

CERTFin

OBIETTIVI

COSTITUIRE UN SINGLE POINT OF CONTACT (POC)
PER IL SETTORE FINANZIARIO

PROMUOVERE LA COOPERAZIONE PUBBLICO-PRIVATO
E INTERSETTORIALE

FAVORIRE LO SCAMBIO DI INFORMAZIONI SU INCIDENTI,
MINACCE INFORMATICHE, VULNERABILITÀ E LEZIONI APPRESE

SVOLGERE ANALISI SU SPECIFICI EVENTI CYBER
E VALUTARNE L'IMPATTO PER IL SISTEMA

SUPPORTARE LA RISPOSTA AGLI INCIDENTI
E IL PROCESSO DI GESTIONE DELLE CRISI

DEFINIRE LINEE GUIDA, METODOLOGIE, PRASSI
E STRUMENTI PER LA GESTIONE DEL RISCHIO INFORMATICO

ACCRESCERE LA CONSAPEVOLEZZA E LA CULTURA
DELLA SICUREZZA

SVILUPPARE LA COOPERAZIONE INTERNAZIONALE

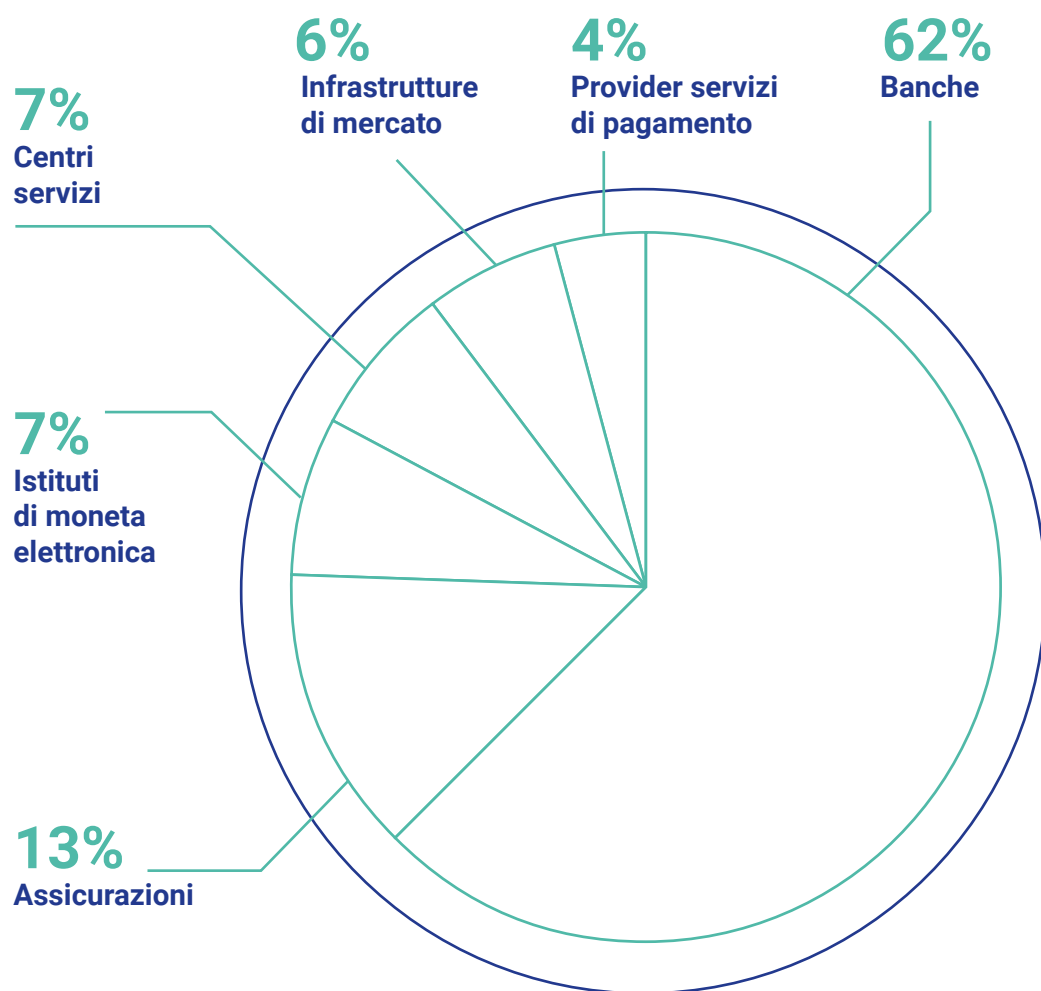


Il CERTFin – CERT Finanziario Italiano è un'iniziativa cooperativa pubblico-privata finalizzata a innalzare la capacità di gestione del rischio informatico degli operatori finanziari e la cyber resilience del sistema finanziario italiano. Fornisce supporto operativo e strategico alle attività di prevenzione, preparazione e risposta agli attacchi informatici e agli incidenti di sicurezza.

Il CERTFin è presieduto dalla Banca d'Italia e dall'Associazione Bancaria Italiana ed è operato dal Consorzio ABI Lab.

CONSTITUENCY E NETWORK

Dopo sei anni di attività, è oggi attiva una rete di oltre 400 esperti di cybersecurity dei servizi finanziari relativi a 68 realtà aderenti:



Il CERTFin collabora attivamente con ACN (Agenzia per la Cybersicurezza Nazionale), con la quale nel gennaio 2023 ha sottoscritto un Protocollo di Collaborazione.

Inoltre, collabora con diversi network e strutture che operano nell'ambito cyber per lo scambio di informazioni volte a proteggere sistemi e risorse critici e contrastare eventuali attacchi in ambito nazionale e internazionale:

Forze dell'Ordine
(Europol, Polizia di Stato, Cnaipic)

Istituzioni e Autorità
(ACN, AGCom, Gpdp, Consob, Ivass, Ania, Codise)

Operatori telco

Centri di eccellenza
(CSIRT Italia, CINI, AIXIA)

CERT internazionali

Gruppi di lavoro europei e internazionali
(EBF, Enisa, EPC, G7, IBFed, Swift)

Comunità internazionali
(Trusted Introducer, First, FS-ISAC)

SERVIZI E ATTIVITÀ

Le attività del CERTFin sono sviluppate secondo logiche di cooperazione a beneficio di tutti gli operatori finanziari aderenti.

FIN-ISAC

L'obiettivo principale del servizio Fin-ISAC è innalzare la cyber resilience delle strutture finanziarie attraverso il potere dell'informazione. Le attività principali includono:

Raccolta e scambio tempestivo di informazioni su minacce informatiche, vulnerabilità, incidenti;

Aggiornamento rispetto allo stato e all'evoluzione delle minacce cyber e delle possibili contromisure da prevedere (modelli di attacco, contromisure, best practice, etc.);

Produzione di report periodici di aggiornamento e dimensionamento delle frodi informatiche di settore attraverso questionari e analisi statistiche.

LE INFORMAZIONI VENGONO RACCOLTE E CONDIVISE IN TEMPO REALE TRAMITE MISP

Piattaforma dedicata per condividere IoC all'interno della Constituency e con fonti esterne. Attualmente sono 35 i PSP italiani direttamente collegati all'istanza MISP del CERTFin. Dall'inizio delle attività di infosharing, il CERTFin ha condiviso più di 45 milioni di IoC.

I NUMERI DEL 2023

2427 → 2711

Alert condivisi su diverse minacce

Report considerando ulteriori informazioni / aggiornamenti

334

Segnalazioni inviate a singole banche su minacce, possibili compromissioni o specifiche vulnerabilità della rete

2363

Indicatori di frode condivisi

284

Alert su Merchant coinvolti in attività fraudolente

CYBER KNOWLEDGE AND SECURITY AWARENESS

OSSERVATORIO CYKSA

Incontri periodici della community con focus su analisi di frodi e attacchi, ma anche approfondimenti normativi e tecnologici:



Confronto e condivisione su specifici temi con il coinvolgimento di cyber advisor e soggetti esterni (es. Polizia Postale, Telco Provider, rappresentanti dei circuiti di pagamento internazionali)

Approfondimento delle normative in materia di sicurezza informatica e cyber risk

Rilevazione frodi per il settore bancario, effettuata annualmente dal CERTFin a partire dal 2012. I risultati vengono pubblicati nel Rapporto Sicurezza e Frodi Informatiche in Banca che contiene trend e analisi di dettaglio sui principali fenomeni di frode che hanno interessato la comunità finanziaria italiana

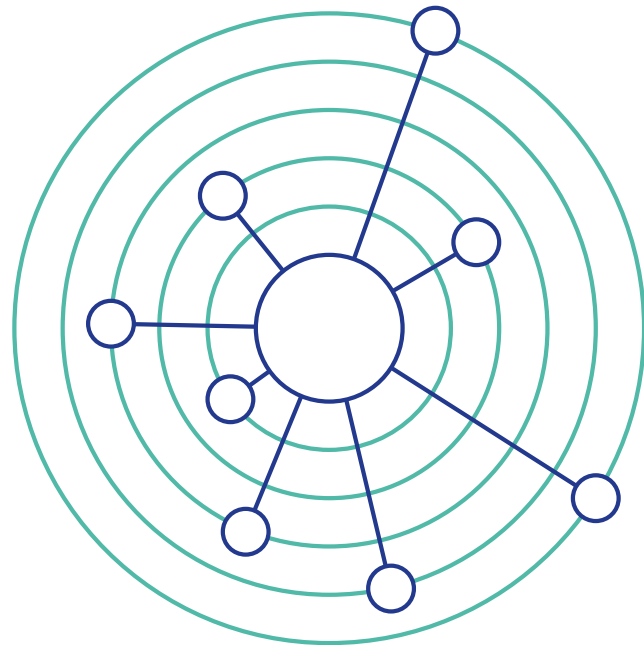
Definizione di campagne di sensibilizzazione sulle tematiche di cybersecurity

THREAT INTELLIGENCE

ANALISI E DEFINIZIONE DEL THREAT LANDSCAPE SCENARIO PER IL SETTORE FINANZIARIO ITALIANO

Attraverso l'utilizzo di una piattaforma altamente ottimizzata, il CERTFin raccoglie, processa e analizza informazioni su eventi cyber provenienti da trusted sources con l'obiettivo di produrre uno scenario per il settore finanziario.

Le sorgenti utilizzate sono condivise da network internazionali e dalle stesse organizzazioni aderenti alla Constituency. Con l'obiettivo di fornire conoscenza e permettere l'adozione di misure preventive per le strutture finanziarie, il CERTFin diffonde bollettini mensili e il Rapporto "Threat Landscape Scenario" a cadenza semestrale.

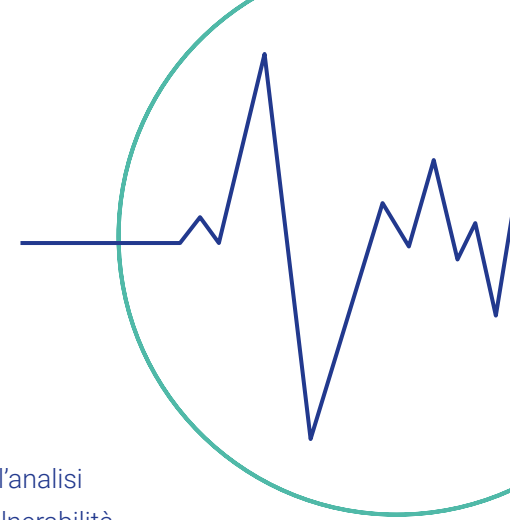


EMERGENCY CENTER

SUPPORTARE I MEMBRI DEL CERTFin QUANDO SI VERIFICA UN INCIDENTE

L'attività di gestione delle emergenze cyber supporta l'analisi e il coordinamento in caso di incidente / artefatto/ vulnerabilità di sicurezza subito da un membro della Constituency del CERTFin, affiancandosi alle capacità interne di natura tecnologica e/o di processo del soggetto aderente.

A evento concluso le informazioni raccolte durante l'emergenza sono anonimizzate e condivise a livello di settore per applicare le strategie di risposta più appropriate, maturate sulla base delle lessons learned.



CYBER EXERCISES

Predisposizione di esercitazioni e simulazioni tra i principali attori del settore bancario e delle entità coinvolte (istituzioni locali, enti internazionali, etc.), finalizzate a potenziare l'effettiva capacità di prevenzione e reazione.

TABLE TOP SIMULATION

CAPTURE THE FLAG

RED TEAMING

CYBERSECURITY AWARENESS

Realizzazione di campagne periodiche di cybersecurity awareness con la partecipazione di istituzioni e banche aderenti.

I NAVIGATI

L'obiettivo della campagna è incoraggiare i clienti bancari a entrare a far parte di una grande famiglia di esperti di cybersecurity, la famiglia "Navigati" per sensibilizzarli ad un uso informato e sicuro degli strumenti e dei canali digitali.

Campagna veicolata su TV, radio, stampa, web, social, affissionistica.

inavigati.it



CYBERSICURI

"Cybersicuri - impresa possibile", la campagna di informazione sulla sicurezza informatica che si rivolge al mondo delle imprese per sensibilizzarle sull'importanza di investire nella sicurezza dei sistemi e nella formazione dei propri dipendenti.

Campagna veicolata su radio, stampa, web, social.

cybersicuri.it



PERCHÉ ADERIRE AL CERTFin

Per prendere parte ad un "trusted circle" tra operatori del settore finanziario per lo scambio di informazioni utili a prevenire e mitigare attacchi cyber e fenomeni fraudolenti

Per ricevere informazioni di intelligence a livello strategico, tattico e operativo

Per partecipare attivamente ad una community in cui il confronto continuo e lo scambio tempestivo di Indicatori di Compromissione e Indicatori di Frode consentono di restare aggiornati sulle tematiche di interesse per il settore

Per incrementare conoscenze e competenze attraverso la partecipazione a sessioni di esercitazione, all'analisi della normativa di settore e agli approfondimenti sulle nuove tecnologie emergenti

Per ricevere supporto in caso di incidente cyber



certfin.it
info@certfin.it

