

TOR VERGATA
UNIVERSITÀ
DEGLI STUDI
DI ROMA

III CONFERENZA NAZIONALE

GT 5.0 1

Partnership
cybersecurity
privacy

**Cybersecurity nelle Infrastrutture critiche:
tipologie di rischio e risposte di sistema**

«Competenze digitali per la Protezione dei Dati, la Cybersecurity e la Privacy»

20 GENNAIO 2020
ore 9.00 – 13.30 14.30 - 18.15
ROMA
Università degli Studi di Roma "Tor Vergata", Facoltà di Economia
Via Columbia 2, Sala del Consiglio, 2° Piano



CERT Finanziario Italiano

La gestione del rischio nelle Infrastrutture critiche: tra norme e compliance

Romano Stasi
Segretario Generale Consorzio ABI Lab
Direttore Operativo CERTFin

TLP GREEN

Principale contesto di riferimento normativo per il settore finanziario

A partire dalle prime iniziative che già nel 2008 avevano avviato l'attività di **mappatura delle infrastrutture critiche**, molteplici sono state le normative che hanno impattato il settore finanziario, in particolare:



DIRETTIVA NIS



CIRCOLARE 285



DIRETTIVA PSD2

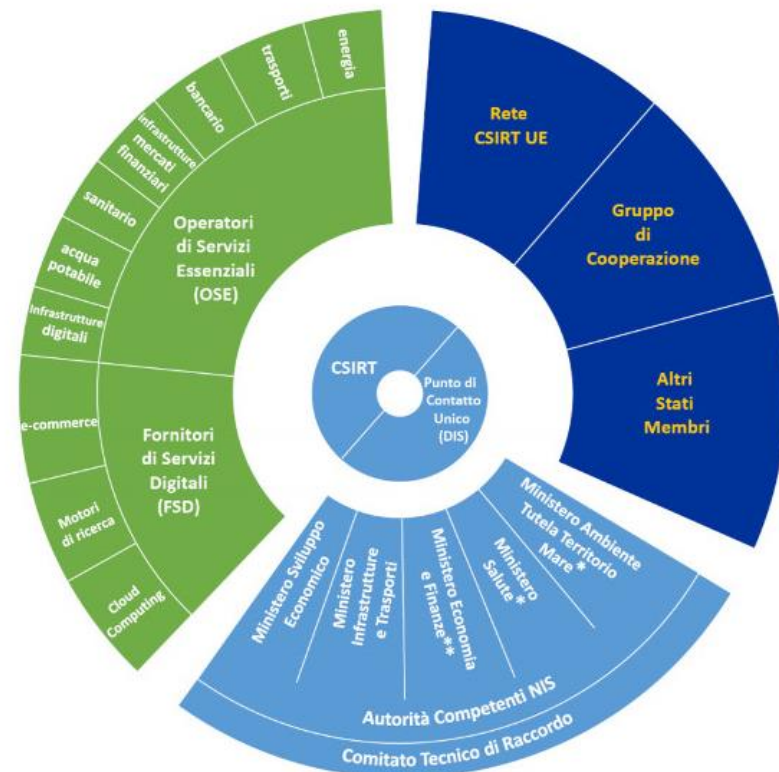


REGOLAMENTO GDPR

La Direttiva NIS: le tappe principali e gli attori coinvolti

- 01/2013 → **Decreto Monti**
- 12/2013 → Adozione del primo **Quadro Strategico Nazionale** e del **Piano Nazionale**
- 2014 → Avvio operatività **CERT-PA**
- 11/2014 → Avvio operatività **CERT nazionale**
- 07/2016 → **Direttiva NIS**
- 02/2017 → **Decreto Gentiloni**
- 05/2017 → **Aggiornamento del Piano Nazionale** per la sicurezza cibernetica
- 02/2018 → **Schema di decreto legislativo** di attuazione della Direttiva NIS
- 9/05/2018 → **Applicazione** Direttiva NIS
- 9/06/2018 → Pubblicazione in GU del **D.Lgs 65/2018**
- 24/06/2018 → Entrata in vigore del **D.Lgs 65/2018**
- 12/2018 → Identificazione **Operatori di Servizi Essenziali (OSE)**
- 07/2019 → Diffusione **Linee Guida** per gli OSE

- 09/2019 → Emanazione **D.L. 105 del 21 settembre 2019 («Decreto cybersecurity»)** sul perimetro di sicurezza cibernetica
- 11/2019 → Emanazione **Legge 133 del 18 novembre 2019**, che converte in legge il D.L. 105



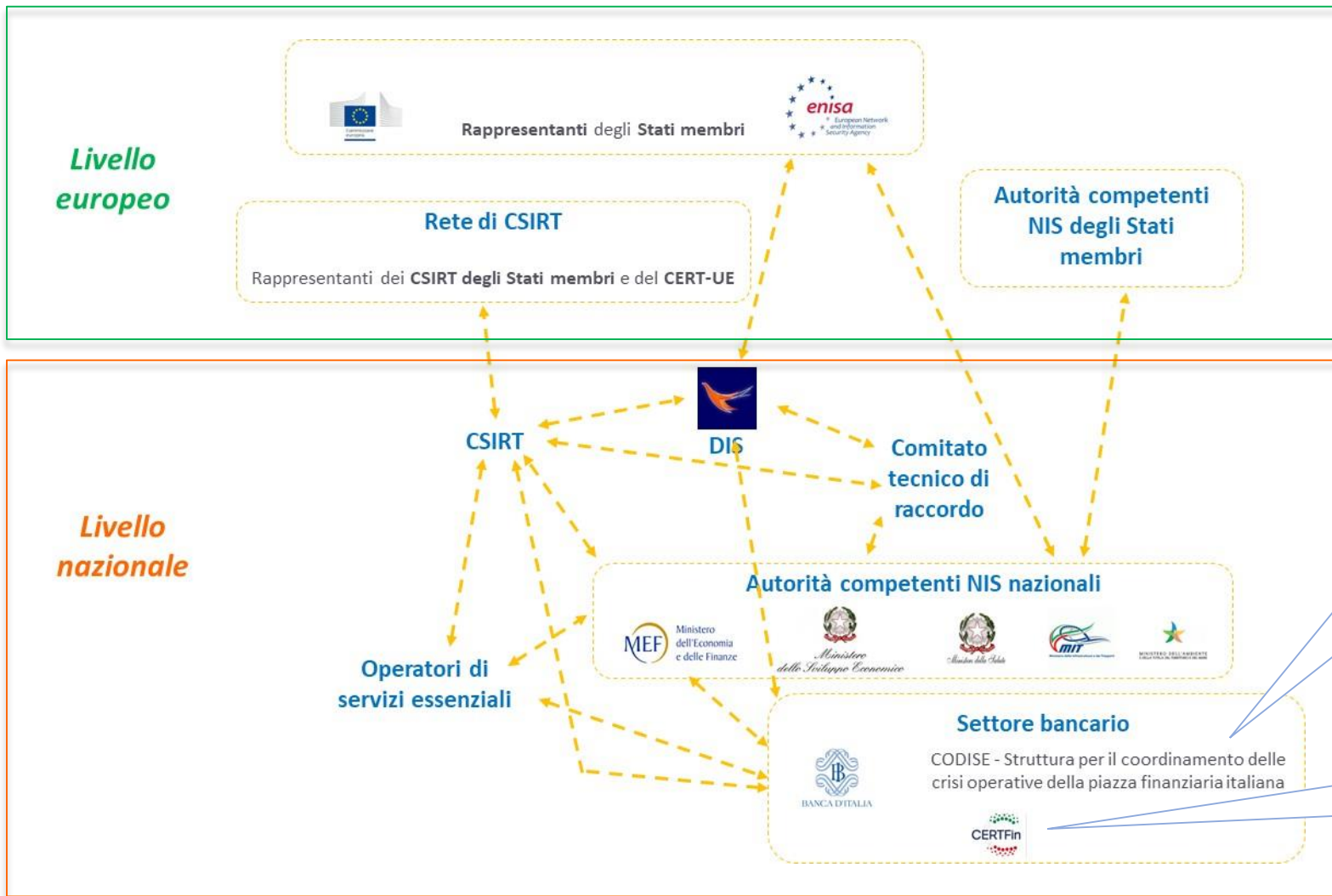
L'Italia si è dotata di una **robusta governance di cybersecurity**, che vede coinvolti sia il settore pubblico che quello privato.

- Servizi interessati
- Attori governativi NIS
- Meccanismi della cooperazione europea

* più regioni e province autonome di Trento e di Bolzano

** in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob

I principali attori della governance cibernetica definiti dallo schema di decreto



Mappatura e coordinamento delle infrastrutture critiche già dal 2008

Dal 2017 attivazione del CERT Finanziario Italiano

Flussi di comunicazione

Principali novità apportate dalla 285 in ambito continuità operativa

La circolare 285 di Banca d'Italia tratta alcune **tematiche specifiche di continuità operativa**, in particolar modo per quanto riguarda:

ESTERNALIZZAZIONI



La normativa vigente prescrive specificatamente di:

- formalizzare i **livelli di servizio assicurati** e le soluzioni di BC conformi alla Bdl;
- stabilire le **modalità di partecipazione alle verifiche dei BCP dei fornitori**;
- contemplare **fornitori alternativi d'emergenza**;
- **stabilire cautele contrattuali** per evitare il rischio di fallimento delle prestazioni in caso di polipsonio.

PROCESSI A RILEVANZA SISTEMICA



Vengono identificati requisiti particolari per questi processi:

- il tempo di **ripristino** non può superare le **4 ore**;
- il tempo di **ripartenza** non può superare le **2 ore**;
- se un evento catastrofico colpisce un Operatore A, causando il blocco dei processi a rilevanza sistemica di un Operatore B, questi ripristina i propri processi sistemici **entro 2 ore** dalla ripartenza dell'Operatore A;
- per quanto riguarda problemi molto gravi, la Banca d'Italia, sentito il CODISE, si riserva la facoltà di adattare i presenti requisiti di ripristino e di darne comunicazione all'operatore.

INCIDENTI DI SICUREZZA INFORMATICA ED ALTRI INCIDENTI



- Vengono previste delle procedure per la **dichiarazione dello stato di crisi** in raccordo con il processo di gestione degli incidenti di sicurezza informatica e altre tipologie di incidente;
- **Devono essere formalizzati** dei processi coordinati o integrati di *incident e crisis management*.

COMUNICAZIONE ALLE AUTORITÀ



- In caso di crisi, successivamente al ripristino dei processi critici, **l'operatore fornisce alla Banca d'Italia e alla BCE valutazioni circa l'impatto dell'evento sull'operatività delle strutture centrali e periferiche e sui rapporti con la clientela e le controparti**;
- In caso di incidenti che possano avere impatti rilevanti sui processi a rilevanza sistemica, la dichiarazione dello stato di crisi prevede l'**immediata richiesta di attivazione del CODISE**.

La Circolare 285 rappresenta il **veicolo normativo** attraverso cui vengono aggiornati tutti i **requisiti di sicurezza** definiti anche dalle normative internazionali.

PSD2 e GDPR: «apertura» vs «difesa»

La direttiva Europea PSD2 «L'APERTURA»



- Rappresenta il punto di partenza all'**apertura** dell'ecosistema bancario;
- **Promuove lo sviluppo di un mercato sempre più aperto, efficiente, innovativo, competitivo e sicuro;**
- **Favorisce la standardizzazione,** introducendo più efficaci meccanismi di scambio e trasferimento di informazioni tra i vari attori coinvolti.



Il regolamento generale sulla protezione dei dati GDPR «LA DIFESA»



- Mira a **rafforzare i meccanismi di difesa e tutela dei dati personali degli individui,** mettendo al centro i diritti e le libertà dei cittadini;
- Stimola i **presidi di governo e sviluppare una nuova visione strutturata sui rischi e sugli impatti.**

GDPR: snodi chiave per l'applicazione e ipotesi di action plan

DATA PROTECTION E DATA GOVERNANCE

La Data Protection rappresenta una prospettiva ortogonale alla Data Governance

ACCOUNTABILITY, PRIVACY BY DESIGN E PRIVACY BY DEFAULT

Substrato su cui poggiano le logiche implementative della Data Protection



SICUREZZA E PROTEZIONE DEI DATI

Sviluppo di un approccio basato sulla valutazione dei rischi e degli impatti

IMPOSTAZIONE DEL MODELLO DEI RUOLI

Equilibrio tra le esigenze di segregation of duties sinergia organizzativa

REGISTRO DEI TRATTAMENTI COME PONTE DATI - PROCESSI

Da adempimento normativo a strumento di gestione, comprensione e auto analisi



Il settore bancario italiano si è attivato per la definizione di **linee guida per l'applicazione del GDPR** e per l'identificazione di un **percorso specifico di implementazione tecnologica**, come strumenti di supporto per le iniziative delle banche.

Proliferano le normative che disciplinano la gestione degli incidenti, prevedendo **diversi livelli e modalità di reporting** a regolatori differenti

- Guidelines on major incident reporting
- Framework Bdl – SSM Istituti Significant
- Framework Bdl Istituti Less Significant
- GDPR
- Direttiva NIS

È necessario **presidiare nel continuo le evoluzioni normative** che impattano su ambiti che si intersecano tra loro, al fine di **individuare eventuali sinergie** che possano portare a **benefici in termini di costi e di effort**.



È utile promuovere la segnalazione degli incidenti alle diverse autorità cogliendo **l'opportunità di standardizzare i requisiti di reporting**.

Accrescere la collaborazione operativa sui temi cyber nel settore bancario: il CERTFin

Come **coordinamento** centrale delle attività di contrasto e prevenzione, il 1° gennaio 2017 è stato avviato il **CERTFin**, un'**iniziativa cooperativa pubblico-privata** finalizzata a innalzare la **capacità di gestione dei rischi cyber** degli operatori bancari e finanziari e la **cyber resilience** del sistema finanziario italiano.



OBIETTIVI

DIFFONDERE LE COMPETENZE CYBER E FARE AWARENESS

- Approfondire **contenuti e impatti** delle **normative** di riferimento sul tema della **cybersecurity**
- Sviluppare **campagne di sensibilizzazione** sulla cybersecurity
- Svolgere **esercitazioni e simulazioni su scenari cyber**

SVILUPPARE ULTERIORMENTE UNA LOGICA DI ISAC ITALIANO

- **Incrementare l'info-sharing** su minacce/vulnerabilità/ incidenti
- Svolgere **analisi evolutive** delle **minacce cyber**
- Monitorare l'evoluzione dei **rischi** emergenti e gli **impatti** per il settore finanziario

COORDINARE LE EMERGENZE E GLI INCIDENTI INFORMATICI

- **Svolgere attività di coordinamento** centrale in caso di **incidente**
- **Supportare operativamente** le strutture di presidio delle **singole realtà**
- **Definire e aggiornare** a livello di settore lessons learned e strategie di risposta

CERTFin – Mission

- Facilitare lo **scambio tempestivo di informazioni** tra gli operatori del settore su potenziali minacce informatiche



- Costituire il **punto di contatto** privilegiato del settore finanziario con l'architettura istituzionale per la protezione cibernetica e la sicurezza informatica

- **Facilitare** la risposta ad incidenti informatici su larga scala



- **Supportare** il processo di gestione di crisi cibernetica

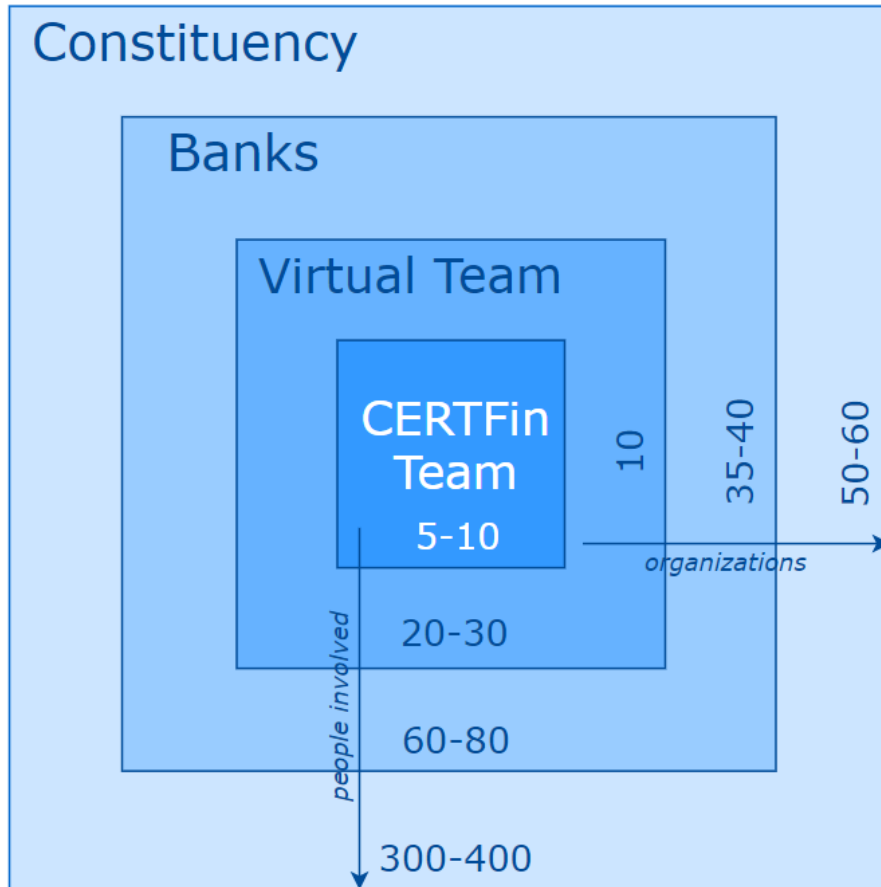
- **Cooperare** con analoghe istituzioni nazionali e internazionali e con altri attori pubblici e privati coinvolti nella cyber security



- **Accrescere la consapevolezza** e la cultura della sicurezza

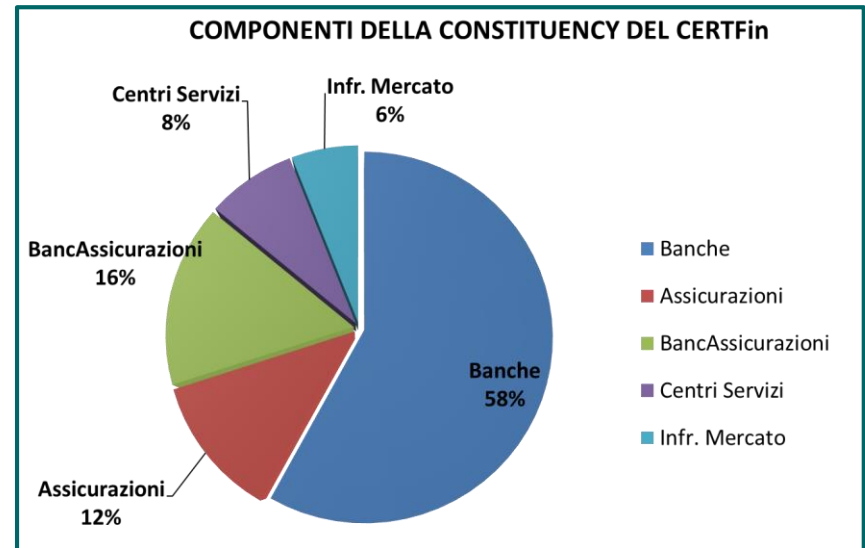
La Constituency del CERTFin

Sin dall'avvio del CERTFin è stato condotta un'intensa attività di sviluppo della Constituency che ha permesso di raggiungere, ad oggi, **50 aderenti**.



Composizione della Constituency:

- 29 Banche
- 6 Imprese Assicuratrici
- 8 BancAssicurazioni
- 4 Centri Servizi
- 3 Operatori di Infrastrutture di mercato



Oltre alla collaborazione tra i diversi attori del sistema finanziario, è necessario **incrementare l'awareness della clientela** verso i rischi cyber.

Le attività del CERTFin

I FILONI DI ATTIVITA'

FINANCIAL INFO SHARING AND ANALYSIS CENTER (FinISAC)



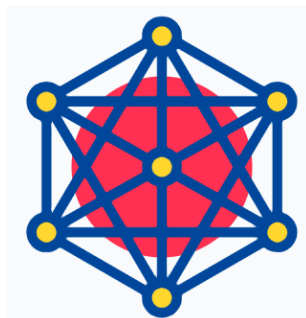
CYBER KNOWLEDGE AND SECURITY AWARENESS



CENTRALE OPERATIVA DI GESTIONE DELLE EMERGENZE CYBER



THREAT INTELLIGENCE AND LANDSCAPE SCENARIO



AWARENESS



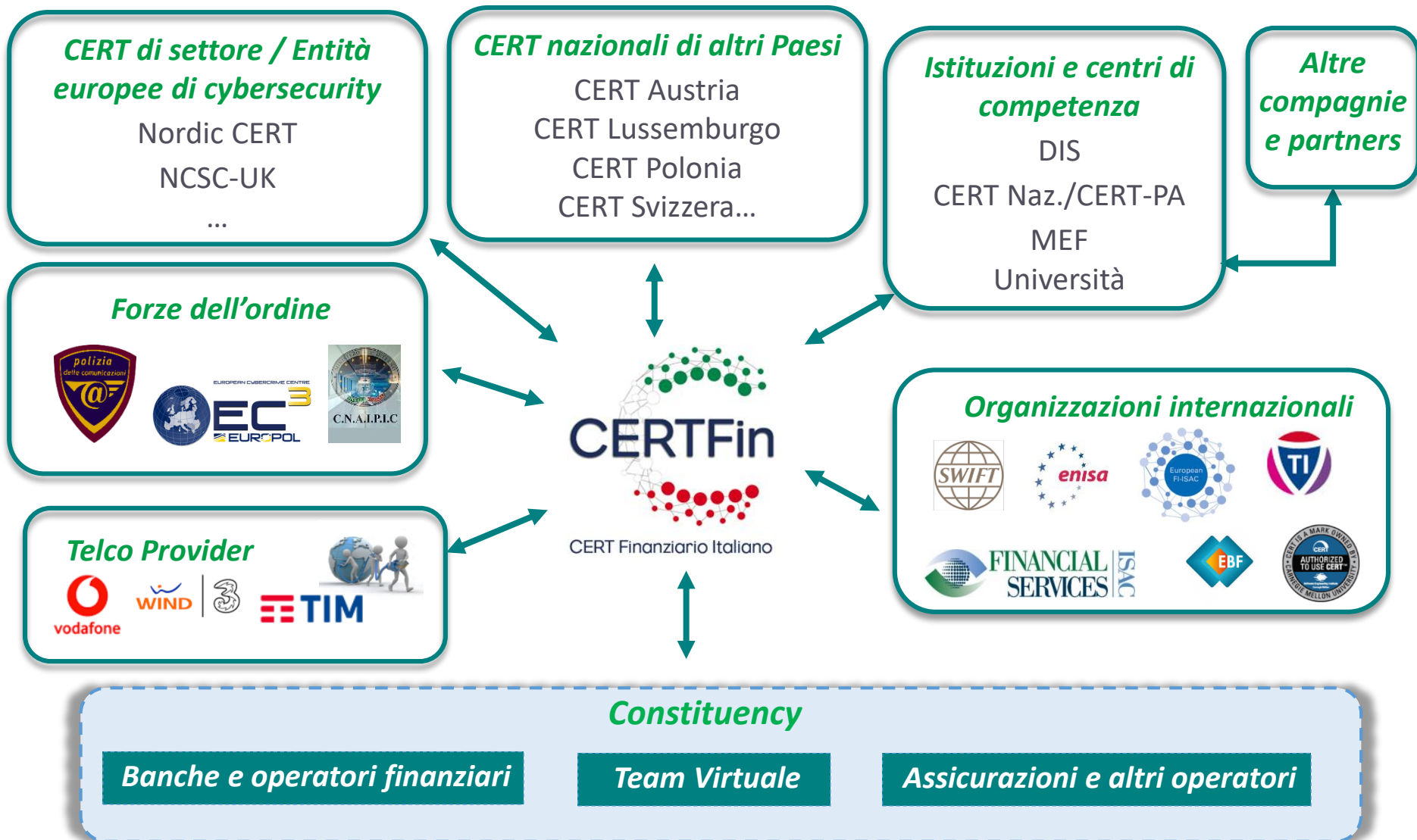
PROGETTI EUROPEI



10 partecipanti al Team Virtuale

Le attività di Info-Sharing

La rete del CERTFin



Le attività di Info-Sharing











La piattaforma MISP

La **Malware Information Sharing Platform (MISP)**, è una piattaforma *open source* sviluppata dal CERT del Lussemburgo, che permette agli utenti di **ricevere informazioni sugli attacchi e sui fenomeni fraudolenti** in maniera strutturata in formato machine readable (STIX)

Events

< previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 next >

Q My Events Org Events

Published	Source org	Member org	Id	Clusters	Tags	#Attr.	Email	Date	Threat Level	Analysis	Info
<input checked="" type="checkbox"/>	D.		10011		family:kelihos fp:green	36	feed_user@deloitte.es	2018-02-26	High	Completed	Daily IOCs for family kelihos
<input checked="" type="checkbox"/>	D.		10009		family:frethog fp:green	11	feed_user@deloitte.es	2018-02-26	High	Completed	Daily IOCs for family frethog
<input checked="" type="checkbox"/>	D.		10010		family:mofin fp:green	81	feed_user@deloitte.es	2018-02-26	High	Completed	Daily IOCs for family mofin
<input checked="" type="checkbox"/>	D.		10008		family:emotet fp:green	385	feed_user@deloitte.es	2018-02-26	High	Completed	Daily IOCs for family emotet
<input checked="" type="checkbox"/>	D.		10006		family:wonton fp:green	3	feed_user@deloitte.es	2018-02-26	High	Completed	Daily IOCs for family wonton
<input checked="" type="checkbox"/>	D.		10007		family:holbar fp:green	99	feed_user@deloitte.es	2018-02-26	High	Completed	Daily IOCs for family holbar
<input checked="" type="checkbox"/>	D.		10004		family:magniber fp:green	21	feed_user@deloitte.es	2018-02-26	High	Completed	Daily IOCs for family magniber
<input checked="" type="checkbox"/>	D.		10005		family:tovus fp:green	12	feed_user@deloitte.es	2018-02-26	High	Completed	Daily IOCs for family tovus
<input checked="" type="checkbox"/>	D.		10002		family:famadin fp:green	3	feed_user@deloitte.es	2018-02-26	High	Completed	Daily IOCs for family famadin
<input checked="" type="checkbox"/>	D.		10003		family:podjot fp:green	36	feed_user@deloitte.es	2018-02-26	High	Completed	Daily IOCs for family podjot

Accresce il **tempestivo e costante scambio di informazioni**, utile per **rilevare, prevenire e contrastare eventi** che impattano l'integrità, la disponibilità e la riservatezza delle informazioni.

Dall'inizio delle attività del CERTFin, sono stati condivisi oltre 8 milioni di IoC
A partire dal 1° gennaio 2020, le segnalazioni di attacchi cyber o frodi informatiche, avviene solo attraverso la piattaforma MISP

Resoconto attività CERTFin gen – dic 2019

Information Sharing – FinISAC (1/2)

SINTESI OPERATIVITÀ

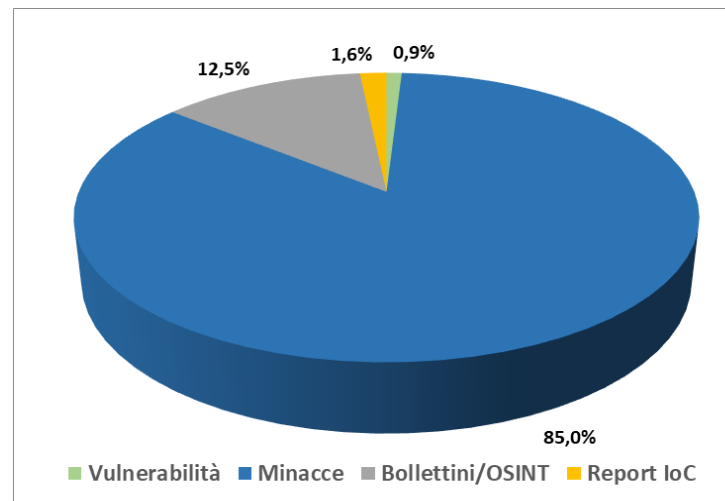
Inviati alert relativi a **858 differenti fenomeni**, che considerando anche eventuali approfondimenti/update sono pari a oltre **1200 segnalazioni**

Inviare **82 segnalazioni a singole banche su minacce, possibili compromissioni o specifiche vulnerabilità sulla rete**

Monitorate **74 segnalazioni a singole organizzazioni su specifiche vulnerabilità sulla rete**

Interessati oltre **99.302 destinatari**

TIPOLOGIE SEGNALAZIONI



RELAZIONI CON LA CONSTITUENCY E CON GLI STAKEHOLDER

15 sessioni di approfondimento con il Team Virtuale

Confronto e **condivisione principali fenomeni** con CNAIPIC, Telco Provider e CERT Nazionale

VOLUME FONTI IN ENTRATA

- **107 OSINT** - Bollettini informativi
- **12 Report IoC**
- **Inviati 350 alert** provenienti
- dalla Constituency del CERTFin
- **Analizzate 6.700 segnalazioni** di network europei/internazionali

Resoconto attività CERTFin gen – dic 2019

Information Sharing – FinISAC (2/2)

PRINCIPALI FENOMENI ANALIZZATI DAL CERTFin – periodo gennaio/settembre

Frodi informatiche

- Tentativi di frode attraverso false PEC di banche
- Fenomeni di SIM swap
- Campagne di phishing
- Oltre 390 money mule segnalati

Attacchi a dati/informazioni

- CEO Fraud (spoofing mail sender)
- Campagne malware ai danni di Banca d'Italia
- Compromissione account di internet banking dei clienti – Ursnif
- Attività malevola di scansione rete
- Variante Mirai per settore finanziario
- Campagne Trickbot
- Campagne Cobalt

Attacchi alla disponibilità di servizi/asset IT

- Minacce Ransom DDoS
- Attacchi DDoS

LESSONS LEARNED

Frodi informatiche

- Esigenza di rafforzare le azioni di contrasto e prevenzione con i Telco provider e fornitori di PEC
- Continuo monitoraggio transazioni anomale

Attacchi a dati e informazioni

- Aumento della frequenza del processo di aggiornamento SW
- Rafforzamento training / awareness su tematiche di cybersecurity, anche verso top management e loro staff
- Proseguimento delle campagne di sensibilizzazione verso la clientela

Attacchi alla disponibilità

- Monitoraggio continuo di vulnerabilità tecnologiche
- Predisposizione piani di response/mitigazione dei DDoS con i Carrier

Oltre la compliance: l'importanza della collaborazione intersettoriale e internazionale



Le normative di riferimento hanno introdotto **nuove regole** in un **ecosistema complesso e interdipendente**, in cui operano **nuovi attori**.

Accanto alla condivisione delle informazioni all'interno del settore è necessario **fare leva sulle interconnessioni operative di sicurezza** per accrescere la collaborazione intersettoriale.



Le autorità internazionali potrebbero **rafforzare le relazioni** tra i singoli Paesi, con l'obiettivo di **creare una rete di scambio proficuo di diverse esperienze** nell'ambito della sicurezza informatica e ridurre i rischi ad essa associati.