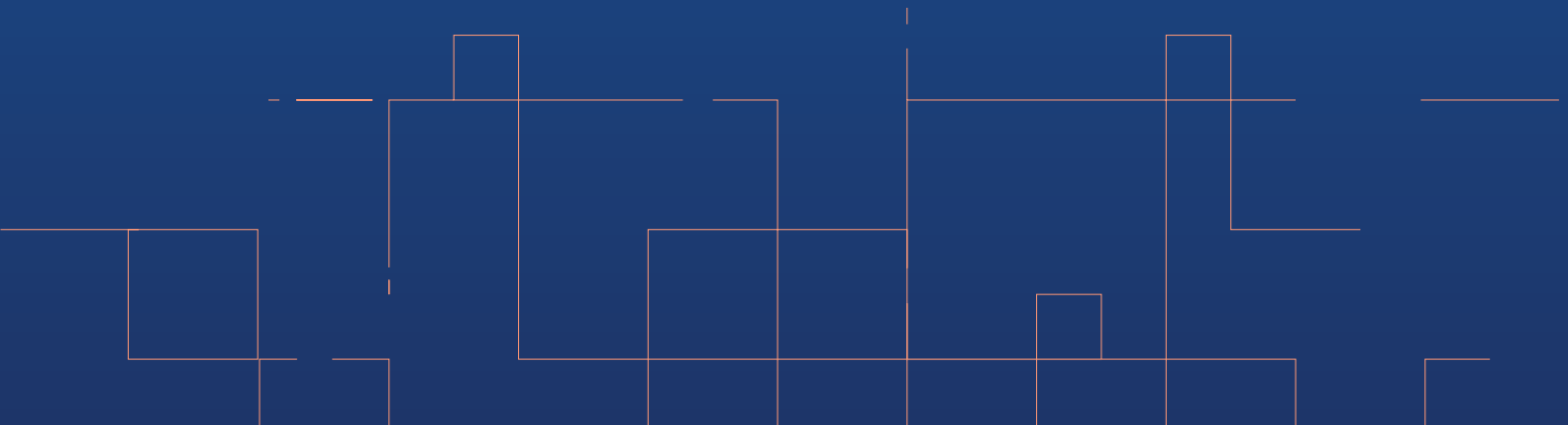
Figura 4.12 **Strumenti tecnologici per il monitoraggio e rilevazioni frodi**

(23 rispondenti)



CERTFin

ATTACCHI RIVOLTI ALLA CONFIDENZIALITÀ, INTEGRITÀ E DISPONIBILITÀ DI DATI, INFORMAZIONI E SERVIZI



5. ATTACCHI RIVOLTI ALLA CONFIDENZIALITÀ, INTEGRITÀ E DISPONIBILITÀ DI DATI, INFORMAZIONI E SERVIZI

In questa edizione 2021 del Report si è ritenuto opportuno ampliare la sezione che intende indagare la presenza di attacchi finalizzati a compromettere la confidenzialità, integrità e disponibilità di dati, informazioni e servizi dell'organizzazione offerti al cliente.

Le domande proposte mirano ad analizzare in maniera esaustiva i principali fenomeni cyber e le tecniche di attacco impiegate dai criminali per colpire le reti telematiche, i sistemi e gli asset IT della banca. Tra questi figurano i consueti data breach, DoS (Denial of Service), DDoS (Distributed DoS), RDDoS (Ransom DDoS), ransomware, cryptolocker e la tattica nascente del double-extortion.

Gli schemi di attacco RDDoS, considerati in passato come eventi straordinari, sono diventati parte integrante del panorama delle minacce per le organizzazioni di quasi tutti i settori, in conseguenza di un'evoluzione nelle tattiche degli attaccantl che, nel corso del 2020, hanno realizzato diverse campagne offensive.

In questa sezione del Report vengono illustrati i principali risultati delle suddette analisi.

Focus attacchi alla confidenzialità

Nel 2020, su un campione di 21 rispondenti, la percentuale di banche che hanno rilevato casi di **data breach** è stata pari al 42,9% (grafico 5.1), con un numero di attacchi andati a buon fine pari a 21.

Le banche hanno comunque provveduto ad attivare i piani di risposta agli incidenti, nonché il rafforzamento dei profili di sicurezza e monitoraggio degli accessi (Cloud Access Security Broker, regole FW, Multi-Factor Authentication - MFA, ricerca attività anomale, etc.), azioni di awareness e misure di prevenzione applicabili alle terze parti atte a consolidare il programma di third-party risk management.

Focus attacchi all'integrità

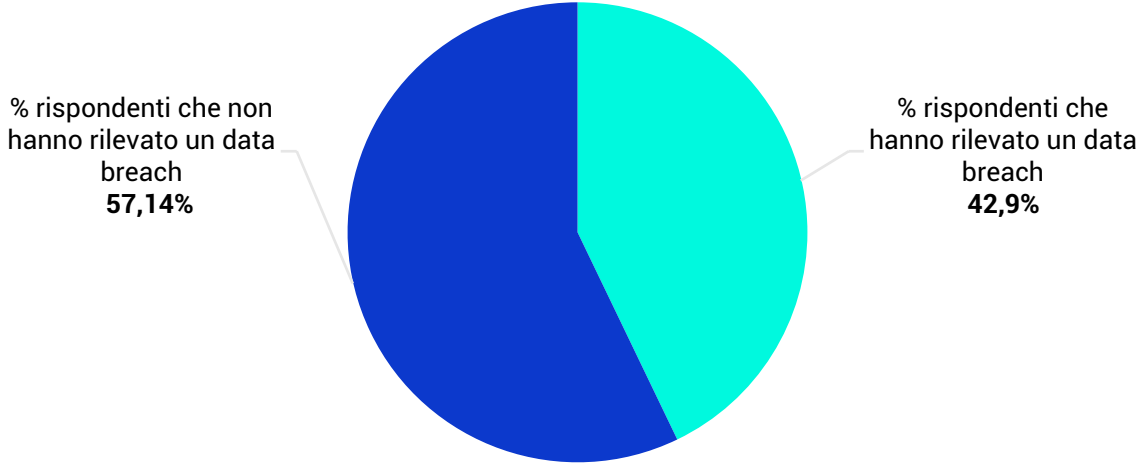
In funzione di un campione di 20 banche rispondenti solo 4 hanno rilevato attacchi all'integrità, per un totale di 293 attacchi. Questi ultimi includono principalmente **attacchi mirati alla clientela**, volti a compromettere le credenziali degli utenti finali mediante l'installazione di trojan bancari.

Per quanto concerne gli **attacchi mirati alle organizzazioni**, si è assistito a schemi e campagne di phishing veicolanti malware di diversa natura (es. Worm, Adware, Trojan, etc.), mirati a compromettere l'integrità dei sistemi mediante l'impiego di caselle di posta elettronica a loro volta compromesse. Tutti i casi sono stati contenuti prima del completamento della compromissione e/o prontamente bloccati dai sistemi di difesa perimetrali. Inoltre, non si sono registrati, per quanto noto, impatti sui dati, né sui servizi, per i singoli utenti coinvolti superiori ai tempi di ripristino delle relative postazioni infettate.

In seguito ad alcuni attacchi le banche hanno provveduto, a scopo precauzionale, al ripristino dei sistemi target, nonostante i sistemi antivirus abbiano gestito efficacemente il tentativo di infezione.

Figura 5.1 **Rilevazione dell'incidenza di data breach**

(21 rispondenti)



Focus attacchi alla disponibilità

In questo paragrafo vengono approfonditi gli attacchi volti a compromettere la disponibilità dei servizi bancari, ovvero azioni condotte al fine di generare disservizi, spesso con fini attivistici, mediante attacchi DoS (Denial of Service) e DDoS (Distributed DDoS), che consistono nel sovraccaricare i server della vittima con un volume massivo di richieste al punto da non rendere più fruibile il servizio all'utente finale.

Analizzando il grafico 5.2, costruito su un campione di 21 banche rispondenti, si osserva che il 57,1% degli istituti ha dichiarato di aver rilevato tentativi di **attacco DoS e DDoS**, con 99 attacchi registrati andati a buon fine. In tutti i casi registrati le banche hanno attivato soluzioni anti-DDoS sul network aziendale e sono state isolate le fonti di attacco intervenendo con il tuning dei filtri e il blacklisting degli IP.

In particolare, le banche riportano di aver impiegato modalità disparate per la mitigazione del fenomeno, quali attivazioni anti-DDoS (automatiche, semi-automatiche e manuali), utilizzo di Traffic Diversion, Scrubbing Center e servizi di laundering del traffico, con il supporto dei carrier interessati e ISP fornitori.

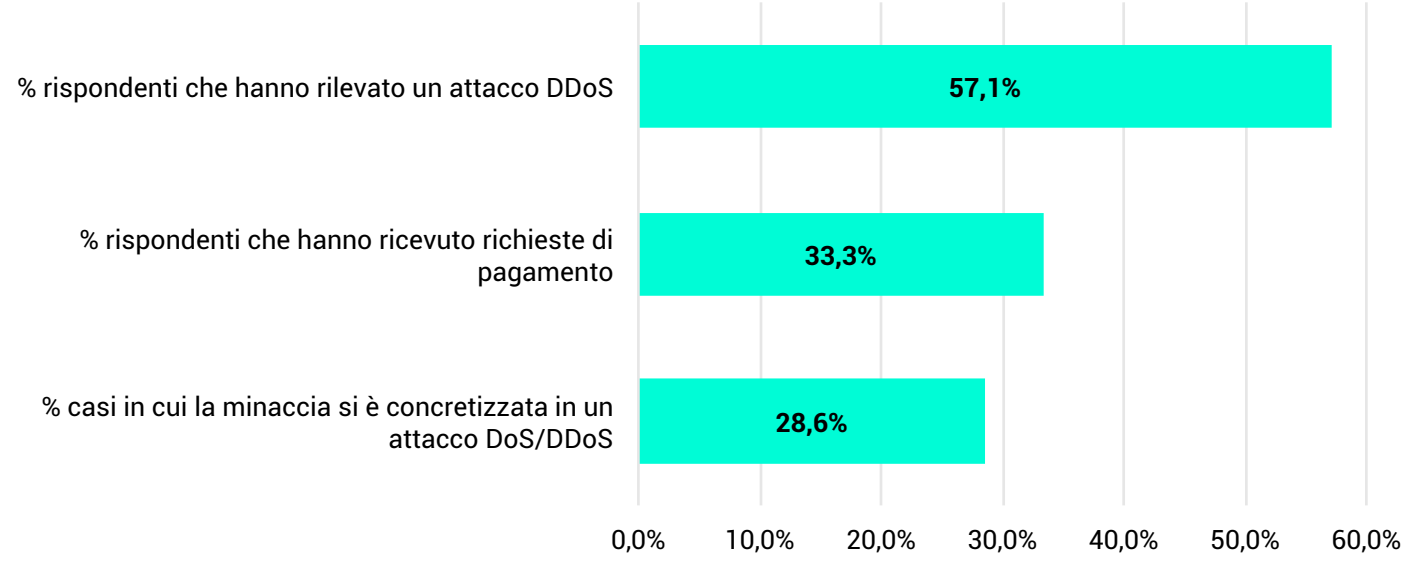
In aggiunta, è stato riproposto lo studio ad hoc del fenomeno **RDDoS** (Ransom DDoS), vista e considerata la recrudescenza del fenomeno, palesatosi principalmente in 3 ondate. Il fenomeno consiste essenzialmente nel minacciare le organizzazioni target rispetto alla possibilità di generare un imminente attacco DDoS, spesso tramite e-mail estorsive firmate da noti gruppi criminali (che tuttavia non ci risultano essere i reali threat actors).

Dalla rilevazione svolta emerge che, nel 2020, 7 banche (33,3% sul totale dei rispondenti) hanno ricevuto note estorsive, a seguito delle quali 6 banche rispondenti (28,6%) hanno assistito alla concretizzazione di un attacco DDoS, per un totale di 9 casi.

Tutti i rispondenti dichiarano di non aver dato seguito alle richieste di pagamento (riportanti la rivendicazione dell'attacco e le indicazioni sulle successive azioni di attacco) e di aver segnalato opportunamente alle autorità competenti, oltre che al CERTFin, gli eventi registrati.

Figura 5.2 **Rilevazione degli attacchi DoS/DDoS e RDDoS**

(21 rispondenti)



Una ulteriore tipologia di fenomeno è la diffusione di **campagne ransomware** (figura 5.3), ovvero una tipologia di malware - veicolata comunemente attraverso il canale e-mail - in grado di bloccare l'accesso ai sistemi o ai file del dispositivo target ricorrendo alla cifratura. Solitamente il criminale, a seguito dell'infezione, chiede alla vittima il pagamento di un riscatto per

ottenere la chiave di decifratura che possa ripristinare nuovamente l'accesso ai documenti e alle cartelle di rete.

In Italia il fenomeno ha avuto un'incidenza del 9,5%, considerato che, su un totale di 21 rispondenti, solamente 2 banche sono state coinvolte, per un totale complessivo di 15 postazioni colpite.

Quanto al fenomeno emergente del double-extortion, anche conosciuto come "doppia estorsione", in questo caso l'attaccante richiede alla vittima un riscatto seguendo il modus operandi tipico di una campagna ransomware, a cui però fa seguito un secondo riscatto a fronte della minaccia di pubblicazione dei dati sottratti. Dalla rilevazione è emerso che solo il 4,8% dei rispondenti risulta essere stato coinvolto dal fenomeno, ma anche in tali casi non sono state sottratte informazioni sensibili.

In relazione ai fenomeni ransomware, i rispondenti riportano di aver impiegato strumenti di protezione host e di rete (e opportune loro configurazioni tecniche) avvalendosi inoltre di campagne di sensibilizzazione e formazione degli utenti rispetto al tema dell'utilizzo consapevole della mail aziendale.

Diversi, invece, sono i dati risultanti degli **attacchi cryptolocker**, ovvero malware molto simili ai ransomware che nascono per cifrare i dati della vittima senza richiedere alcuna richiesta di riscatto, desumendo che l'obiettivo principale sia quello di creare un mero danno reputazionale al soggetto coinvolto. Dalla rilevazione svolta emerge che nel 2020 nessuna banca ha registrato fenomeni di cryptolocker.

A conclusione delle analisi riportiamo che, rispetto al totale degli attacchi registrati nel 2020 (445 eventi) relativi ai fenomeni appena trattati, su un totale di 17 rispondenti 6 istituti (35,3% - figura 5.4) hanno effettuato almeno una segnalazione a Banca d'Italia, secondo quanto previsto dalla normativa vigente.

Figura 5.3 **Rilevazione di attacco ransomware**

(21 rispondenti)

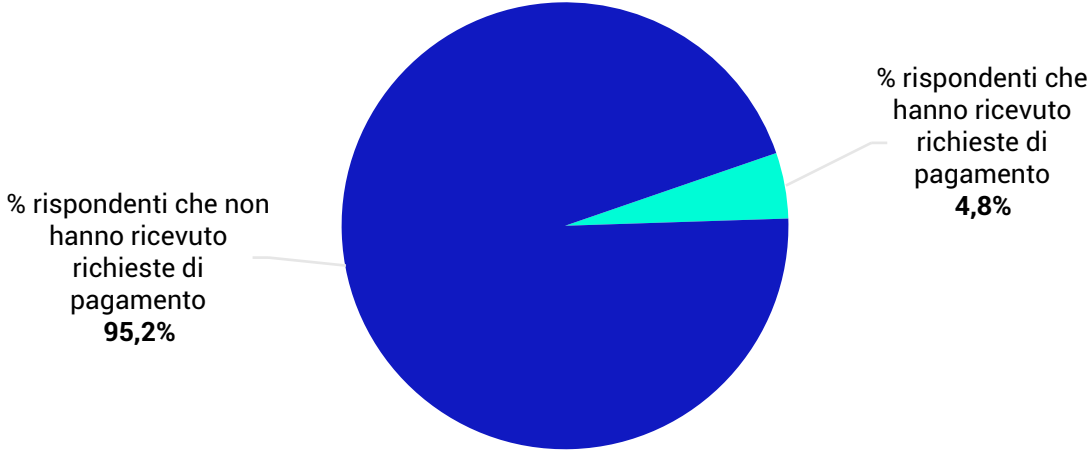
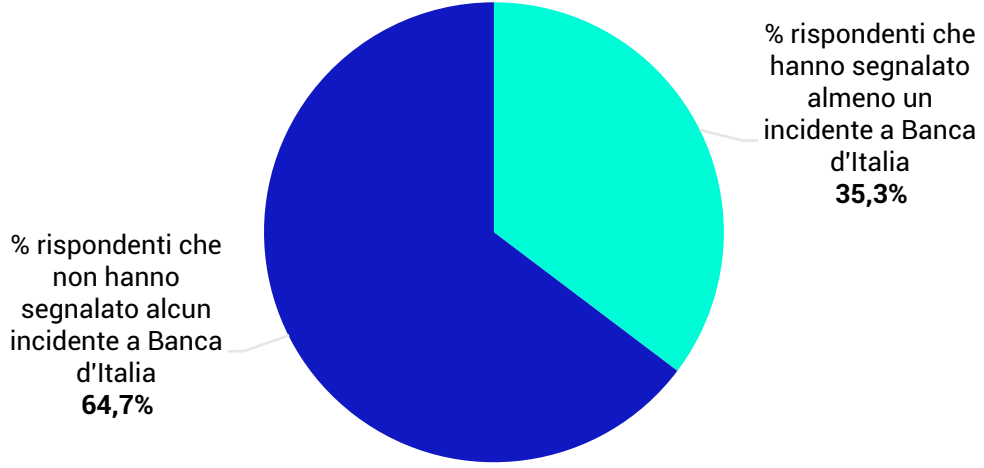


Figura 5.4 **Segnalazione incidenti a Banca d'Italia**

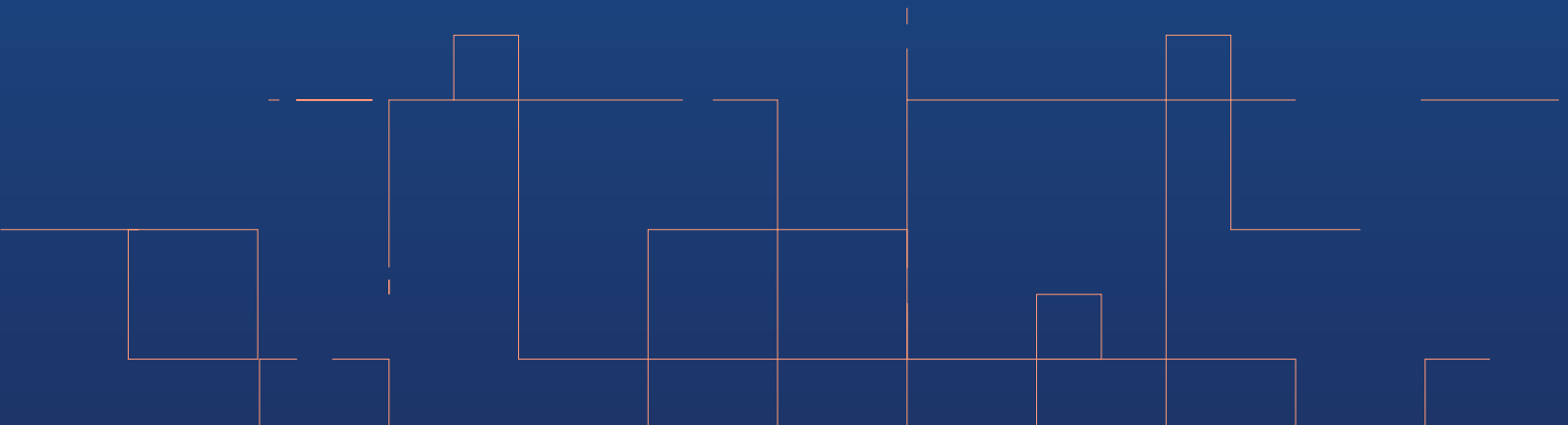
(17 rispondenti)



CERTFin

APPENDICE

Approfondimenti a cura di Exprivia, TIM, Reply, Cleafy, Lutech, Accenture, KPMG, Kaleyra



LA MICRO-SEGMENTAZIONE SOFTWARE GRAZIE ALL'AI PERMETTE DI VISUALIZZARE E CONTROLLARE I FLUSSI DATI INTERNI DI UNA ORGANIZZAZIONE CON ELEVATO LIVELLO DI DETTAGLIO

Da quasi trent'anni la gestione dei flussi di comunicazione all'interno delle infrastrutture IT è stata gestita da apparati fisici che si avvalgono delle possibilità di controllo offerte dall'indirizzamento TCP-IP, applicando regole di filtraggio del traffico in fase trasmissiva, dopo le sorgenti e prima dei riceventi.

Nel frattempo, il panorama tecnologico intorno è profondamente mutato: le nostre infrastrutture non sono più quelle di 30 anni fa, così come le esigenze di comunicazione e di protezione sono cambiate in quantità e qualità.

Per questo motivo, oggi è giunto il momento di valutare nuovi approcci tecnologici, che svincolino il controllo e la gestione della comunicazione dai tecnicismi della rete di comunicazione e che siano basati sul controllo centralizzato, ma prevedano regole distribuite, che siano in grado di integrare nativamente anche i livelli applicativi e le identità coinvolte nella comunicazione. Soluzioni quindi che presentino un livello di astrazione superiore a quello della sola comunicazione di rete, che siano svincolate dal contesto fisico della infrastruttura e siano scalabili per la numerosità di sistemi coinvolti e di tecnologie.

Nel corso degli anni l'evoluzione dei sistemi informativi è stata caratterizzata dalla sempre crescente numerosità dei sistemi. Le soluzioni sono passate da modelli verticali a silo a sistemi integrati ed interagenti fra di loro; tutto ciò ha fatto accrescere in quantità e varietà le comunicazioni all'interno delle farm, che spesso vengono definite come traffico **East-West**. Questo accrescimento in numerosità e varietà causa un'elevata difficoltà a controllare le comunicazioni fra i vari componenti; di conseguenza, identificare eventuali connessioni malevole diventa molto difficile e time-consuming.

Gartner definisce la micro-segmentazione come *"the process of implementing isolation and segmentation for security purposes within the virtual data center."*[1] Inoltre, *"reduces the risk of a lateral spread of advanced attacks in enterprise data cen-*

[1] Fonte: Gartner, "Technology Insight for Microsegmentation," March 2017

ters and enables enterprises to enforce consistent segmentation policies across on-premises and cloud-based workloads."[2]*.* La micro-segmentazione sembra quindi essere un buon modello di segregazione e controllo dei flussi interni ad una infrastruttura, in grado di soddisfare requisiti di complessità e scalabilità incombenti. La micro-segmentazione è inizialmente nata come estensione del concetto di segmentazione delle reti di comunicazione ad opera degli strumenti di network management.

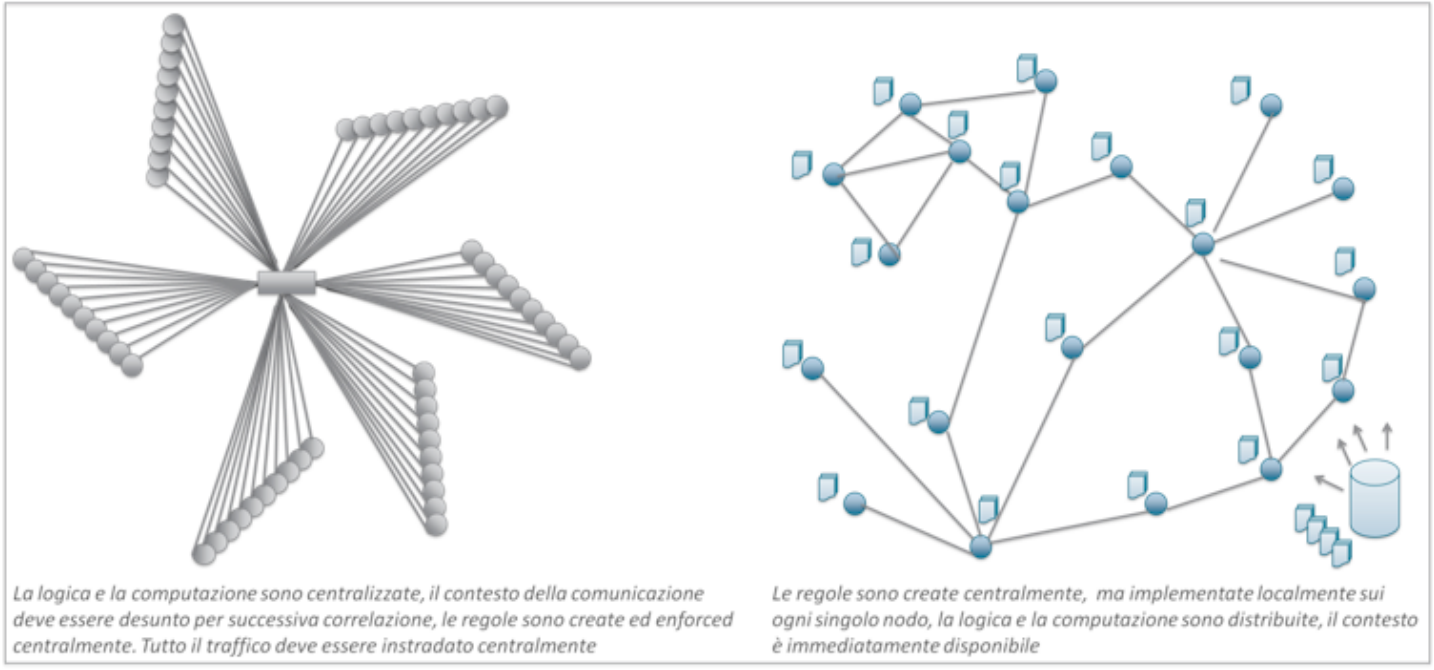
Tuttavia, l'approccio tradizionale "fisico" alla micro-segmentazione è basato sulla segregazione di segmenti di rete e ha posto, nel tempo, sempre maggiori problemi di implementazione, in quanto rende strettamente interdipendenti gli aspetti fisici, legati alle regole di indirizzamento di rete, alla realtà infrastrutturale esistente, sovente in conflitto con le esigenze "logiche" di segregazione e controllo delle applicazioni che travalicano il contesto fisico.

La trasposizione di "regole" logiche in configurazioni fisiche tende quindi a diventare molto complessa ed estremamente fragile rispetto a qualsiasi variazione nel network. Inoltre, inevitabilmente, tali regole sono limitate al mondo della connettività: per esempio, non possono essere espresse nei termini dei processi applicativi che devono interagire fra loro e neppure di utenze (personali o tecniche). I problemi, poi, sono recentemente aumentati nei contesti di infrastrutture ibride, che prevedono sistemi fisici on-prem, virtualizzate e in cloud, in quanto ognuno di questi ambienti deve necessariamente gestire il networking con famiglie di tecnologie specializzate e differenti fra loro. Sono apparse e si sono diffuse sul mercato intere categorie di prodotti di "armonizzazione" delle configurazioni network che, pur essendo di aiuto nella gestione della complessità, accrescono costi e richieste di competenze per i team.

L'approccio software alla micro-segmentazione prevede una gestione centralizzata delle regole, ma l'enforcement è localizzato sui singoli nodi/workload che vengono dotati di agenti che controllano tutte le connessioni di rete, avendo la possibilità di ottenere e gestire rilevanti informazioni relative ai contesti locali (applicazioni, utenze, o.s.). Ogni nodo/workload riceve dal controllore centrale l'attribuzione di specifiche tag che li caratterizzano ulteriormente. Le tag possono essere desunte automaticamente o attribuite direttamente. Questo approccio permette **una completa astrazione** dal contesto fisico di una infrastruttura enterprise di qualsivoglia complessità.

[2] Fonte: Gartner, "Hype Cycle for Cloud Security 2017," July 2017

Figura 1 **La micro-segmentazione fisica vs. software**



La logica e la computazione sono centralizzate, il contesto della comunicazione deve essere desunto per successiva correlazione, le regole sono create ed enforced centralmente. Tutto il traffico deve essere instradato centralmente

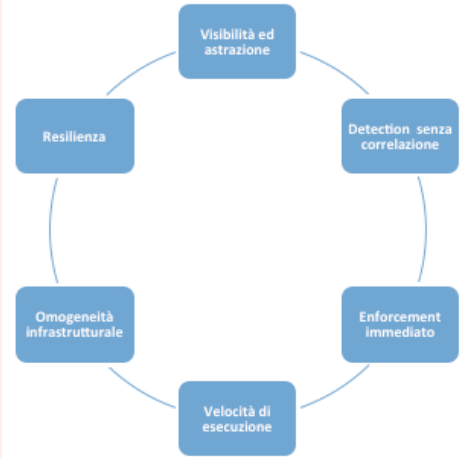
Le regole sono create centralmente, ma implementate localmente sui ogni singolo nodo, la logica e la computazione sono distribuite, il contesto è immediatamente disponibile

Le **regole** possono essere definite a **livello logico** ed essere espresse anche in funzione dei livelli più alti (6, 7) della pila OSI, risultando indipendenti dalle infrastrutture fisiche e dalle corrispondenti esigenze di gestione. La semplicità e l'espressivi-

tà delle regole fa sì che possano essere definite in modo logico, veloce ed efficace. Le regole non dipendono più dalla tecnologia della infrastruttura, né dalla locazione del workload, e sono stabili nel tempo e nello spazio. Ogni sistema può essere associato a quante tag identificative si desidera, associabili manualmente o automaticamente da sorgenti quali naming convention, asset management, CMDB, etc.

La visione centralizzata offerta da questa tecnologia permette di utilizzare strumenti di Artificial Intelligence e Machine Learning per ulteriori ottimizzazioni: la discovery dei flussi è automatica e crea una visualizzazione di tutte le comunicazioni e le dipendenze delle applicazioni. La mappa visualizzata mostra come i carichi di lavoro comunicano fra loro. Gli algoritmi utilizzano questi dati, modellano la rete come un grafico annotato e utilizzano le tecniche di apprendimento automatico senza supervisione per raggruppare workload simili in gruppi, in base a modelli di comunicazione. Le seguenti attività possono essere automatizzate:

Figura 2 **Micro-segmentazionesoftware: i vantaggi**



- Classificazione dei workload
- Creazione di tag per applicazioni e relativi livelli
- Suggerimento di regole per la segmentazione a livello di flusso e micro-segmentazione a livello di processo

La micro-segmentazione software permette di ottenere immediatamente una completa visibilità dei propri flussi dati interni, non più mediata dalla continua necessità di complesse correlazioni e interpretazioni dei dati. Di conseguenza, l'identificazione dei flussi è istantanea, certa e mai ambigua. Tutto ciò permette la facile definizione di regole di allerta e di blocco, semplici e assolutamente generali e resilienti.

Gli aspetti di sicurezza impattati dalla micro-segmentazione software sono molto significativi e impattano tutte le 5 aree identificate dal Cybersecurity Framework del NIST:

Identify: attraverso la console centrale si ottiene una visibilità completa e immediata delle comunicazioni che avvengono fra i workload, senza il rischio di perdere interazioni "offuscate" da flussi analoghi sulle medesime connessioni.

Protect: le regole di protezione sono immediatamente attive non appena i workload sono creati e associati alle loro tag: l'approccio logico permette di proteggere ambiti operativi e applicativi ben distinti con poche ed efficaci regole.

Detect: la tecnologia permette di identificare immediatamente flussi di comunicazione inattesi e potenzialmente anomali, senza la necessità di applicare complesse correlazioni fra differenti sorgenti e avendo contestualmente tutte le informazioni necessarie a contestualizzare quanto osservato (utenze, processi coinvolti, etc.).

Respond: vettori di attacco identificati o sospetti (flussi, utenze, processi) possono essere istantaneamente isolati da tutti i sistemi con semplici regole che possono essere distribuite ed attivate in pochi minuti.

Recover: Una volta bloccati i potenziali vettori di attacco, le regole di blocco permetteranno una progressiva e automatica ripresa dei servizi non appena le condizioni malevole saranno eliminate dai sistemi infettati.

IL SUPPORTO DELLE TELCO PER FAVORIRE I PROCESSI DI SICUREZZA NEL MONDO BANCARIO

Lo scenario di riferimento

Negli ultimi 25-30 anni, il "modo di fare Banca" si è enormemente evoluto ed una delle direttrici di questa evoluzione si è basata sui servizi che le piattaforme Telco hanno messo a disposizione nel corso del tempo.

Negli **anni '80 e '90** le Telco hanno contribuito all'evoluzione delle reti interbancarie e di filiali, oltre che all'evoluzione dei servizi di Call Center e Contact Center.

Nel **primo decennio del 2000** sono state abilitatrici dell'online banking, dell'aumento di prestazioni ed affidabilità delle Reti interbancarie e di filiali e di progetti di continuità operativa (collegamenti CED to CED).

Inoltre, le Telco sono state protagoniste dell'evoluzione dell'approccio da Multicanalità ad Omnicanalità nella relazione con la clientela, nonché dello sviluppo dei primi strumenti anti-frode (SMS Banking e servizi OTP basati sulla ricezione dell'SMS o di chiamate telefoniche).

Nell'ultimo decennio le piattaforme Telco e gli strumenti ad esse collegati (es. smartphone) sono stati fondamentali per la nascita ed evoluzione dell'APP Banking, diventando abilitatori di processi di sottoscrizione contrattuale a distanza. Questo è avvenuto grazie anche all'introduzione di soluzioni di firma elettronica avanzata e qualificata e ad un utilizzo di massa dello smartphone e delle APP come principale strumento anti-frode abilitante i processi di pagamento, anche per vincoli normativi PSD2.

Gli **ultimi 5 anni** hanno visto la crescita esponenziale dei rischi che corrono sulla rete e **l'ultimo anno,** in particolare, ha visto una forte accelerazione verso ciò che viene ormai considerato il "new normal".

In questo scenario di cambiamento del "modo di fare Banca", le piattaforme Telco si pongono come strumento abilitatore per consentire alle Banche di mantenere un ruolo centrale nell'ambito dei processi di pagamento, sia nel rapporto con i Clienti che nell'efficientamento dei propri processi.

Fondamentale in questo senso il supporto che le Telco sono in grado di offrire per l'identificazione certa di un titolare di conto corrente collegato da remoto.

Le nuove sfide

Una delle più importanti sfide che il mondo delle Banche oggi si trova ad affrontare è il contrasto al fenomeno delle frodi che corrono sulla rete. La partita si gioca insieme e, per vincerla, è necessaria una "alleanza": le Banche devono far evolvere i loro processi e le loro piattaforme tecnologiche di analisi comportamentale dell'utente, le Telco devono fornire alle Banche le informazioni sui "comportamenti rilevanti di rete", nel rispetto del quadro normativo di riferimento, anche e soprattutto in ambito Privacy.

In questo scenario le piattaforme delle Telco stanno progressivamente aprendo lo "scrigno" delle informazioni sui comportamenti in rete a favore delle Banche, per consentire al mondo bancario di arricchire di informazioni utili i propri strumenti di analisi comportamentale e per costruire gli "score di rischio" sulla base di informazioni quali:

- "c'è stato un cambio di SIM o di Cellulare?"
- "il titolare di una carta di debito quanto è vicino geograficamente all'ATM durante un prelievo?"
- "il numero telefonico chiamante è effettivamente quello che dice di essere?"
- "da quanto tempo è stata sostituita la SIM?"

L'approccio di TIM intende supportare i processi di antifrode, semplificando le attività delle banche, in un ecosistema nel quale Telco diverse possono mettere a disposizione delle banche informazioni di rete diverse, nel contenuto e nella forma.

Gli strumenti a disposizione per contrastare il fenomeno SIM SWAP

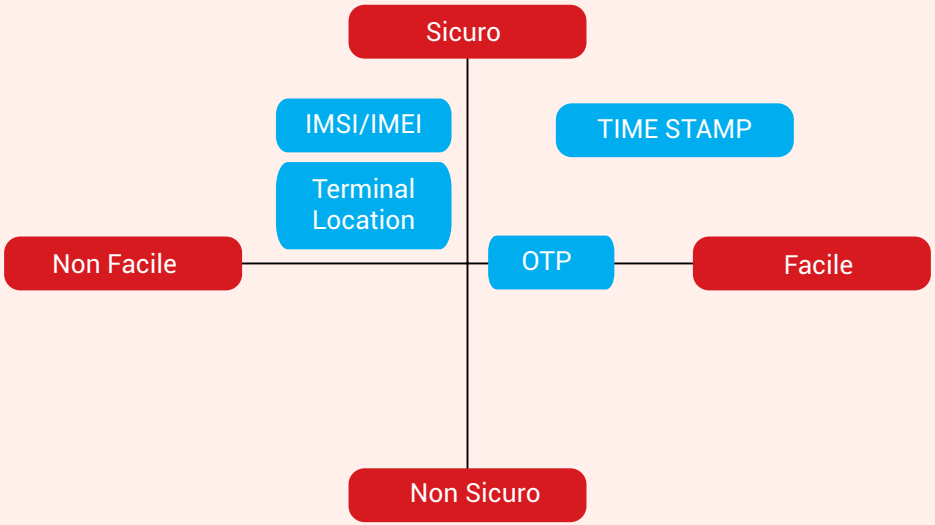
Negli ultimi anni le Banche, in collaborazione con il mondo delle Telco, stanno mettendo in atto una serie di contromisure per combattere il fenomeno SIM SWAP.

Come noto, l'attacco SIM swap parte da una nuova SIM con lo stesso numero telefonico della vittima, ma emessa a sua insaputa grazie all'intervento del frodatore. In questo modo il frodatore ha il pieno possesso del numero della vittima su cui arrivano i codici OTP via SMS e, avendo generalmente già raccolto i codici di accesso statici con altre modalità (phishing tradizionale), riesce a disporre transazioni fraudolente a suo favore.

Il percorso per una soluzione in grado di arginare questi fenomeni non è così scontato e varia a seconda degli strumenti utilizzati, che possono assicurare diversi gradi di sicurezza, affidabilità e facilità/difficoltà di implementazione.

Analizziamo nel dettaglio gli strumenti a disposizione (figura 1):

Figura 1 **Mappatura delle soluzioni a disposizione**



One Time Password (OTP): nell'ambito della crittografia e della sicurezza informatica è una password che è valida solo per una singola sessione di accesso o una transazione. L'OTP essendo "usa e getta" non è vulnerabile agli attacchi con replica: se un intruso riesce a intercettare una OTP che è stata già utilizzata per accedere a un servizio o eseguire una transazione, non sarà in grado di riutilizzarla, in quanto non sarà più valida. D'altra parte, in un attacco SIM SWAP la vulnerabilità dell'OTP è data dalla clonazione della SIM e non dell'OTP stessa, di conseguenza questo strumento non è sufficiente a garantire la sicurezza delle operazioni effettuate.

Terminal Location: è uno strumento per geolocalizzare la cella del terminale che si sta utilizzando. È utile per tutti quei casi in cui la posizione del cliente può avere significatività per gli aspetti di sicurezza ma la sua affidabilità si basa sulla triangolazione dei tempi di risposta tra dispositivo e antenna e non è estremamente precisa. Inoltre, utilizzare i dati geolocalizzati degli utenti richiede a monte la gestione della privacy secondo GDPR, del relativo consenso utente e una gestione ad hoc per la storicizzazione dei dati.

Verifica IMSI/IMEI: è uno strumento per verificare l'IMSI e l'IMEI. L'IMSI (International Mobile Subscriber Identity) è il numero che identifica univocamente ogni utenza di telefonia mobile di reti GSM o UMTS mentre l'IMEI (International Mobile Equipment Identity) è un codice numerico che identifica univocamente un terminale mobile. Tramite questa soluzione è possibile verificare nel tempo se una SIM o un telefono appartenenti ad una stessa utenza sono stati cambiati ottenendo un'altissima affidabilità nel tentativo di difendersi dal SIM SWAP. Per contro questa soluzione richiede una gestione onerosa in termini di conservazione dei dati e verifica degli stessi nel tempo poiché IMSI e IMEI sono dati estremamente sensibili in termini di sicurezza e privacy.

TIME STAMP: è uno strumento per verificare l'ultimo cambio SIM di un utente evitando la storicizzazione del dato. Al momento è **l'unico strumento per garantire la sicurezza delle operazioni che non necessita di nessun tipo di gestione dati e che permette una verifica in tempo reale**, lasciando la possibilità alla Banca di applicare policy personalizzate a seconda del timing riscontrato.

Analizzando il grafico di mappatura delle soluzioni attualmente a disposizione (vedi figura 1), **lo strumento di verifica del TIME STAMP risulta essere ad oggi la soluzione più sicura e più facile da implementare** poiché non richiede investimenti per la gestione e l'analisi costante dei dati rispetto alle altre soluzioni esistenti.

L'approccio proposto da TIM per fronteggiare il fenomeno del SIM Swap prevede una suite di soluzioni; in particolare per la gestione del TIME STAMP è stata sviluppata un'API (Mobile To Network) in grado di fornire alle Banche la possibilità di avere in tempo reale data e ora dell'ultimo cambio SIM effettuato da un cliente TIM.

Tale dato permette alla Banca, in tempo reale, di adottare le proprie strategie/ policy di sicurezza più opportune, senza dover storicizzare nessun dato e senza utilizzare informazioni sensibili (come IMSI e IMEI) del cliente.

L'EVOLUZIONE DI URSNIF: DA INFOSTEALER A VETTORE DEL MOBILE MALWARE CERBERUS

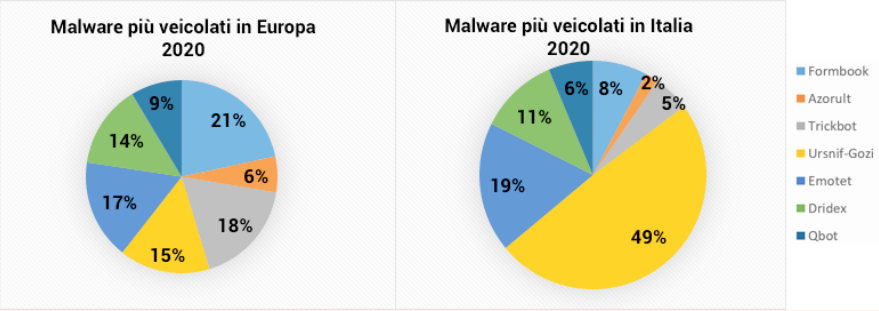
A seguito della pandemia si è riscontrato un notevole aumento del fenomeno di phishing e malspam che ha contribuito alla diffusione massiccia di malware bancari in Europa, con l'Italia tra i principali target.

Come mostrato in Figura 1, i malware bancari più diffusi in Europa durante tutto il 2020 sono stati Formbook, Trickbot, Emotet e Ursnif. Il trend è stato mantenuto anche durante il Q1 del 2021, ad eccezione di Emotet che ha avuto un netto calo della sua attività a causa dello smantellamento della botnet principale da parte dell'Europol.

Per quanto riguarda l'Italia, il 2020 ha avuto come protagonista lo storico malware bancario **Ursnif**, con un picco di attività rilevato a partire da inizio Q3. In particolare, si è notato un aumento nel numero di sample malevoli e di varianti diffuse, grazie anche alla formula sempre più di tendenza di **Malware as a Service** (MaaS).

Figura 1 **Trend rilevati dei malware più veicolati in Europa e in Italia nel 2020**

Fonte: Communication Valley Reply



Da quando Ursnif ha cominciato ad intensificare la sua attività è diventato di fatto uno dei malware più diffusi in Europa e, grazie alle oltre 40 campagne individuate, il più veicolato nel nostro Paese. Le varianti di malware appartenenti alla famiglia di Ursnif sono state l'elemento chiave delle nostre analisi e attività di intelligence.

La modalità di attacco principale utilizzata da Ursnif è l'**attacco MITB** (malware-in-the-browser), minaccia conosciuta e consolidata nel tempo. È una variante dell'attacco MITM (man-in-the-middle) sfruttata principalmente dai malware bancari, in cui un attaccante, infettando il browser, riesce a frapporsi all'interno di un canale di comunicazione tra due entità allo scopo di intercettare informazioni sensibili delle vittime.

Il metodo utilizzato dai threat actors per veicolare il malware consiste nello sfruttare tecniche di ingegneria sociale e massicce campagne di malspam. Tra i temi più sfruttati troviamo la pubblica amministrazione e i settori di logistica ed energetico, usati come oggetto per veicolare un documento Office infetto.

Una volta che l'utente apre il documento e clicca su "Abilita Contenuto", una funzione "macro" avvia uno snippet di codice PowerShell offuscato che costituisce il dropper del malware. La funzione del codice nella macro è quella di avviare l'infezione, contattando l'endpoint remoto dal quale viene scaricato ed eseguito il loader finale di Ursnif.

Al fine di evadere la detection e complicare le attività di reverse engineering il payload non viene scaricato in chiaro, ma vengono avviati dal malware una serie di processi di ricostruzione del codice.

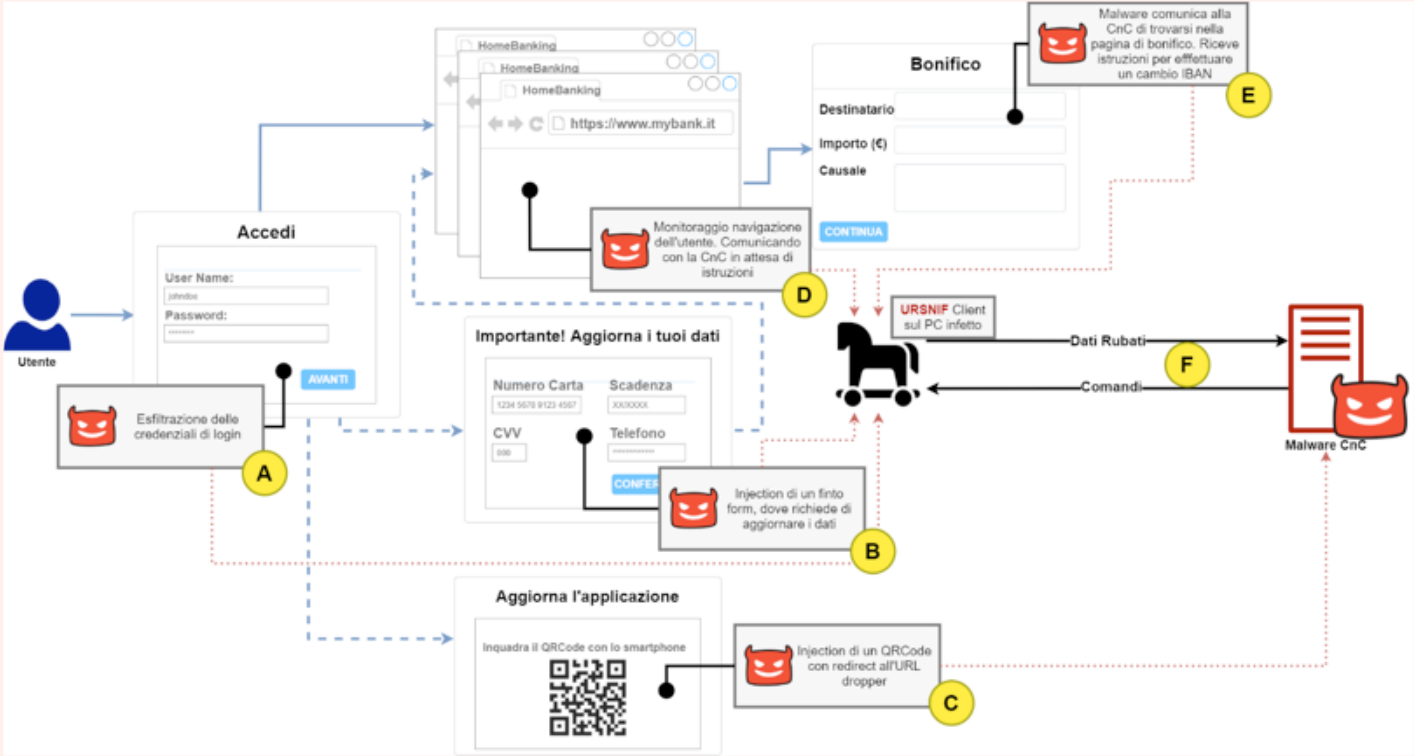
In base alle varianti, infatti, il loader viene suddiviso in più file scaricati in sequenza (dropper a catena) o, in alternativa, racchiuso all'interno di un unico file al cui interno sono presenti diverse funzioni che causano rumore. L'installazione continua con una serie di decodifiche del codice scaricato, ottenendo man mano le varie componenti del malware.

Una volta "deoffuscato" il codice, si passa alla parte finale di persistence. Questa fase va a creare una *dll* malevola contenente la configurazione principale all'interno del file system dell'utente. In seguito, viene eseguita l'infezione delle *dll* configurate per i browser target.

L'infezione aggiunge al browser la funzione di un proxy in ascolto per particolari richieste HTTP. Tali richieste vengono effettuate dal browser verso un endpoint in locale attraverso le quali il malware inietta in pagina il codice malevolo, esfiltrando in seguito le informazioni. In questo modo il malware riesce a comunicare con il suo server CnC passando tramite il dispositivo dell'utente, rendendo invisibile agli occhi del browser stesso l'indirizzo finale del server dell'attaccante (figura 2 – F).

All'avvio del browser infetto il malware si attiva ed ha così inizio la comunicazione con il *server CnC* remoto. Questo resta in ascolto finché non rileva l'accesso ad una delle pagine target per le quali è stato configurato e si attiva andando ad interagire con l'utente/browser, come raffigurato in figura 2.

Figura 2 **Flowchart delle attività malevole sulle pagine target**



L'analisi di queste ultime campagne ha permesso non solo di confermare pattern e tecniche di attacco noti, ma ha consentito anche di identificare e studiare alcune nuove varianti del malware che hanno introdotto interessanti variazioni alla formula. Tali variazioni sono state raggruppate in **due varianti**: la classica *money stealer* e la nuova *phisher*.

L'elemento che accomuna le varie tecniche è la funzionalità di *credential stealing* (figura 2 – A), che viene attivata nel momento in cui l'utente inserisce i dati di accesso sul portale di homebanking. Da questo momento in avanti si notano le vere differenze nei comportamenti delle due tecniche.

Partendo dalla **variante classica**, il cui scopo consiste *nel furto di denaro*, viene utilizzato un framework JavaScript dedicato per svolgere le attività all'interno del browser, adattato ad hoc per ogni banca bersagliata. Tramite tale framework, il malware monitora la navigazione (figura 2 – D) dell'utente all'interno del portale di homebanking ed esfiltra una serie di informazioni contestuali che condivide con la CnC fino a che non raggiunge una pagina target nella quale deve passare alla modalità attiva.

Solitamente le pagine target sono quelle in cui è possibile effettuare un pagamento, per effettuare quello che viene definito *hook payment* (figura 2 – E). Quello che avviene è l'esecuzione di una serie di istruzioni che vanno a *modificare i dettagli del bonifico*, in maniera completamente trasparente per l'utente, facendo in modo che la banca riceva estremi di pagamento differenti da quelli che l'utente ha inserito.

La **nuova variante utilizza** invece un approccio basato sul *phishing*, della quale sono state individuate due versioni differenti che utilizzano tecniche distinte.

La **prima tecnica** si basa unicamente sull'esfiltrazione del maggior numero possibile di informazioni, che vengono poi utilizzate per attacchi di spearphishing mirati. Anche in questo caso si può notare il supporto del framework JavaScript iniettato nel browser dal malware, che abilita l'intercettazione degli eventi in pagina e la comunicazione con la CnC.

La particolarità, in questo caso, consiste nella *modifica del contenuto della pagina* visibile all'utente (figura 2 – B), che va a creare una maschera di input dove vengono richieste informazioni sensibili (tra le più comuni troviamo la carta di credito e il numero di telefono).

La **seconda tecnica**, invece, utilizza un approccio completamente differente, riscontrato solo in alcuni dei target del malware. Al posto di iniettare nuovi campi di input, il malware inietta una vera e propria pagina aggiuntiva in cui viene richiesto non solo di inserire il numero di telefono ma anche di scaricare e installare, attraverso un *QRCode* (figura 2 – C), una presunta nuova versione dell'applicazione di mobile banking.

Il link associato al QRCode reindirizza la vittima alla pagina di phishing di un falso store, all'interno della quale è possibile effettuare il download di una applicazione malevola.

Su questi fake store sono pubblicate app con riferimenti a diversi brand del settore finance ed e-commerce, tutte veicolanti il noto mobile banking malware **Cerberus**.

Cerberus abusa di un permesso speciale relativo al servizio di accessibilità che gli permette di effettuare una privilege escalation. Questa gli consente quindi di abilitare i moduli per il furto di dati, keylogging, SMS e registrazione di chiamate. La particolarità della versione del malware analizzata è la presenza di una tecnica di *anti sandbox* per effettuare l'arresto dell'esecuzione, che sfrutta i dati dei sensori del dispositivo per verificare la presenza di un ambiente emulato. Il malware effettua inoltre *attacchi di tipo overlay* che permettono di esfiltrare le credenziali bancarie sovrapponendo una pagina di phishing (*fake webview*) all'applicazione target.

Sulla base degli IoC raccolti, si è notato una differenziazione dei comportamenti della suddetta variante in relazione ai target colpiti. Ciò porta a concludere che, in un contesto nel quale malware differenti condividono caratteristiche simili, nell'immediato futuro anche altre famiglie di malware potranno adottare le tecniche descritte precedentemente ovvero incrementare il ventaglio di funzionalità malevole implementate.

NUOVI MALWARE E PATTERN DI ATTACCO DI RECENTE RILEVAZIONE E DI INTERESSE PER IL CONTESTO FINANZIARIO

Il contesto finanziario già da diversi anni risulta essere uno dei settori maggiormente colpiti da minacce cyber nelle quali il cliente finale e l'applicazione utilizzata per accedere al proprio servizio bancario risultano essere i veri target dell'attacco.

Nel corso del 2020 e 2021 è stato osservato un notevole incremento della distribuzione e dell'utilizzo di Banking Trojan, che colpiscono dispositivi Android al fine di effettuare attacchi di Account Takeover (ATO) verso la clientela finale. Quello che si nota infatti è una **vera e propria evoluzione delle minacce Android** che possiamo racchiudere nei seguenti punti:

- **SMS sniffer + Overlay Attacks**: questi Banking Trojan vengono distribuiti principalmente all'interno di campagne Social Engineering al fine di intercettare credenziali di autenticazione e codici di autorizzazione (2FA)
- **RAT**: sono dei Banking Trojan con funzionalità molto avanzate che abilitano il controllo remoto del device infetto (Remote Access Tool). Questo paradigma consente principalmente agli attaccanti di non dover effettuare un nuovo enrollment per effettuare attacchi di tipologia Account Takeover (ATO)
- **RAT + modulo ATS**: queste modalità di attacco non sono state ancora rilevate su larga scala ma rappresentano la possibilità di effettuare anche attacchi ATS (Automatic Transfer System) o Swap IBAN su dispositivi mobile Android

I più classici Banking Trojan Android vengono distribuiti all'interno di campagne Social Engineering per intercettare credenziali di autenticazione e messaggi SMS dal device mobile compromesso al fine di ottenere credenziali, codici di autenticazione/autorizzazione e informazioni relative alle carte di credito. Questa tipologia di minaccia risulta essere un'alternativa molto efficace rispetto ad attacchi più costosi e meno scalabili come i "SIM Swap".

Invece, i più recenti Banking trojan (es. Alien, Oscorp, TeaBot, etc.) possono essere considerati dei veri e propri **RAT** (Remote Access Tool) in quanto hanno come obiettivo il completo controllo del device infetto per effettuare attacchi di Account Takeover (ATO).

Queste famiglie di RAT tipicamente abusano di una funzionalità messa a disposizione da Android, gli **Accessibility Services**, per abilitare diverse tecniche di attacco ed ottenere credenziali di autenticazione, informazioni relative alle carte di credito, codici OTP/2FA ed SMS. Attualmente, le tecniche più utilizzate sono gli **Overlay attack** (un paradigma di Social Engineering dove all'apertura dell'applicazione bancaria viene sovrapposta una pagina identica utilizzata per esfiltrare dati sensibili), funzionalità di keylogging e diverse soluzioni di "**live screen recording**", implementando anche sofisticate tecniche di **evasion** come la disabilitazione automatica di antivirus, offuscamento del codice, cifratura delle comunicazioni con il server C2, etc.

Queste tipologie di minacce solitamente hanno una durata piuttosto lunga nel tempo (mesi o addirittura anni), in cui vengono rilasciate nuove funzionalità e nuovi target.

Nella maggior parte dei casi vengono distribuite tramite campagne di Social Engineering (phishing/smishing/vishing), tuttavia sono stati intercettati alcuni casi sporadici in cui Banking Trojan sono stati distribuiti tramite lo store ufficiale di Google.

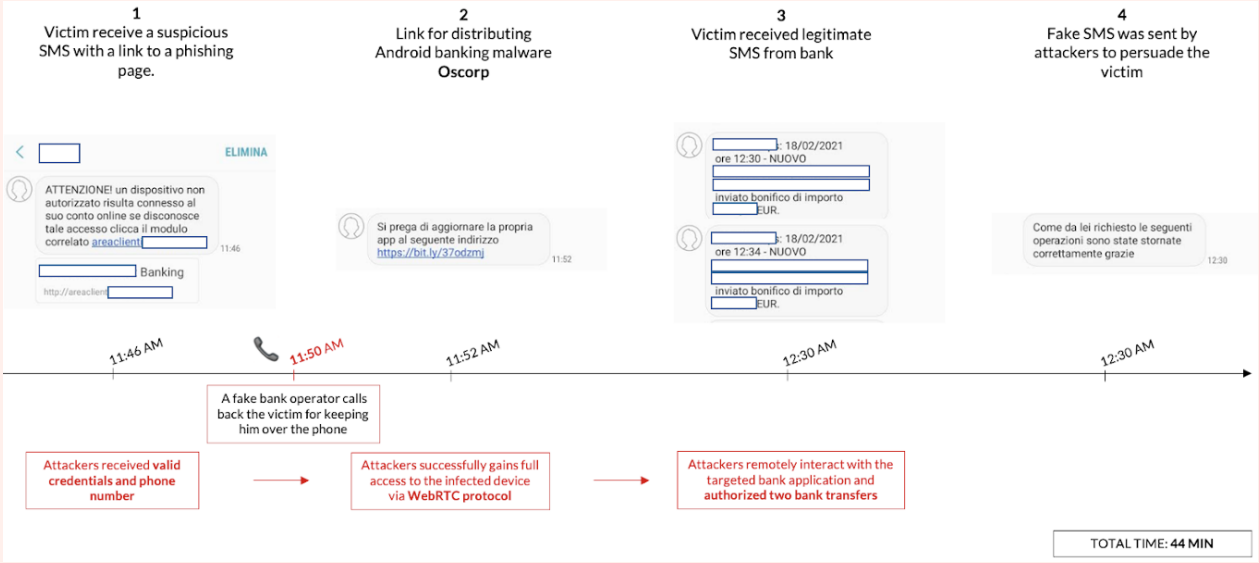
Tipicamente, le tecniche più consolidate ed utilizzate dai vari gruppi che operano dietro queste minacce consistevano nell'effettuare un Overlay attack e nell'intercettazione dei messaggi SMS. Tuttavia si sta riscontrando anche un maggiore utilizzo delle funzionalità di interazione remota real-time con il device Android compromesso. Un esempio emerso recentemente (Febbraio 2021) è stato **Oscorp**, un Banking Trojan che, per ottenere questa interazione remota, ha introdotto l'utilizzo del protocollo **WebRTC**.

"**WebRTC** *(Web Real-Time Communication) è un framework opensource per ambienti web in grado di abilitare una Real Time Communication (RTC) all'interno del browser di navigazione tramite un insieme di APIs ben definite. [...]" (Fonte: webrtc.github.io)*

Più nello specifico, durante il 2021 alcuni casi di frode sono stati ricondotti all'utilizzo di Oscorp, il quale veniva distribuito all'interno di campagne di Social Engineering dove operatori telefonici persuadevano le vittime per installare l'applicazione malevola nel proprio device mobile.

Con la seguente immagine viene descritta una timeline di eventi raccolti durante l'analisi di una di queste specifiche campagne:

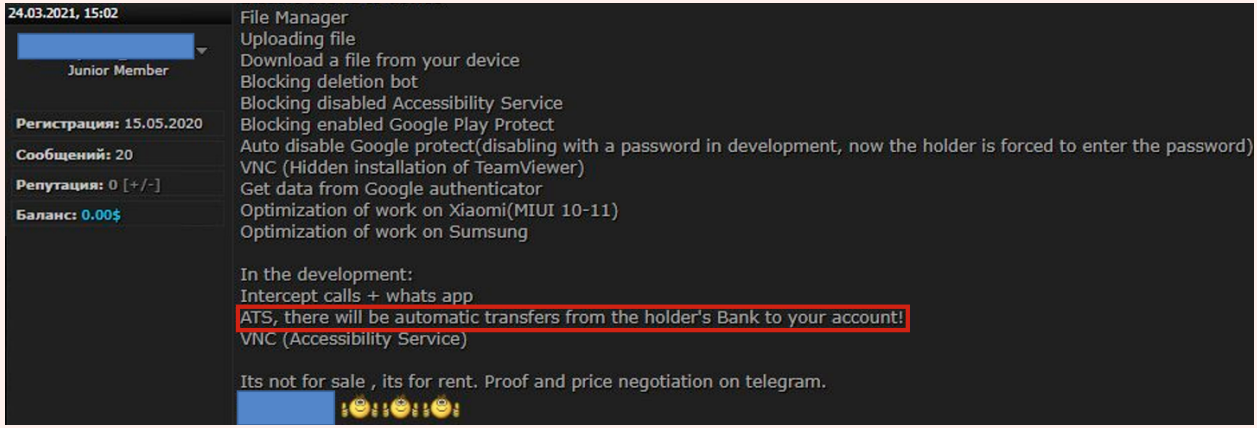
Figura 1 **Timeline degli eventi raccolti durante un attacco tramite il Banking Trojan Oscorp (Febbraio 2021)**



Infatti, combinare l'utilizzo di protocolli come WebRTC con l'abuso degli Accessibility Services abilita gli attaccanti ad ottenere il pieno controllo di un device Android e la possibilità di avere un'interazione remota real-time. Questo paradigma consente principalmente agli attaccanti di non dover effettuare un nuovo enrollment per eseguire attacchi di tipologia Account Takeover (ATO) bypassando di conseguenza le comuni contromisure antifrode che si basano unicamente su indicatori di device fingerprinting (es. modello device utilizzato, indirizzo IP, etc.).

Osservando quindi la velocità di evoluzione delle minacce sul mondo mobile Android e monitorando alcune fonti di discussione legate al mondo del Cybercrime è possibile aspettarsi che il punto di arrivo di questi Banking Trojan sia quello di riuscire ad effettuare attacchi di tipo ATS (Automatic Transfer System) oltre al completo controllo del device compromesso.

Figura 2 **Annuncio di un nuovo malware Android con modulo ATS in fase di sviluppo (Marzo 2021)**



MODELLI DI CYBER SECURITY AWARENESS INTERNA ALLE ORGANIZZAZIONI

di Vito Villa e Marco Ceccon

Nel corso dell'ultimo decennio il panorama dei cyber attacchi è radicalmente cambiato, adattandosi all'evoluzione delle nuove tecnologie informatiche adottate dalle Organizzazioni, ai nuovi paradigmi di elaborazione dei dati (Multicloud) e ai sistemi di protezione e sicurezza degli stessi. Dunque, potremmo facilmente asserire che lo scenario in cui viviamo e lavoriamo consiste in un complesso ecosistema costantemente in fase evolutiva e messo a rischio da una serie di minacce che sono in grado di adattarsi ai cambiamenti.

Le maggiori minacce che incombono tradizionalmente sulla sicurezza delle informazioni sono sicuramente quelle relative alle infezioni da malware, con la loro capacità di infiltrarsi nelle reti e nei sistemi, oltre a quelle riferite al phishing e al social engineering che, sebbene più recenti, possono avere impatti negativi molto rilevanti sul business delle aziende.

Prendendo spunto dai rapporti del Clusit che ogni anno analizzano gli attacchi più significativi, possiamo osservare che nel corso dell'ultimo decennio le minacce di cui sopra si sono rivelate in costante crescita.

Figura 1 **Estratto dai Rapporti Clusit sulla sicurezza ICT in Italia (2017 e 2021)**

Rapporto 2017 sulla Sicurezza ICT in Italia

Distribuzione generale delle tecniche di attacco

TECNICHE DI ATTACCO PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	Variazioni 2016 su 2015	Trend 2017
SQL Injection	197	435	217	110	184	35	-80,98%	↓
Unknown	73	294	239	199	232	338	45,69%	↑
DDoS	27	165	191	81	101	115	13,86%	→
Known Vulnerabilities / Misconfigurations	107	142	256	195	184	136	-26,09%	↓
Malware	34	61	57	127	106	229	116,04%	↑
Account Cracking	10	41	115	86	91	46	-49,45%	↓
Phishing / Social Engineering	10	21	3	4	6	76	1.166,67%	↑
Multiple Techniques / APT	6	13	71	60	104	59	-43,27%	↓
0-day	5	8	3	8	3	13	333,33%	↑
Phone Hacking	0	3	0	3	1	3	200,00%	↑

Rapporto 2021 sulla Sicurezza ICT in Italia

Distribuzione delle tecniche di attacco

TECNICHE DI ATTACCO PER TIPOLOGIA	2017	2018	2019	2020	2020 su 2019	Trend 2020
Malware	446	585	729	783	7.4%	↑
Unknown	277	408	317	372	17.4%	↑
Known Vulnerabilities / Misconfigurations	127	177	127	184	44.9%	↑
Phishing / Social Engineering	102	160	291	289	-0.7%	→
Multiple Techniques / APT	63	98	65	95	46.2%	↑
Account Cracking	52	56	86	85	-1.2%	→
DDoS	38	38	23	34	47.8%	↑
0-day	12	20	30	23	-23.3%	↓
Phone Hacking	3	9	1	3	200.0%	↑
SQL Injection	7	1	1	3	200.0%	↑
TOTALE	1127	1552	1670	1871	+12%	

Dunque, la domanda che verrebbe più spontanea porsi è se le attuali tecnologie antivirus, antimalware e antispam siano adeguate a contrastare questa evoluzione costante del problema. La nostra opinione, come specialisti di sicurezza informatica che lavorano da diversi decenni nel settore, è che le tecnologie di protezione si sono certamente evolute per contrastare le continue tecniche utilizzate dagli attaccanti, ma che le stesse risultano meno efficaci se non opportunamente affiancate da comportamenti umani consapevoli.

In questo ambito di riferimento bisogna considerare come l'anno pandemico appena trascorso abbia comportato un ulteriore aumento degli attacchi cyber, che hanno sfruttato proprio le debolezze delle persone e la mancanza di una loro adeguata formazione in materia di cyber sicurezza di base.

Oltre a quanto esposto, si aggiungano una serie di regolamenti, direttive e leggi (come, ad esempio, il Regolamento GDPR, la direttiva NIS e il Cyber Security Act), che hanno l'obiettivo di far sì che le istituzioni e le Organizzazioni siano più resilienti di fronte ai cyber attacchi che possono compromettere l'erogazione di beni e servizi il cui funzionamento dipende appunto dalle tecnologie informatiche e dalla loro messa in sicurezza. Anche in questo contesto si rileva una scarsa conoscenza dei requisiti imposti dal legislatore da parte di dirigenti, manager e lavoratori che potrebbero sfociare in impatti contrattuali, legislativi e di responsabilità civile con conseguenze anche critiche per le Organizzazioni.

A tal proposito, una recente proposta della Commissione Europea al Parlamento in merito all'aggiornamento della direttiva NIS (NISD2), che regola la resilienza delle entità che erogano beni e servizi per la collettività, esorta dirigenti e manager a seguire regolarmente corsi di formazione specifici per acquisire conoscenze e competenze sufficienti al fine di individuare e valutare i rischi e le pratiche di gestione della cyber sicurezza e il loro impatto sulle operazioni delle Organizzazioni che gestiscono.

Quale formazione è necessaria

Lavorando a stretto contatto con le Organizzazioni, in generale si riscontrano programmi di formazione minimali verso i lavoratori sia in termini di tempo dedicato alla formazione, sia in termini di argomenti trattati, che risultano oggettivamente insufficienti per far fronte alle esigenze attuali di protezione efficace dei dati personali e delle informazioni di business.

In termini generali le istruzioni che andrebbero somministrate agli utenti dovrebbero trattare i seguenti argomenti di base:

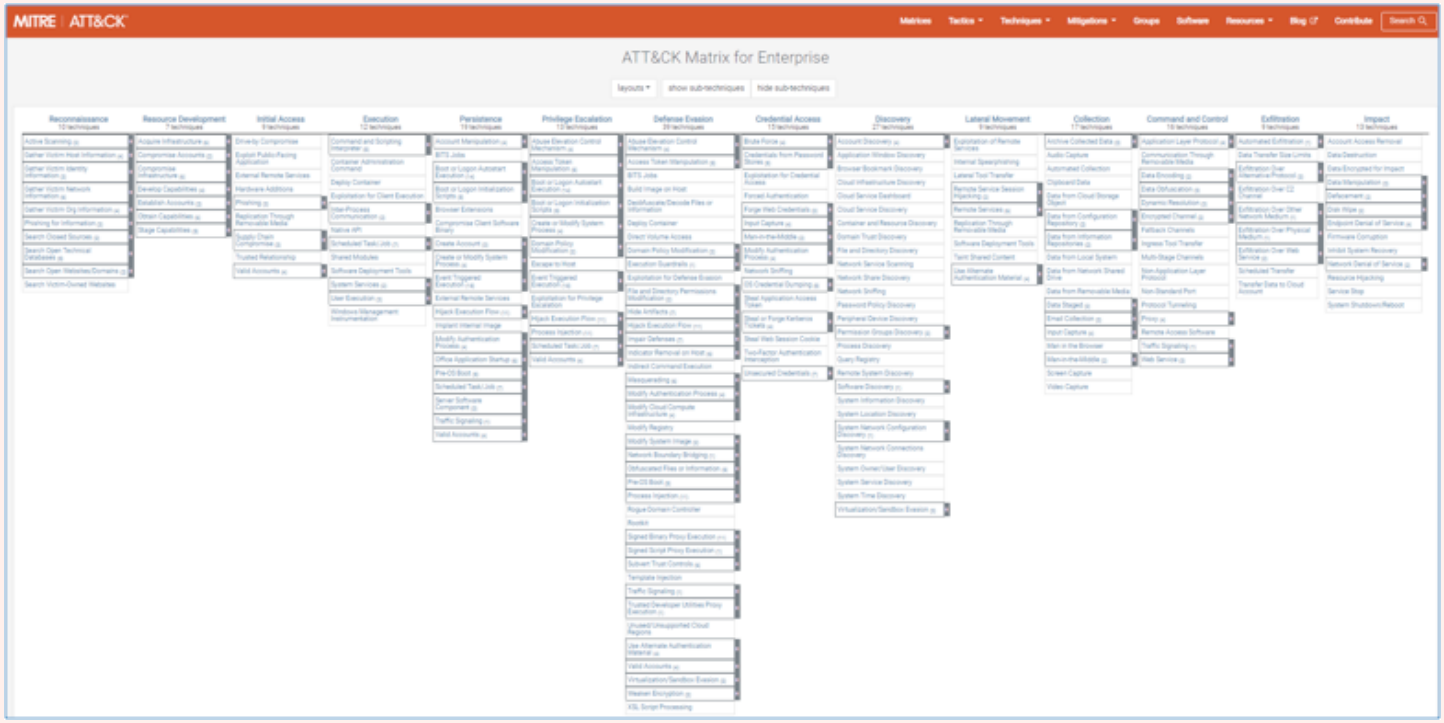
1. formazione di sintesi sulle norme che regolano la protezione dei dati personali, la resilienza dei sistemi e la sicurezza delle informazioni, sugli obblighi legislativi delle Organizzazioni e sulle responsabilità dei lavoratori che trattano dati durante

l'esercizio delle proprie mansioni;
2. formazione sulle politiche e le procedure operative messe a disposizione dalle Organizzazioni per il governo della sicurezza delle informazioni;
3. formazione di base in materia di cyber security.

Relativamente a quest'ultimo aspetto, una formazione carente o addirittura assente sulla cyber security costituisce una importante vulnerabilità e può comportare rischi elevati di attacchi come il phishing e il social engineering.

È evidente che un lavoratore non opportunamente istruito non può essere in grado di riconoscere un tentativo di attacco cyber e, inconsapevolmente, può favorire uno dei primi passi della "cyber kill chain" (fasi di Initial access ed Execution evidenziate in figura 2), che generalmente ha lo scopo di esfiltrare dati o minare la disponibilità dei sistemi e servizi.

Figura 2 **Fasi della cyber kill chain di un attacco informatico (Fonte: Mitre.org - https://attack.mitre.org/)**



I modelli di formazione

In termini di modelli di formazione è importante individuare che cosa sia effettivamente necessario per accrescere in modo efficace ed efficiente la conoscenza sui temi di cyber security per i non addetti ai lavori e quindi ridimensionare i livelli di rischio che insistono sulle persone.

Gli esperti di Cyber Security rilevano come una formazione non opportunamente progettata non possa bastare per costruire un livello di consapevolezza idonea a poter fronteggiare le innumerevoli insidie a cui gli utenti sono sottoposti nella quotidianità. Riguardo ai modelli di formazione, qui di seguito alcuni esempi ed alcune considerazioni a riguardo:

Formazione frontale: consiste nella classica formazione con docente in aula o in remoto che, spiegando in diretta, è in grado di interagire con i discenti e rispondere a tutte le richieste di chiarimento che dovessero servire per approfondire e comprendere i vari temi. È sicuramente la formazione più efficace su cui un'azienda può contare, consigliabile nei casi di una platea formata dai primi livelli aziendali.

Formazione e-Learning: si tratta di formazione attraverso strumenti elettronici e software utile per consentire ai lavoratori di fruire della formazione da qualunque luogo e in qualsiasi momento. Negli ultimi anni la domanda di questi strumenti è cresciuta costantemente. L'efficacia di questo tipo di formazione è fortemente dipendente dalla qualità dei contenuti e dalle funzioni esposte dalla piattaforma che, al minimo, deve permettere il monitoraggio delle somministrazioni oltre a comprovarne la comprensione mediante sessioni di domande.

Formazione Self Learning: consiste nella diffusione di materiale di formazione in forma documentale elettronica o cartacea. In questo caso tutto è lasciato alla volontà dei lavoratori che devono istruirsi in autonomia attraverso i materiali disponibili. Questa modalità di formazione non è indicata a causa di alcuni elementi negativi come la mancanza di controllo dell'effettiva fruizione dei corsi oltre alla mancanza del fattore di misurazione delle competenze.

Formazione "Security pills": definito anche come modello di formazione in "pillole", consiste in un modello di formazione di pochi minuti con un carattere tipicamente prescrittivo che non permette agli utenti di comprendere le motivazioni per le quali

vengano richieste determinati comportamenti.
Questa forma di somministrazione risulta estremamente lacunosa e poco idonea a colmare i delta culturali sulla cyber security utili a ridimensionare i rischi che insistono sulle persone.

Formazione "Technology driven": consiste nella somministrazione della formazione ai lavoratori mediante un ciclo virtuoso di misurazione delle competenze attuato tramite un software di supporto.
La soluzione risolve molte delle problematiche emerse nei modelli descritti precedentemente.
Consiste nell'implementazione di programmi automatizzati che sfruttano tecnologie "people-centric" in grado di colmare la necessità di continua misurazione delle competenze e della somministrazione specifica della formazione, permettendo ai lavoratori di accrescere nel tempo le proprie competenze sulle buone pratiche di sicurezza delle informazioni e protezione dei dati personali.

Conclusioni

Tradizionalmente la difesa cyber delle Organizzazioni è sempre stata basata unicamente sui presidi tecnologici su reti e sistemi focalizzando l'attenzione su indirizzi IP, porte e segmentazione, etc.

Al mondo di oggi gli attaccanti hanno cambiato il loro modo di agire, potendo facilmente utilizzare alcuni social network o i servizi correlati a motori di ricerca o applicazioni simili per lanciare campagne di attacchi mirati contro le Organizzazioni.

Appare quindi chiaro come anche i metodi di difesa debbano adattarsi, agendo su vulnerabilità che non sono più solamente tecnologiche ma che hanno una connotazione più orientata al fattore umano. Per tale motivo appare chiaro come il futuro della difesa cyber debba obbligatoriamente passare per una formazione continua di utenti e lavoratori, preferendo modelli di formazione moderni, continui e più efficaci rispetto a modelli tradizionali ormai superati.

MODELLI E STRUMENTI DI ANALISI PER IL FRAUD MANAGEMENT

Negli ultimi anni abbiamo assistito ad una crescente attenzione al tema della **prevenzione delle frodi** e della contestuale rilevanza del **fraud management**, entrambi trainati dall'aumento degli eventi di frode – soprattutto in ambito cyber – perpetrati ai danni dei clienti degli istituti di credito.

Lo stato emergenziale provocato dalla pandemia ha inoltre determinato un notevole mutamento delle abitudini di una parte della clientela degli istituti bancari, che ha dovuto abbandonare forzatamente i servizi allo sportello per spostarsi verso i servizi di online banking - canale poco o per nulla utilizzato da alcune fasce di utenti e fortemente oggetto dei tentativi più sofisticati di attacco. Tutti questi elementi hanno concorso e portato alla proliferazione delle frodi e dei crimini informatici.

Nonostante le banche si adoperino per avere **strategie chiare** e **contromisure definite**, la continua nascita ed evoluzione di sofisticati pattern di frode tende a rendere poco efficace una parte degli investimenti, economici e non, impiegati.

Sono molteplici i fattori di contesto che aumentano il rischio di frodi informatiche e gli impatti sulle istituzioni finanziarie:

FATTORI DI CONTESTO

- **Consumer Behaviour**
  - Online shopping
  - Data Sharing
  - Social Media
- **Data Breaches**
  - 3rd parties
  - Dark web
  - Internet of Things
- **Payment Digitalisation**
  - Online applications
  - Real Time
  - Remote Banking
- **Access To Technology**
  - Malware
  - Credential Stuffing
  - Social Engineering
- **Organised Crime**
  - Fraud rings
  - Speed of attack
  - Mule accounts

IMPATTI

1. Economic Losses
2. Reputational Risk
3. Regulatory Attention

Così come nel tempo sono cambiati - per complessità e raffinatezza - i meccanismi, gli schemi, gli strumenti e i soggetti a cui sono rivolte le frodi, è altrettanto importante nonché imperativo che allo stesso modo evolvano i sistemi, i protocolli, le metodologie ed i modelli di prevenzione e di contrasto delle frodi, affinché si possano realizzare i presupposti per una efficace ed efficiente azione di contrasto, prevenzione e repressione di questi fenomeni.

I frodatori utilizzano una vasta gamma di metodi per perpetrare le frodi e sfruttare il disallineamento tra sistemi di sicurezza e controlli antifrode. Di seguito riportiamo i principali use case per le frodi digitali:

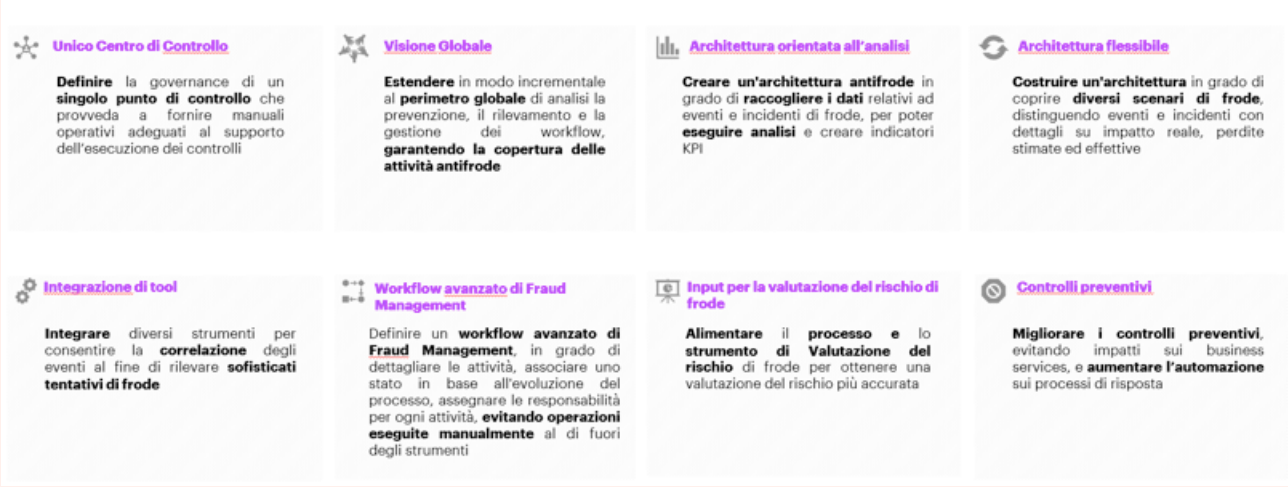
- **Phishing**: E-mail con il logo contraffatto che invita il destinatario a fornire dati riservati;
- **Social Engineering**: Furto di identità sfruttando le credenziali del cliente acquisite tramite social engineering;
- **SIM swapping**: Modifica delle credenziali telefoniche dopo nuova/falsa registrazione della SIM;
- **Malware per raccogliere le credenziali e device fingerprints**: Installazione di Malware su dispositivi client (workstation, smartphone) per la raccolta delle credenziali;
- **Skimming per raccogliere i dettagli di pagamento per usi fraudolenti**: Skimming sulle carte agli sportelli bancari o ATM;
- **Credential Stuffing**: Attacco automatizzato per forzare il processo di autenticazione;
- **Data Breaches**: Furto di identità usando dati derivanti da data breaches;
- **Identità sintetiche che consentono account mule e frodi su depositi**: By-pass del processo di onboarding che abilita gli account mule.

In risposta a tutto questo gli istituti bancari stanno sempre di più prevedendo ed incrementando il budget destinato al mondo antifrode, contemplando altresì una crescita di investimenti dedicati in sviluppo di tecnologie applicate al fraud management.

Enterprise Fraud Management, Big Data Analytics, Artificial Intelligence e **Machine Learning**: sono molti ed in continua crescita i sistemi, le tecniche e gli strumenti che sono stati sviluppati nel corso degli anni per aiutare il mondo bancario – e più in generale il settore finanziario – a contrastare il fenomeno delle frodi.

Il perimetro di azione dei cyber frodatori allo stesso modo è ampio e diversificato deve essere eterogeneo il panorama dei tool impiegati a contrasto: è fondamentale che le banche non si limitino solo a uno specifico strumento ma orientino la strategia di gestione e prevenzione verso più scenari e condizioni, impiegando tool differenti - dedicati a specifiche funzionalità - ma tutti diretti e gestiti a livello centrale.

Pertanto, per una corretta prevenzione, rilevazione ed analisi a sostegno di una più ampia strategia di antifrode, risulta auspicabile un **approccio globale, combinato e parallelo**, che può essere declinato attraverso i seguenti **8 key pillars**:



La nostra esperienza, acquisita nel corso degli anni come supporto alla gestione e repressione del fenomeno delle frodi, ci permette di definire e disegnare un **Target Model Fraud** a 3 livelli:

1. **Fraud Prevention and Detection Layer,** che prevede la ricezione di flussi di dati da diversi canali al fine di rilevare potenziali tentativi di frode e poter quindi generare gli allarmi necessari. Features:
   - Miglioramento delle capacità di rilevazione tramite Machine Learning e Intelligenza Artificiale;
   - Integrazione con fonti di dati esterne per migliorare l'analisi delle frodi
   - Integrazione con Hub di autenticazione per bloccare preventivamente i tentativi di frode
   - Implementazione di un motore unico per tutti i canali
2. **Fraud Handling Layer,** per ricevere e gestire gli allarmi generati dal layer di detection. Features:
   - Gestione tramite un unico *case e incident manager* per tutti i canali, per poter progettare un processo cross channel
   - Potenziamento delle capacità di correlazione degli eventi, al fine di identificare e risolvere casi di frode sofisticati basati su eventi provenienti da diversi canali
   - Accelerazione del processo di risposta agli incidenti sostituendo le attività manuali ripetitive con flussi di lavoro automatizzati grazie all'introduzione di strumenti quali *SOAR* (Security Orchestration, Automation and Response)
3. **Fraud Intelligence Layer,** per analizzare gli eventi fraudolenti occorsi, migliorare le regole di rilevazione e valutare possibili nuove minacce. Features:
   - Utilizzo di tool di analisi verticale per ogni canale con funzionalità avanzate, come Machine Learning e Intelligenza Artificiale
   - Integrazione con gli strumenti di valutazione del rischio di frode per migliorarne le valutazioni

Sono molteplici i *benefici*, sia tecnici che di business , che questo modello porta con sé:

BENEFICI TECNICI,

- Riduzione dei tempi per l'implementazione di nuove tecnologie e modelli analitici

- Architettura flessibile e scalabile
- Soluzione tecnologica modulare e replicabile
- Integrazione multi vendor
- Apprendimento automatizzato del modello attraverso l'uso di feedback
- Riduzione di interventi manuali con contestuale miglioramento qualitativo

BENEFICI DI BUSINESS

- Riduzione del rischio di frode
- Incremento della customer satisfaction ed aumento della fidelizzazione
- Riduzione dei reclami dei clienti
- Aumento del livello di sicurezza del cliente
- Miglioramento della qualità del servizio fornito al cliente
- Incremento della Brand & Company Identity
- Aumento della capacità di identificazione dei fenomeni fraudolenti

Un *Target Model Fraud* non può prescindere da solide e valide componenti, interconnesse le une con le altre.

È tuttavia importante ricordare che le azioni, i processi e le strategie messe in atto a contrasto delle frodi non possono prescindere da un ulteriore elemento, tanto importante quanto essenziale: la **user experience** del cliente.

Questa risulta pertanto essere un'ulteriore sfida in ambito fraud management: trovare il giusto compromesso nel delicato equilibrio tra **esperienza utente**, intesa come l'insieme degli elementi che riguardano le interazioni tra il cliente e la banca, e l'erogazione del servizio-prodotto in piena sicurezza.

LA PROPOSTA DI DIRETTIVA NIS 2.0 E IL PERIMETRO NAZIONALE DI SICUREZZA CIBERNETICA

Appena due anni dopo la scadenza del termine per il recepimento della direttiva NIS da parte degli Stati membri, **il 16 dicembre 2020 la Commissione europea ha presentato**, nell'ambito della Strategia europea per la cybersecurity, **una proposta di direttiva NIS 2.0**.

Questa proposta mira a **sostituire e sviluppare ulteriormente il quadro europeo di Network and Information Security**, entrato in vigore nel 2016 e considerato uno degli atti più importanti della legislazione sulla sicurezza cibernetica emanati dall'Unione Europea.

La ragione principale per la quale la Commissione ha deciso di velocizzare i tempi di aggiornamento rispetto alle previsioni precedenti è **l'affermazione di nuove tecnologie nel panorama mondiale** che hanno contribuito ad **alimentare le preoccupazioni sulla sicurezza dei relativi sistemi**.

Rispetto alla precedente normativa, **la Proposta avanzata dalla Commissione Europea, attualmente al vaglio del Consiglio e del Parlamento Europeo, mira ad introdurre una serie di novità** che avranno un impatto significativo per gli attuali OSE e per i nuovi soggetti che ricadranno nei settori annoverati dalla normativa.

Proprio in questo ambito, un'evidente novità riguarda l'**estensione dei settori**, ai quali si aggiungono:

- Pubblica Amministrazione
- Servizi Postali
- Produzione e Distribuzione Prodotti Chimici
- Produzione e Distribuzione Prodotti Alimentari
- Gestione Rifiuti

Inoltre, la norma prevede l'introduzione delle **categorie di soggetti "essenziali" e "importanti"** quale novità rispetto alla pre-

cedente normativa.

Un terzo elemento di novità è dato dalla previsione della cosiddetta **"Regola di taglia"** secondo la quale saranno inclusi nel perimetro tutti i soggetti considerati medie e grandi imprese, e non solo le grandi imprese, come previsto dai criteri di selezione suggeriti dalla prima Direttiva NIS.

Verrà anche ampliato l'elenco di misure tecnico-organizzative da adottare nelle fasi di gestione del rischio. In particolare, saranno previsti controlli su sistemi informatici di terze parti (gestori) e sulla crittografia.

Nella proposta spicca anche un **incremento notevole delle sanzioni** imposte in caso di violazione delle misure di gestione del rischio e degli obblighi di notifica. Tali sanzioni potranno ammontare **fino a 10 000 000 di euro o al 2% del fatturato totale mondiale annuo** dell'operatore interessato.

In ultimo, le nuove disposizioni stabiliscono un **tempo massimo per la notifica di incidente rilevante** al CSIRT, ovvero entro le 24 ore successive all'evento, mentre il Report Finale (post-incidente) dovrà essere consegnato 1 mese dopo la conclusione dell'incidente.

La Commissione infine propone la costituzione di un **gruppo di supporto**, **denominato EU-Cyclon** (European Cyber Crisis Liaison Organization Network), che si occuperà della gestione e coordinamento degli incidenti e crisi su vasta scala, al fine di assicurare un proficuo scambio di informazioni fra Stati membri ed Istituzioni.

Nel caso specifico del settore bancario, la normativa fa riferimento ad un'altra proposta di regolamento relativo alla resilienza operativa digitale per il settore finanziario (il cosiddetto **Regolamento DORA**).

L'articolo 1, comma 4 (Cooperazione a livello nazionale) della NIS 2.0 dispone che gli Stati Membri debbano assicurare la dovuta **cooperazione con le autorità finanziarie nazionali** designate dal Regolamento Dora.

L'articolo 12 della Direttiva NIS 2.0 invece stabilisce un Gruppo di Cooperazione per facilitare la cooperazione strategica e lo

scambio di informazioni fra gli Stati Membri. Il comma 3 dello stesso articolo stabilisce che le **tre Autorità Europee di Vigilanza** (**EBA** - European Banking Authority; **EIOPA** - European Insurance and Occupational Pensions Authority; **ESMA** – European Securities and Markets Authority) **possono partecipare alle attività del Gruppo di Cooperazione**, in accordo con l'articolo 17(5)(c) del Regolamento Dora.

Sul piano nazionale, invece, si segnala che l'articolo 1, comma 1 della legge 18 Novembre 2019, n. 133 ha istituito **il Perimetro di sicurezza nazionale cibernetica**, con l'obiettivo di "assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di [...] un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale [...]" (art 1(1), L. n.133, 18 novembre 2019).

Tali soggetti dispongono di reti, sistemi e servizi informatici:

- il cui malfunzionamento, interruzione – anche parziale – o uso improprio può pregiudicare la sicurezza nazionale;
- necessari per l'esercizio di una funzione essenziale dello Stato;
- necessari per l'assolvimento di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato.

I soggetti inclusi nel perimetro sono le **amministrazioni pubbliche**, gli **enti e gli operatori nazionali, pubblici e privati** (tra cui anche gli operatori dei servizi essenziali, ai sensi della Direttiva NIS attualmente in vigore, individuati all'interno del settore bancario) aventi sede nel territorio nazionale che offrono prestazioni relative alla fornitura di un **servizio essenziale** per il mantenimento delle attività essenziali e dal cui malfunzionamento, interruzione, anche parziale, possa derivare un pregiudizio per la sicurezza nazionale

I soggetti del "Perimetro" sono stati individuati con un Decreto attuativo quattro mesi dopo l'entrata in vigore della legge ed elencati all'interno di un atto amministrativo, adottato e periodicamente aggiornato dalla Presidenza del Consiglio dei Ministri, su proposta del CISR.

L'Articolo 1, comma 3, definisce le **procedure secondo cui i soggetti del Perimetro di sicurezza nazionale cibernetica segnalano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici**, come illustrato nella figura 2, e le misure volte a garantirne elevati livelli di sicurezza.

Figura 1 **Procedure di segnalazione degli incidenti**

Tali misure si riferiscono a vari aspetti tipici della sicurezza informatica di una organizzazione tra le quali si citano, ad esempio, la **struttura organizzativa preposta alla gestione della sicurezza** e le **politiche di sicurezza e gestione del rischio** interne all'organizzazione.

Un altro aspetto interessato dalle misure di sicurezza riguarda la **mitigazione e gestione degli incidenti e la loro prevenzione**, anche attraverso interventi su apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza.

In ultimo, la **protezione fisica e logica dei dati**, la **gestione delle reti e dei sistemi informativi**, la **gestione operativa**, ivi compresa la contiguità del servizio, e il **monitoraggio, test e controllo** rappresentano tutti aspetti considerati dall'articolo in questione.

I soggetti compresi all'interno del Perimetro di sicurezza cibernetica che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici, appartenenti a categorie individuate, ne danno **comunicazione al Centro di valutazione e certificazione nazionale (CVCN),** istituito presso il Ministero dello sviluppo economico; la comunicazione comprende anche la **valutazione del rischio** associato all'oggetto della fornitura, anche in relazione all'ambito di impiego.

Il CVCN può effettuare verifiche preliminari ed imporre condizioni e test di hardware e software. L'articolo 13 del Decreto del Presidente della repubblica (D.P.R.) 5 febbraio 2021, n. 54 specifica la lista di funzioni secondo le quali sono individuate le categorie dei beni, sistemi e servizi ICT oggetto della valutazione da parte del CVCN.

In particolare, le funzioni in questione sono:

- commutazione oppure protezione da intrusioni e rilevazione di minacce informatiche in una rete, ivi inclusa l'applicazione di politiche di sicurezza;
- comando, controllo e attuazione in una rete di controllo industriale;
- monitoraggio e controllo di configurazione di una rete di comunicazione elettronica;
- sicurezza della rete riguardo alla disponibilità, autenticità, integrità o riservatezza dei servizi offerti o dei dati conservati, trasmessi o trattati;
- autenticazione e allocazione delle risorse di una rete di comunicazione elettronica;
- implementazione di un servizio informatico per mezzo della configurazione di un programma software esistente oppure

dello sviluppo, parziale o totale, di un nuovo programma software, costituente la parte applicativa rilevante ai fini dell'erogazione del servizio informatico stesso.

Gli art. 7 e 8 del D.P.C.M. 131/2020 richiedono ai soggetti coinvolti nel Perimetro i seguenti adempimenti:

1. I soggetti pubblici e privati devono **trasmettere**, rispettivamente alla Presidenza del Consiglio dei Ministri competente per l'innovazione tecnologica e la digitalizzazione e al Ministero dello sviluppo economico i seguenti documenti:
   - **Elenco dei beni ICT** con l'indicazione delle reti, dei sistemi informativi e dei servizi informatici che li compongono e relativa analisi del rischio, osservando i criteri individuati dall'art.7, comma 2.
   - **Elenco contenente la descrizione dell'architettura e della componentistica** relativa ai propri beni ICT, di cui sopra.
2. Tali documenti devono essere trasmessi **entro sei mesi** dal ricevimento della comunicazione di avvenuta inclusione nel Perimetro di Sicurezza Nazionale Cibernetica.
3. La trasmissione dei suddetti elenchi, così come il loro futuro aggiornamento, deve avvenire **attraverso la specifica piattaforma digitale messa a disposizione dal DIS** e costituita per lo svolgimento delle attività di prevenzione, preparazione e gestione delle crisi cibernetiche affidate al Nucleo Sicurezza Cibernetica (NSC).

Il D. L. n. 105 del 2019 introduce il **Centro di valutazione e certificazione nazionale (CVCN)** affidandogli incarichi relativi all'approvvigionamento di prodotti, processi, servizi di tecnologie dell'informazione e della comunicazione (ICT) e associate infrastrutture - qualora destinati a reti, sistemi informativi, sistemi informatici ricompresi nel Perimetro di Sicurezza Nazionale Cibernetica.

In particolare, il Centro **a) contribuisce all'elaborazione delle misure di sicurezza**, per ciò che concerne l'affidamento di forniture di beni, sistemi e servizi ICT; **b) svolge attività di valutazione del rischio** e di verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità; **c) elabora e adotta schemi di certificazione cibernetica**, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea.

Gli articoli 5, 6 e 7 del D.P.R. 5 febbraio 2021, n. 54 descrivono le tre fasi del procedimento di verifica e valutazione dei beni,

sistemi e servizi ICT in esame:

- **Fase 1) Verifiche preliminari, individuazione di condizioni e test (art. 5)**: in questa prima fase, il CVCN richiede al soggetto incluso nel perimetro le informazioni preliminari al fornitore e definisce le eventuali tipologie di test (corretta implementazione, test di intrusione) da eseguire.
- **Fase 2) Preparazione esecuzione dei test (art. 6)**: a seguito della comunicazione, attraverso una piattaforma informatica il CVCN verifica se l'oggetto di fornitura è stato già sottoposto a precedenti valutazioni o se sono in corso valutazioni; in caso negativo a) il CVCN può affidare l'esecuzione dei test ad un laboratorio accreditato, informandone il soggetto incluso nel perimetro e il fornitore; b) il CVCN invita il fornitore a predisporre le attività preliminari all'esecuzione dei test e definiscono la sede in cui svolgere tali attività.
- **Fase 3) Esecuzione dei Test (art 7)**: il CVCN comunica l'avvio dei test al soggetto incluso nel perimetro e al fornitore. I test sono eseguiti presso i laboratori del CVCN. Infine, il CVCN redige un rapporto di prova nel quale sono indicati in dettaglio l'ambiente di test, le prove eseguite ed i relativi esiti.

Il sistema sanzionatorio

L'articolo 1, commi 9-12, definisce un **articolato sistema sanzionatorio** per i casi di violazione degli obblighi previsti dalla legge in esame (art 1(9-12), L. n. 133, 18 novembre 2019).

Secondo il comma 12 le **autorità competenti** per l'accertamento delle violazioni e per l'irrogazione delle sanzioni amministrative sono la Presidenza del Consiglio dei Ministri per i soggetti pubblici e il Ministero dello sviluppo economico per i soggetti privati. Il comma 9 invece specifica le somme minime e massime relative all'ambito sanzionabile. Tali somme vanno da un **minimo di 200 000 euro** ad un **massimo di 1 800 000 euro**.

EVOLUZIONE DEI FENOMENI DI FRODE ATTUATI ATTRAVERSO LE TELCO E POSSIBILI TECNICHE DI CONTRASTO

Aumentare la sicurezza per Telco e Banche migliorando la customer experience

Risultati preliminare sperimentazione gratuita anti sim-swap

Come anticipato nel Report 2020, a partire da luglio dello scorso anno Kaleyra ha fornito le proprie competenze e infrastruttura per la realizzazione di un servizio antifrode volto a rilevare il fenomeno di SIM SWAP durante l'invio di SMS OTP per l'esecuzione di transazioni bancarie. L'approccio proposto permette di recepire dagli MNO (Mobile Network Operators) aderenti alla sperimentazione il codice IMSI della SIM ricevente il SMS OTP e condividerlo, previa procedura di hashing, con il soggetto bancario al quale si sta richiedendo l'esecuzione di una transazione. Il soggetto bancario può, in near real time o a posteriori, verificare se sia avvenuto o meno un cambio nel codice IMSI associato al numero mobile, segnale di potenziale SIM SWAP, e quindi decidere per il blocco della transazione o l'esecuzione di ulteriori steps di verifica.

I risultati preliminari riportati dalle banche e istituti finanziari che partecipano alla sperimentazione hanno mostrato come il servizio abbia permesso di monitorare oltre 10M di transazioni nei soli primi 3 mesi di esercizio per circa 1.5M di SIM coinvolte rilevando oltre 10.000 eventi di SIM SWAP.

I tentativi di frode registrati nel periodo di osservazione sono stati circa 813 senza nessun evento di falso positivo; grazie all'introduzione da parte delle banche della ricezione in real time del codice IMSI (hashato) al momento dell'invio del OTP di conferma transazione, il 100% delle frodi sono state intercettate e oltre il 95% delle frodi basate su SIM SWAP sono state bloccate in tempo.

Evoluzione del servizio anti sim-swap

A fronte dei risultati positivi della sperimentazione, sembra possibile prevedere un'evoluzione del servizio anti sim-swap in

un vero e proprio Hub anti-frode in grado di semplificare l'accesso al servizio in real time a soggetti bancari e finanziari e di velocizzare l'integrazione con i sistemi degli operatori per il recupero delle informazioni di identificazione dell'utente (IMSI e altri attributi registrati presso gli MNO).

- Il nuovo Hub renderà disponibili un set standard di REST API tramite le quali i soggetti interessati potranno, anche in maniera svincolata dall'invio del SMS OTP, verificare le informazioni rilevanti per l'identificazione e autorizzazione dell'utente.
- L'Hub anti-frode, riconosciuto l'operatore di appartenenza del numero mobile da verificare, indirizzerà la richiesta all'operatore di destinazione secondo le modalità specifiche di integrazione.
- Ricevuta la risposta dai sistemi di rete dell'operatore, questa sarà restituita in formato normalizzato su un endpoint o una coda condivisa con la banca. In questo modo, banche e istituti finanziari potranno accedere, tramite un'unica integrazione, alle informazioni rese disponibili da ogni singolo operatore.

L'implementazione di un Hub anti-frode permetterà non solo di erogare il servizio anti SIM SWAP ma di implementare con il supporto degli operatori nuovi servizi per nuovi casi d'uso come KYC in fase di onboarding, autenticazione per login al proprio account o aree riservate delle App/web, autorizzazione ad operazioni e transazioni importanti o considerate rischiose.

Figura 1 **Schematizzazione del flusso per il nuovo servizio anti sim swap**

Verified SMS/ verified Calls

Nel corso del 2020 Google, tramite i propri Business Partner, ha lanciato diversi servizi, ad oggi completamente gratuiti lato Google, per ammodernare le Comunicazioni Business sul canale SMS e sul canale voce e contrastare nello stesso tempo i fenomeni di phishing/smishing e spam con l'obiettivo di aumentare l'engagement e la fiducia dei consumatori finali con il brand.

In particolare, nella seconda metà del 2020 è stato lanciato in Italia il servizio di verified SMS (vSMS), tramite il quale è possibile garantire al destinatario non solo l'autenticità del SMS ricevuto in termini di SenderId e di contenuto del SMS stesso, ma anche mostrare informazioni aggiuntive rispetto a un normale SMS volte a rafforzare il senso di sicurezza e fiducia dell'utente.

Un'organizzazione che aderisce al servizio di verified SMS può registrare in maniera univoca a livello mondiale un logo, un business name e una breve descrizione del proprio business che saranno mostrati direttamente all'interno dell'App di messaggistica sul dispositivo dell'utente alla ricezione del SMS nel momento in cui ne sia confermata l'autenticità.

Il servizio di verified SMS prevede inoltre che il contenuto del messaggio sia cifrato in maniera irreversibile tramite hash e quindi temporaneamente salvato sui server del servizio stesso; il device abilitato alla ricezione di verified SMS, alla ricezione di un messaggio, esegue la medesima cifratura tramite hash e ne verifica la corrispondenza con quanto salvato sui server del servizio. Se viene confermata la correttezza e autenticità del messaggio ricevuto rispetto a quello salvato dal provider, il device recupera le informazioni business dell'organizzazione (logo, business name e descrizione salvati alla registrazione del brand al servizio) e le mostra insieme al testo del messaggio con un badge blu a conferma della verifica eseguita con successo.

Un eventuale messaggio fraudolento, che arrivasse tramite grey route con un senderId simile o anche identico a quello ufficiale della Banca, non potrebbe essere verificato dal device dato che il provider di origine non avrebbe accesso al servizio per salvare la propria versione dell'algoritmo di hash e sarebbe mostrato privo di tutte le informazioni di validazione altrimenti presenti (logo, business name, descrizione, badge blu) indicando all'utente che si tratta appunto di una frode.

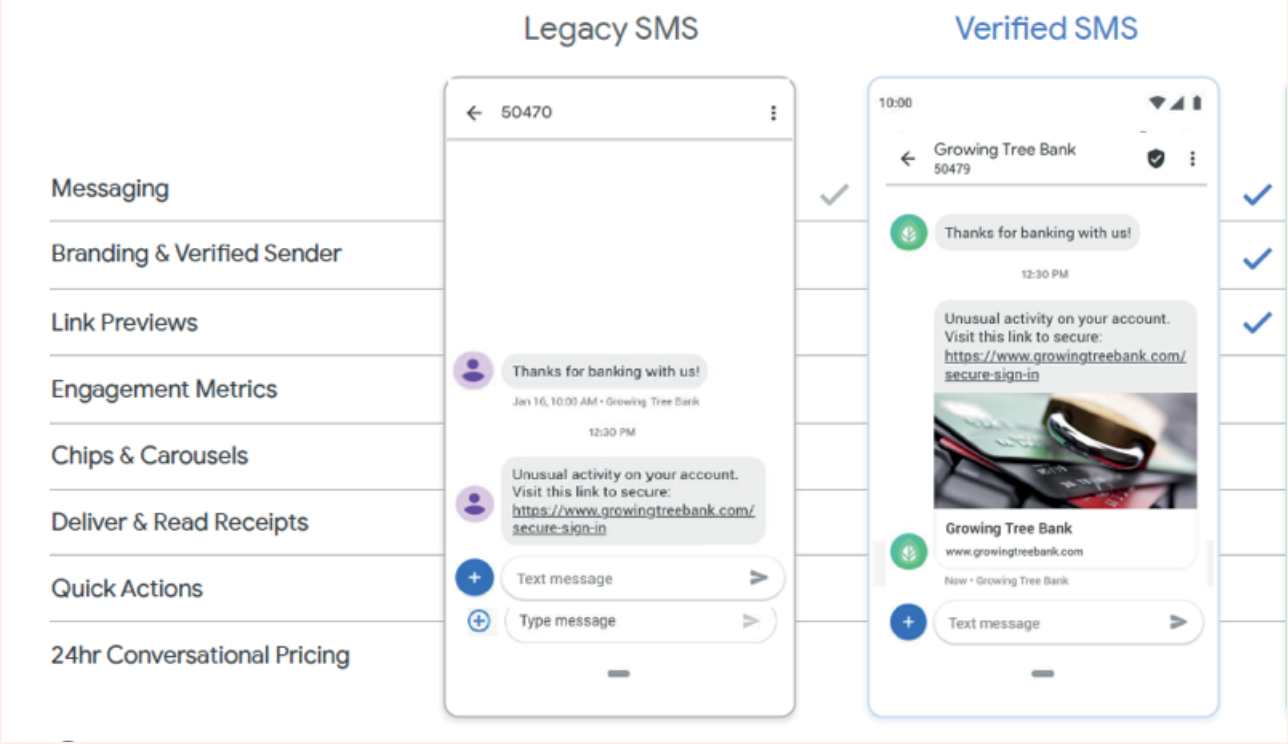
In aggiunta, nessun SMS/MMS potrebbe mai simulare o forzare il sistema operativo a mostrare le informazioni che la Banca ha registrato per l'esecuzione del servizio.

Verified Call è un analogo servizio per il canale telefonico che permette alle organizzazioni di chiamare i propri clienti mostrando sul telefono dell'utente il proprio logo, il proprio business name e opzionalmente il motivo della telefonata a prescindere dal fatto che il numero sia registrato o meno nella rubrica del dispositivo, garantendo così un incremento del rate di risposta e un aumento della fiducia dell'utente verso il brand.

L'organizzazione che aderisce al servizio registra nei server del servizio stesso il proprio logo, il proprio business name, i numeri di telefono dai quali viene generata la chiamata e l'eventuale lista di possibili motivi per la chiamata. Al momento del setup della chiamata il provider registra nei server del servizio il numero chiamante, il numero chiamato, la fase della chiamata e l'eventuale motivo. Alla ricezione della telefonata, il dispositivo dell'utente verifica se nei server del servizio esiste un record con il medesimo numero chiamato, chiamante e fase della telefonata, e se viene verificata la corrispondenza, vengono mostrate le informazioni che il brand ha salvato: logo, descrizione e motivo della chiamata.

Il servizio Verified Call permetterà quindi di abbattere il livello di telefonate indesiderate cui l'utente risponde, aumentando invece il tasso di risposta delle telefonate eseguite dal brand. Il servizio vCall sarà lanciato in Italia nei prossimi mesi, dopo il lancio in altri paesi dove è stato sperimentato con successo.

Figura 2 **Esempio di visualizzazione di un verified SMS vs SMS tradizionale**



Sistemi di identificazione friction-less tramite terminale mobile

Un tema particolarmente importante nei prossimi anni sarà quello di rendere sempre più immediata e semplice l'autenticazione e l'identificazione forte degli utenti tramite servizi e strumenti che non necessariamente richiedono all'utente stesso la memorizzazione, ricezione o generazione di un codice sul proprio device per l'accesso al proprio account o l'esecuzione di particolari operazioni.

In particolare, i seguenti macro-scenari possono beneficiare di questi servizi:

- Identificazione
- Autorizzazione
- Know Your Customers (KYC)

Il mercato si presenta oggi con diverse soluzioni standard e proprietarie che permettono di realizzare una "strong authentication" silente o trasparente all'utente tipicamente legate alle informazioni che l'operatore di telefonia conosce (es. anagrafiche, SIM, stato di registrazione sulla rete) e può mettere a disposizione, direttamente o tramite aggregatore, all'organizzazione.

In ciascuno dei tre macro-scenari identificati queste soluzioni possono mettere in contatto i sistemi della banca o dell'organizzazione tramite API normalizzate con i sistemi dei diversi operatori per la verifica dell'identità dell'utente partendo dal numero del device mobile. Ad oggi, gli operatori possono fornire diversi livelli di informazioni alle organizzazioni per l'identificazione e/o autorizzazione, dal codice IMSI associato alla SIM (o l'informazione circa l'ultimo cambio IMSI) ad informazioni anagrafiche registrate all'attivazione della SIM come nome, cognome, residenza, fino ad un set ulteriore di informazioni legate ad esempio a Carta d'Identità o attributi/preferenze che l'utente abbia accettato di condividere per l'erogazione di determinati servizi, o a informazioni di geo-localizzazione.

La condivisione delle informazioni per fini di identificazione e autorizzazione o KYC è sempre fatta nel rispetto delle normative privacy utilizzando algoritmi di hash in modo che sia impossibile risalire al dato originale, ma solo alla verifica positiva o negativa dei dati.

www.certfin.it