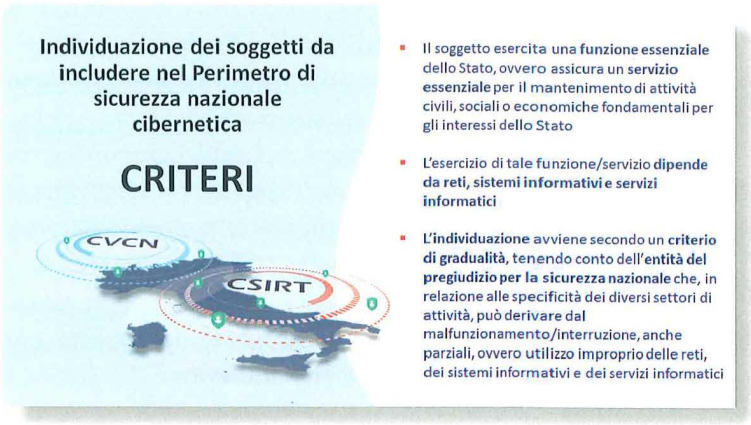
n. 124/2007 – viene allegato alla Relazione sulla politica dell'informazione per la sicurezza, riferita al 2020.

EVOLUZIONE DELLE POLICY CYBER A LIVELLO NAZIONALE E INTERNAZIONALE

L'attuazione del Perimetro di sicurezza nazionale cibernetica

L'iniziativa, promossa dal Comparto, che meglio rappresenta gli sforzi profusi dal Paese sotto il profilo delle policy cyber, è sicuramente quella del "Perimetro di sicurezza nazionale cibernetica". Si tratta di un provvedimento che, è bene ricordare, prevede – per la prima volta – oltre a obblighi quali il rispetto di stringenti misure di sicurezza e la notifica degli incidenti, anche specifiche disposizioni in materia di forniture di beni, sistemi e servizi ICT, appartenenti a determinate categorie, destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici utilizzati dai soggetti inclusi nel Perimetro per l'esercizio della funzione/servizio essenziale per la sicurezza nazionale ("beni ICT perimetro").



OBBLIGHI IN CAPO AI SOGGETTI PERIMETRO

- Notifica degli incidenti aventi impatto sui "beni ICT perimetro", così da assicurare un immediato flusso di informazioni a favore delle strutture deputate alla prevenzione, preparazione e gestione degli eventi cibernetici (in particolare NSC e CSIRT, entrambi incardinati nel DIS).
- Adozione di misure di sicurezza per i "beni ICT perimetro" relative a organizzazione, processi e procedure, anche in relazione al procurement ICT.
- Screening tecnologico degli approvvigionamenti ICT appartenenti a categorie specifiche, destinati ai "beni ICT perimetro". La procedura prevede che il soggetto che intenda procedere a tali acquisizioni ne dia comunicazione al Centro di Valutazione e Certificazione Nazionale (CVCN, operante presso il Ministero dello Sviluppo Economico) che, entro un massimo di 60 giorni, può effettuare verifiche preliminari ed imporre condizioni e test di hardware e software (questi ultimi devono essere conclusi nel termine di ulteriori 60 giorni). Tali attività sono svolte dai Centri di Valutazione (CV) dei Ministeri dell'Interno e della Difesa – in stretta sinergia con il CVCN – per le forniture di beni, sistemi e servizi ICT da impiegare sulle rispettive reti, sistemi e servizi informatici.

Al riguardo, se il 2019 è stato caratterizzato dalla definizione dell'atto normativo e dal relativo iter parlamentare che ha condotto alla sua adozione, il 2020 si è connotato per l'elaborazione dei relativi decreti attuativi. Nel novembre 2019 il Comitato Interministeriale per la Sicurezza della Repubblica (CISR) aveva infatti assegnato al Comparto Intelligence il ruolo di coordinare l'implementazione del Perimetro, attraverso la costituzione di 6 gruppi di lavoro e relativi sottogruppi. Ciò ha portato, a seguito di una complessa e articolata attività di coordinamento interministeriale, con il determinante apporto del Dipartimento per gli Affari Giuridici e Legislativi della Presidenza del Consiglio, concretizzatasi in oltre 150 riunioni nell'arco del 2020: all'adozione del DPCM n. 131/2020 per la definizione dei criteri per l'identificazione dei soggetti da includere nel Perimetro e di quelli per l'individuazione dei relativi "beni ICT perimetro"; alla predisposizione del DPCM (in fase avanzata di approvazione) per la definizione delle modalità di notifica degli incidenti e delle misure di sicurezza, comprese quelle sul procurement ICT; all'elaborazione del Regolamento – approvato in via definitiva dal Consiglio dei Ministri il 29 gennaio 2021 – relativo alle ispezioni e alle modalità di scrutinio tecnologico da parte del Centro di Valutazione e Certificazione Nazionale (CVCN) e dei CV; alla stesura del DPCM contenente le categorie di prodotti ICT da sottoporre alle valutazioni del CVCN e dei CV in fase di procurement da parte dei soggetti perimetro, esaminato dal CISR a fine novembre 2020; alla definizione del DPCM relativo all'accreditamento e ai raccordi tra CVCN, CV e laboratori.

Nel citato DPCM n. 131/2020, in attuazione del criterio di gradualità contemplato dal D.L. n. 105/2019, sono stati definiti 11 settori di attività, all'interno dei quali devono essere poi individuati i soggetti da includere nel Perimetro. Il 25 novembre 2020, su proposta del CISR, previa indicazione da parte delle Amministrazioni competenti, è stato, pertanto, adottato dal Presidente del Consiglio dei Ministri l'atto – non soggetto a pubblicazione e per il quale è escluso il diritto di accesso – contenente l'elencazione dei soggetti inclusi nel Perimetro ai quali, come previsto, il DIS ha dato la relativa comunicazione, il 22 dicembre. Alla luce di quanto descritto, da giugno 2021 inizierà, quindi, l'operatività del "sistema Perimetro", specie in materia di notifiche di incidenti cibernetici.

L'implementazione della Direttiva NIS

Il DIS, in veste di punto di contatto unico NIS, ha assicurato gli opportuni raccordi con le Autorità competenti NIS, attraverso riunioni plenarie bimestrali

e costanti interazioni bilaterali. In queste occasioni sono state oggetto di esame tanto l'attuazione della Direttiva NIS in Italia (ad esempio per quel che concerne la definizione delle attività di ispezione e di verifica, nonché il livello di maturità raggiunto dagli operatori di servizi essenziali-OSE nell'applicazione delle misure di sicurezza), quanto le iniziative europee in materia, in particolare nell'ambito del Gruppo di Cooperazione NIS (NISCG), in cui i Paesi Membri si confrontano su aspetti concernenti l'implementazione della Direttiva. In questo contesto, sono state, altresì, assicurate sinergie con l'Ufficio del Consigliere Militare del Presidente del Consiglio dei Ministri, punto di contatto italiano del programma europeo di protezione delle infrastrutture critiche, nelle attività propedeutiche alla revisione della Direttiva UE 114/2008 sulle Infrastrutture Critiche Europee (ICE), al fine di garantire l'armonizzazione delle due normative, evitando in tal modo eventuali accresciuti oneri per gli operatori. Analogamente, di stretta intesa con il Ministero dell'Economia e delle Finanze, si è proceduto rispetto all'avvio delle negoziazioni a livello UE relative alla proposta di Regolamento sulla resilienza operativa digitale per il settore finanziario ("DORA").

Il DIS partecipa in rappresentanza del nostro Paese alle attività del NISCG, nel cui ambito nel corso dell'anno è stato, tra l'altro, affrontato l'avvio del processo di revisione della Direttiva NIS (la cd. NIS 2), rispetto alla quale, operando in stretto coordinamento con le Autorità NIS italiane, sono state presentate delle proposte volte ad incrementarne l'efficacia.

Autorità competenti NIS nazionali	Ambito di competenza
Ministero dello Sviluppo Economico	Settore energia
	Settore delle infrastrutture digitali
	Servizi digitali
Ministero delle Infrastrutture e dei Trasporti	Settore trasporti
Ministero dell'Economia e delle Finanze in collaborazione con Banca d'Italia e Consob	Settore bancario
	Settore infrastrutture dei mercati finanziari
Ministero della Salute, Regioni e Province autonome di Trento e di Bolzano (direttamente o per il tramite delle Autorità sanitarie territorialmente competenti)	Settore sanitario
Ministero dell'Ambiente e della Tutela del territorio e del mare, Regioni e Province autonome di Trento e di Bolzano (direttamente o per il tramite delle Autorità territorialmente competenti)	Settore fornitura e distribuzione di acqua potabile

Il NISCG, sulla base del programma biennale di lavoro, attiva dei gruppi di lavoro (Work Stream) dedicati all'approfondimento di specifiche tematiche (seguiti direttamente dal DIS), ovvero concernenti i settori di attività sottoposti alla Direttiva NIS (ai quali partecipano le Autorità competenti NIS nazionali, in stretta intesa con il DIS).

Work Stream NIS Cooperation Group

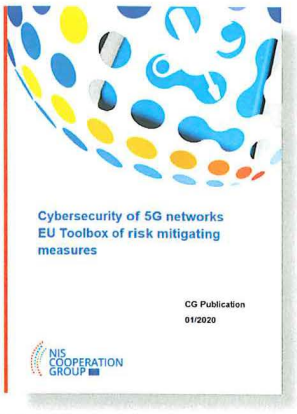
OGGETTO	AMMINISTRAZIONE NAZIONALE COINVOLTA	OBIETTIVI
Gestione incidenti e crisi cibernetiche su vasta scala a livello UE	DIS (co-leader)	Definizione e implementazione del progetto Cyber Crisis Liaison Organisation Network (CyCLONe) e delle relative procedure di funzionamento. 29 settembre 2020 lancio di CyCLONe
5G	DIS (co-leader) e Min. dello Sviluppo Economico	Implementazione della Raccomandazione della Commissione 2019/534 in materia di sicurezza cibernetica delle reti 5G. Predisposizione e implementazione del Toolbox europeo e stesura dei relativi report di attuazione
Misure di sicurezza per gli operatori di servizi essenziali	DIS	Aggiornamento delle linee guida sulle misure di sicurezza per gli operatori di servizi essenziali
Notifiche di incidente	DIS	Revisione del meccanismo di notifica degli incidenti NIS e predisposizione Annual Summary Report
Fornitori di Servizi Digitali	Min. Sviluppo Economico	Attività di implementazione della Direttiva NIS negli specifici settori e armonizzazione con le normative settoriali Condivisione di casi d'uso e best practice di cybersecurity Raffinamento dei criteri e delle soglie per la notifica degli incidenti e per l'identificazione degli operatori di servizi essenziali
Settore energetico		
Settore infrastrutture digitali		
Settore sanitario	Min. Salute	
Sotto-settore trasporto aereo - Aviazione civile	Min. Infrastrutture e Trasporti	

In particolare, é stata assunta la guida dei Work Stream su:

- "Gestione di incidenti e crisi cibernetiche su vasta scala a livello UE", in raccordo con l'Agenzia francese per la sicurezza dei sistemi informatici (ANSSI), nel cui contesto è stato definito il progetto Cyber Crisis Liaison Organisation Network (CyCLONe) di gestione degli incidenti e delle crisi cibernetiche su larga scala di cui alla Raccomandazione della Commissione 2017/1584 (cd. Blueprint);
- 5G, insieme a Belgio, Estonia, Francia, Olanda, Repubblica Ceca e Svezia, coadiuvati dalle Presidenze di turno del Consiglio dell'UE, per l'implementazione della Raccomandazione della Commissione 2019/534 in materia di sicurezza cibernetica delle reti 5G.

Nel NISCG è stata anche effettuata una disamina dei rischi cyber correlati alla pandemia e alle applicazioni di tracciamento dei contatti dei cittadini con soggetti risultati positivi al Covid-19 adottate dai diversi Stati Membri, al fine di assicurarne l'interoperabilità, la sicurezza cibernetica, nonché la protezione dei dati personali trattati.

Sviluppo delle reti di nuova generazione (5G)



Costante è stata, al riguardo, l'attenzione della Commissione europea rispetto alla sicurezza delle reti 5G degli Stati Membri. In tale ambito, in continuità con le iniziative avviate con la citata Raccomandazione del 26 marzo 2019, il NISCG ha adottato il Toolbox delle misure di sicurezza, pubblicato il 29 gennaio 2020.

Di concerto con il Ministero dello Sviluppo Economico (MiSE), sin dalle fasi preparatorie, sono stati forniti contributi determinanti alla stesura del documento. Il Toolbox contiene una serie di misure strategiche e tecniche, nonché azioni di supporto destinate, su base volontaria, agli Stati Membri al fine di promuovere un approccio armonizzato alla sicurezza delle reti 5G. Al riguardo, l'Italia non si è limitata ad uniformarsi alle citate linee guida, ma le ha recepite all'interno dell'ordinamento giuridico nazionale. Attraverso il cd. Decreto liquidità (D.L. n. 23/2020, convertito dalla legge n. 40/2020), la disciplina sul Golden Power (D.L. n. 21/2012 convertito, con modificazioni, dalla legge n. 56/2012) è stata, infatti, emendata prevedendo un richiamo alle linee guida europee, e quindi al Toolbox, quale riferimento per il processo istruttorio delle notifiche relative all'acquisto di tecnologia 5G da fornitori extra-europei.

Tale aspetto è stato evidenziato nel Report sull'implementazione del Toolbox da parte degli Stati Membri, pubblicato nell'ottobre 2020, nel quale l'Italia è stata citata quale esempio, insieme a pochi altri Paesi. In particolare, con rife-

rimento alla misura relativa alle restrizioni nei confronti dei fornitori "ad alto rischio", l'attuale impianto normativo (Golden Power, Perimetro di sicurezza nazionale cibernetica e Decreto MiSE del 12 dicembre 2018, cd. Decreto Telco) consente al nostro Paese di monitorare i contratti stipulati con fornitori extra-europei e, con il perfezionamento dei decreti attuativi del Perimetro, affiderà al CVCN il compito di condurre le opportune verifiche tecniche sulla presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano. Per quel che concerne, poi, la misura di cui al Toolbox sulla diversificazione dei fornitori di sistemi 5G, è stata in particolare richiamata l'applicazione della normativa sul Golden Power a casi specifici in cui, tra le prescrizioni imposte agli operatori, vi è quella relativa all'elaborazione di un piano di diversificazione delle piattaforme tecnologiche della componente "core" della rete 5G.

Sul fronte nazionale è, inoltre, proseguito lo sviluppo delle reti 5G italiane. Al riguardo, l'attenzione del Comparto Intelligence resta alta in merito ai profili di rischio che derivano dai nuovi scenari tecnologici, specie con l'avvento delle reti core 5G in configurazione Stand Alone, che, tramite l'attivazione delle funzioni più avanzate, come la suddivisione logica di risorse di rete fisiche (cd. network slicing), e lo spostamento delle infrastrutture di calcolo verso l'utente finale (cd. edge computing), abiliteranno applicazioni innovative quali le comunicazioni mobili a banda ultra larga, realtà aumentata, veicoli a guida autonoma, chirurgia da remoto, reti di sensori e smart cities e automazione industriale di nuova generazione.

Nel settore delle reti di accesso radio (RAN), il Comparto segue con particolare interesse lo sviluppo di architetture basate su tecnologie aperte, quali l'iniziativa Open RAN, uno standard industriale che definisce i componenti della parte radio e come comunicano tra loro, per favorire una maggiore trasparenza e una diversificazione dei fornitori.

Ulteriori attività in ambito internazionale

Il nostro Paese è coinvolto, specie con riguardo ai negoziati di documenti di policy e atti normativi, in ambito ONU, OSCE, UE, NATO, G7 e G20. Il DIS, in costante raccordo con il Ministero degli Affari Esteri e della Cooperazione Internazionale (MAECI), ha assicurato nel corso dell'anno la propria partecipazione a più di cento riunioni a livello multilaterale, dapprima in presenza poi, in ragione della pandemia, in videoconferenza. Al fine, poi, di definire una posizione nazionale condivisa e in grado di tutelare gli interessi dell'Italia, il Dipartimento ha continuato ad attuare, per i profili di diretta competenza, uno stretto coordinamento, oltre che con la Farnesina, con i Dicasteri interessati, in particolare, la Difesa (per i dossier NATO) e il MiSE (specie per i lavori dell'ITU, inclusa la predisposizione del relativo Global Cybersecurity Index).

In sede OSCE, invece, il DIS ha affiancato il MAECI nella conduzione del

periodico Communication Check, organizzato dal Segretariato di quell'organizzazione per accrescere il livello di prontezza dei punti di contatto degli Stati partecipanti, nonché nei costanti aggiornamenti sullo stato di implementazione delle misure di confidence building, volte a prevenire l'insorgenza di possibili conflitti derivanti dall'impiego delle tecnologie ICT.

Di tutto rilievo, inoltre, sono le attività svolte in ambito UE per definire una posizione comune dell'Unione da riversare nei lavori dell'Open Ended Working Group (OEWG) dell'ONU sulle questioni cyber, con l'obiettivo di fornire pieno sostegno ai risultati già conseguiti in materia, in particolare in seno allo UN Group of Governmental Experts (UN GGE), specie con riguardo all'applicabilità delle norme di diritto internazionale alle condotte degli Stati nello spazio cibernetico.

Sempre per quel che concerne gli sforzi profusi dall'UE per rafforzare la resilienza ad attacchi cyber, il DIS ha contribuito, per la parte di competenza, al negoziato, avviato nel 2018 e giunto a termine nel dicembre 2020, della "proposta di Regolamento per la creazione di un Centro di competenza europeo per lo sviluppo industriale, tecnologico e della ricerca in materia di cybersecurity e della rete dei Centri di coordinamento nazionali"(vds. più avanti, riquadro di pag. 24), volta a promuovere la sovranità tecnologica e la leadership dell'UE (e dei suoi Stati Membri) e, conseguentemente, ad accrescerne l'autonomia strategica nel settore e la competitività industriale.

Nell'ambito dei tavoli europei un contributo è stato, altresì, fornito con riguardo a ruolo e funzioni che la futura Joint Cyber Unit – a suo tempo annunciata dal Presidente della Commissione europea von der Leyen e parte integrante della "Strategia dell'UE per la cybersecurity nel decennio digitale", varata il 16 dicembre – andrebbe a svolgere nell'ambito dell'ecosistema cyber dell'Unione, quale strumento volto a coordinare le diverse realtà europee competenti, a vario titolo, in materia di sicurezza cibernetica.

GESTIONE DELLE SITUAZIONI DI CRISI CIBERNETICA

Nucleo per la Sicurezza Cibernetica

A partire dal 2018, il NSC svolge le proprie funzioni riunendosi mensilmente per attività di prevenzione, preparazione, risposta e ripristino rispetto ad eventuali situazioni di crisi cibernetica, con l'obiettivo di rafforzare la resilienza cyber del Paese, con il determinante apporto di AISI, AISE, della Polizia Postale e, ove necessario, del Comando Operazioni in Rete della Difesa.

Oltre alle attività ordinarie, il NSC è stato attivato numerose volte anche nel 2020 per valutare possibili impatti di attacchi cyber sulla sicurezza nazionale e sulla protezione cibernetica – in particolare anche ai danni di strutture italiane di eccellenza impegnate nel fronteggiare l'emergenza pandemica da Covid-19 – e approntare opportune contromisure. Nell'occasione, gli esperti del NSC, avvalendosi delle strutture tecniche preposte, hanno valutato gli episodi registrati provve-

dendo ad allertare la rete sanitaria nazionale allo scopo di innalzare le difese cyber di tali infrastrutture.

Quanto alle attività di prevenzione e preparazione, il NSC ha:

- raccolto, analizzato e disseminato, attraverso lo CSIRT italiano, dati su incidenti e compromissioni di reti e sistemi delle Amministrazioni;
- studiato misure di coordinamento interministeriale;
- proseguito nella predisposizione di attività di formazione quali, ad esempio, i corsi destinati ai dirigenti delle Amministrazioni NSC, anche di fascia apicale;
- promosso e coordinato la partecipazione nazionale ad esercitazioni cyber, tra le quali meritano particolare menzione la pianificazione di esercizi multisettoriali in ambito UE (e.g. Cyber Europe) e NATO (e.g. Crisis Managament Exercise-CMX), nonché la Blueprint Operational Level Exercise (Blue OLEx).

Compiti del Nucleo per la Sicurezza Cibernetica

Cyber Crisis Liaison Organisation Network

Il lancio ufficiale della rete Cyber Crisis Liaison Organisation Network (CyCLONe) è un risultato conseguito grazie al lavoro svolto in particolare dall'Italia (attraverso il DIS) e dalla Francia (ANSSI), che hanno guidato i lavori in ambito europeo. CyCLONe è volto a garantire la preparazione, la conoscenza situazionale dell'Unione, nonché il raccordo nella gestione delle crisi ed il supporto al decisore politico sia nazionale che europeo. La rete si incardina nel framework delineato dal Blueprint per una risposta coordinata agli incidenti e alle crisi su larga scala organizzando la cooperazione transfrontaliera su tre piani: politico, rappresentato dai dispositivi integrati per la risposta politica alle crisi (IPCR) del Consiglio UE; operativo, da CyCLONe; e tecnico, dalla rete degli CSIRT. In questo contesto, CyCLONe rappresenta l'infrastruttura transfrontaliera utile ad un efficace coordinamento tra il Presidente del NSC e i suoi omologhi negli altri Stati Membri.

In seno a CyCLONe, con il supporto del NIS Cooperation Group, viene organizzato con cadenza annuale l'evento UE di alto livello Blue OLEx a cui partecipano gli Executive, ovvero i vertici delle Autorità cyber nazionali in Europa, nonché gli omologhi delle Istituzioni UE. Componente fondante è l'esercizio svolto dagli Executive stessi con lo scopo di testare e rafforzare le capacità degli Stati in caso di situazioni di crisi cibernetica in Europa, nell'ambito del Blueprint, al fine di migliorare la cooperazione tra Stati Membri e con le Istituzioni UE, sia sul versante della prevenzione e risposta alle minacce del cyberspazio, sia su quello della resilienza.

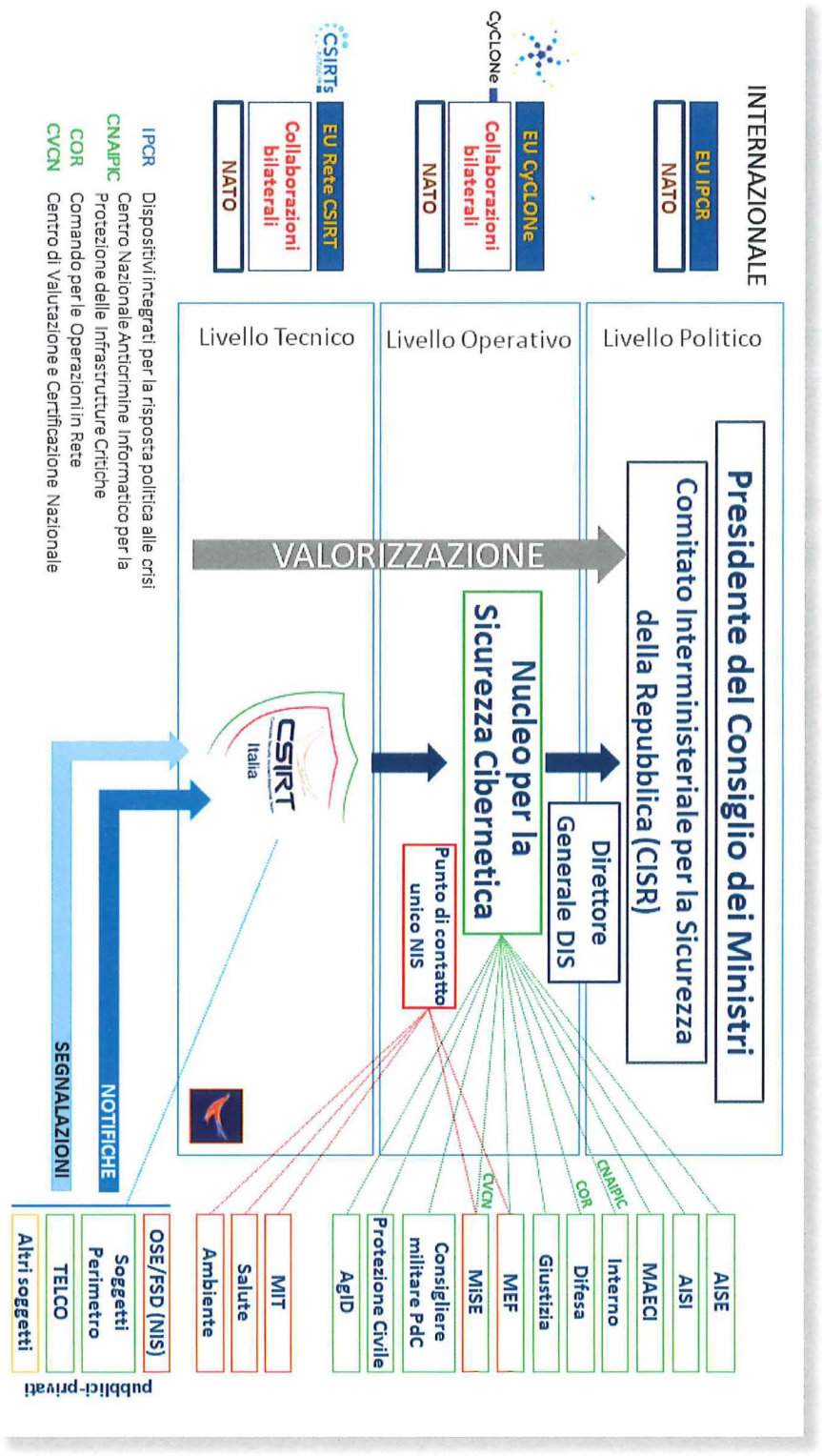
Ruolo di coordinamento nelle situazioni di crisi cibernetica

L'architettura nazionale di sicurezza cibernetica si incardina perfettamente nella piattaforma definita dal citato Blueprint, con il livello:

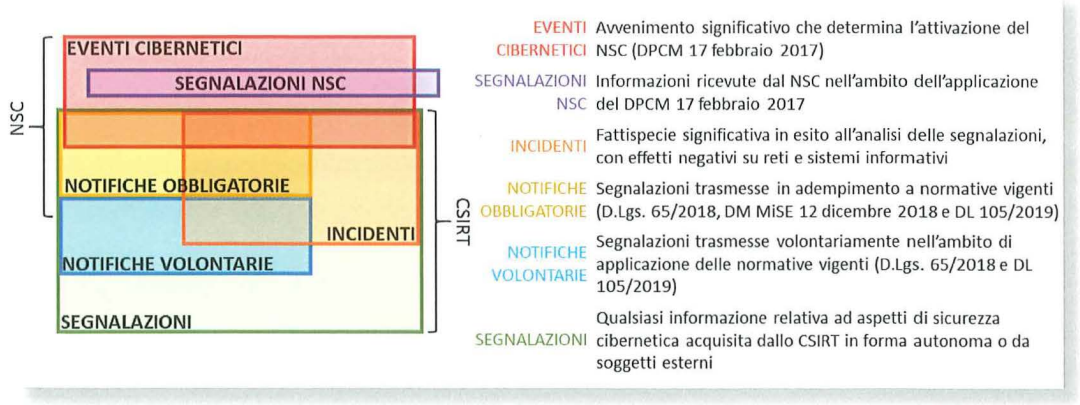
- politico, rappresentato dal Presidente del Consiglio dei Ministri e dal CISR;
- operativo, costituito dal NSC;
- tecnico, realizzato dallo CSIRT italiano.

Avendo al suo interno lo CSIRT italiano, l'Unità per l'Allertamento (UdA), il Punto di contatto unico NIS (PoC) e il NSC, il DIS ricopre due dei tre livelli funzionali a consentire una prevenzione e risposta adeguata a potenziali attacchi cyber al Sistema Paese, fornendo altresì supporto al livello politico, quale coordinatore delle situazioni di crisi cibernetica. La struttura sinergica così definita determina un processo che, in pieno raccordo con le omologhe articolazioni europee e internazionali, vede la valorizzazione delle segnalazioni o notifiche acquisite dallo CSIRT in merito a possibili incidenti trattati a livello tecnico o in eventi cibernetici che necessitano dell'attivazione del NSC per la valutazione della sussistenza di situazioni di crisi.

Per quanto la maggior parte delle attività del NSC siano sensibili e protette, per adempiere alle sue funzioni istituzionali, alcune sono rese note al pubblico. Si fa riferimento, ad esempio, all'evento cibernetico relativo a SolarWinds Orion, per il quale, a seguito di interlocuzioni con gli omologhi europei tramite CyCLONe, è stata avviata – in piena sinergia con lo CSIRT italiano – una campagna pubblica di sensibilizzazione per mitigare i rischi, nonché di mappatura dell'esposizione potenziale dei soggetti preposti a gestire le funzioni ed i servizi essenziali per la sicurezza nazionale (inclusi nel Perimetro), gli OSE e gli enti della Pubblica Amministrazione. L'attività è ancora in corso al tempo della stesura di questo documento ed è stata oggetto di condivisione con i membri di CyCLONe.


INTERNAZIONALE
EU IPCR
NATO
CyCLONe
EU CyCLONe
Collaborazioni bilaterali
NATO
CSIRTs Network
EU Rete CSIRT
Collaborazioni bilaterali
NATO
Livello Politico
Livello Operativo
Livello Tecnico
Presidente del Consiglio dei Ministri
Comitato Interministeriale per la Sicurezza della Repubblica (CISR)
VALORIZZAZIONE
Direttore Generale DIS
Nucleo per la Sicurezza Cibernetica
Punto di contatto unico NIS
CSIRT Italia
IPCR Dispositivi integrati per la risposta politica alle crisi
CNAIPIC Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
COR Comando per le Operazioni in Rete
CVCN Centro di Valutazione e Certificazione Nazionale
SEGNALAZIONI
NOTIFICHE
AISE
AISI
MAECI
Interno
Difesa
Giustizia
MEF
MISE
CVCN
Consigliere militare PdC
Protezione Civile
AgID
MIT
Salute
Ambiente
OSE/FSD (NIS)
Soggetti Perimetro
TELCO
Altri soggetti
pubblici-privati

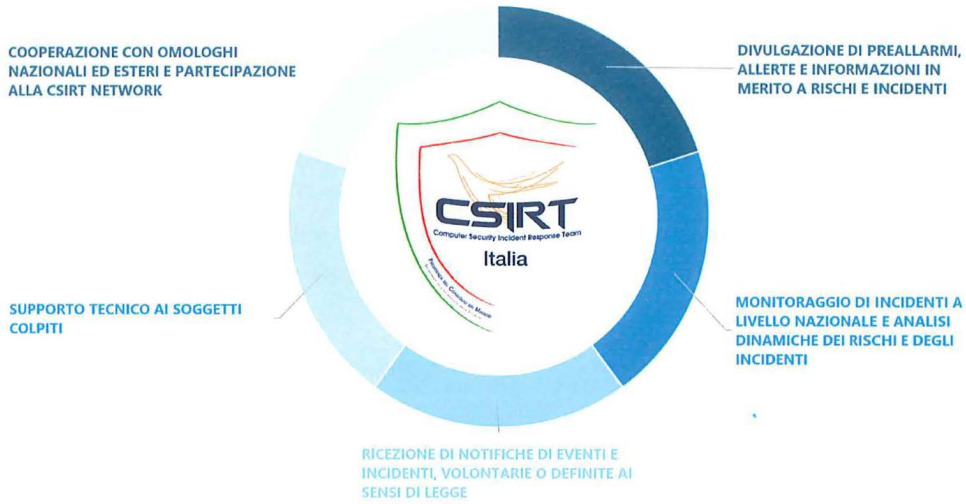
Terminologia: tassonomia degli eventi cibernetici e delle segnalazioni



ATTIVITA' DELLO CSIRT ITALIANO

Compiti dello CSIRT

Come anticipato nel Documento di Sicurezza Nazionale del 2019, a partire dal 6 maggio 2020 è divenuto operativo presso il DIS lo CSIRT italiano, assumendo i compiti fino a quel momento assolti dal CERT della Pubblica Amministrazione dell'Agenzia per l'Italia Digitale e dal CERT Nazionale del MiSE. Tale struttura tecnica, incaricata di svolgere attività di prevenzione e gestione degli incidenti informatici con impatto, effettivo o potenziale, sul territorio nazionale, è andata a rafforzare la governance unitaria della sicurezza cibernetica nazionale.



Tra i principali compiti svolti dallo CSIRT italiano, emergono: le attività di divulgazione, tramite preallarmi e allerte, di informazioni relative a rischi e incidenti cibernetici; il monitoraggio degli incidenti a livello nazionale; la ricezione delle notifiche di incidenti, volontarie o definite ai sensi di legge e l'eventuale, successivo inoltro al NSC; il supporto ai soggetti colpiti per facilitare la gestione

tecnica dell'evento cibernetico; le attività di cooperazione e collaborazione con altri omologhi esteri, inclusa la diffusione delle informazioni verso altri Stati eventualmente coinvolti da incidenti avvenuti in territorio nazionale.

Lo CSIRT partecipa attivamente alla rete UE degli CSIRT. Dalla sua attivazione, il Team italiano ha preso parte a numerosi meeting, side-meeting e conferenze ed eventi internazionali afferenti all'ambito della rete CSIRT, nell'ottica del potenziamento della proiezione internazionale.

RETE UE DEGLI CSIRT

La rete UE degli CSIRT è composta dagli CSIRT degli Stati Membri dell'Unione e dal CERT-UE, al fine di sviluppare la fiducia tra i Paesi europei e promuovere una cooperazione operativa rapida ed efficace. Tale rete è diventata uno dei principali punti di riferimento, grazie all'attivazione di piattaforme per la condivisione di informazioni e all'organizzazione di periodiche riunioni, volte anche allo scambio di esperienze e best practice per una risposta coordinata a specifici incidenti.

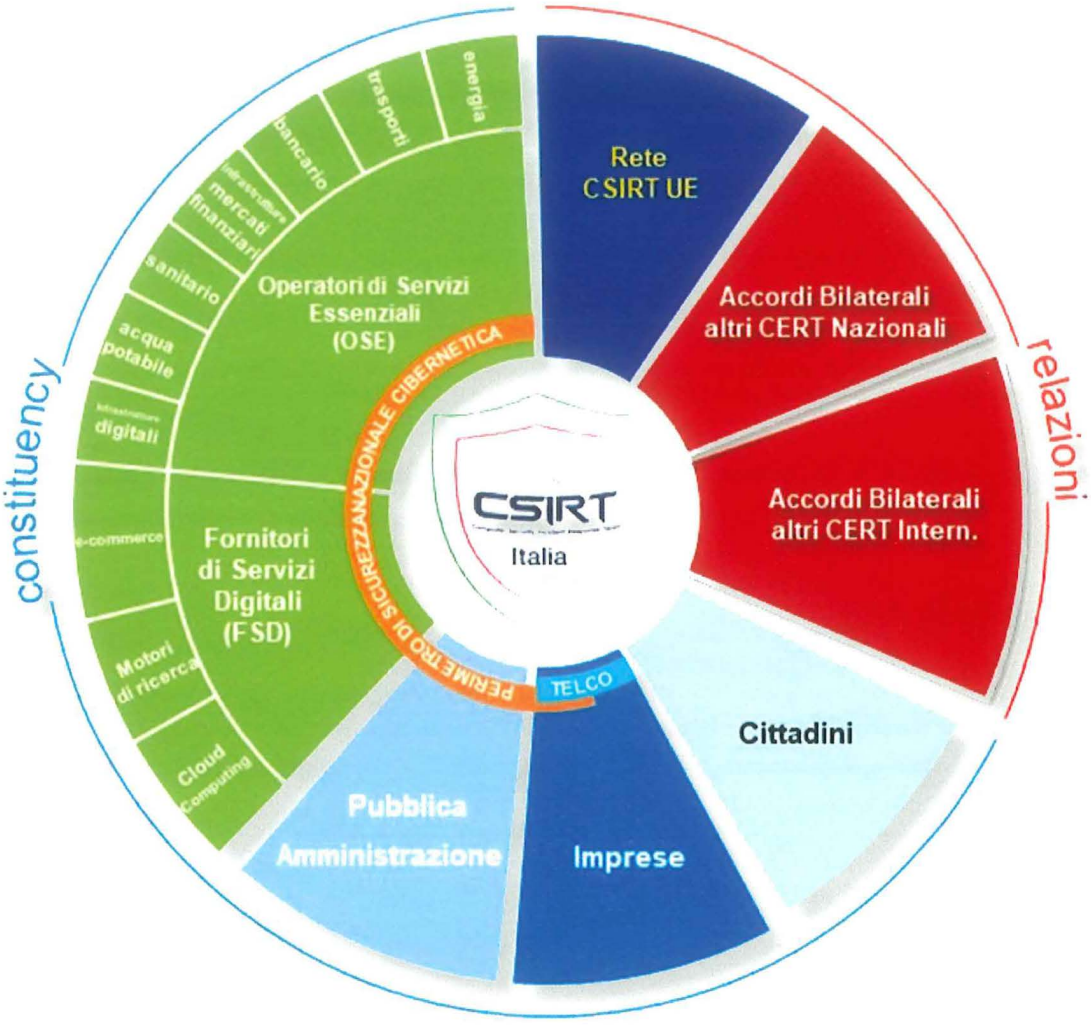
Sono stati molteplici anche gli incontri in conference call con l'intera rete nell'ottica di rafforzare i rapporti di collaborazione fra le parti e la condivisione di report tecnici, elaborati dallo CSIRT italiano, relativi a incidenti avvenuti ai danni di soggetti nazionali, ma con possibili implicazioni per gli altri Stati Membri.

Al riguardo, in ragione della natura tipicamente transnazionale degli eventi cibernetici, lo CSIRT, dalla sua nascita, ha costantemente interagito – a livello bilaterale – con gli omologhi organismi esteri, operanti in Stati sia europei che extra-europei.

Ciò ha permesso di mettere a sistema le rispettive competenze per l'effettuazione di analisi congiunte, consentendo di approfondire la conoscenza di vulnerabilità e di infrastrutture/servizi gestiti dai cyber-criminali, come nel caso della pubblicazione relativa a un framework di "Phishing-As-A-Service" realizzata insieme al CERT della Lettonia.

Canali di comunicazione

Sono stati predisposti e attivati diversi canali per la condivisione di informazioni con la constituency – composta da soggetti appartenenti alle Pubbliche Amministrazioni (centrali e locali) e al settore privato, come OSE, Fornitori di Servizi Digitali (FSD), soggetti inclusi nel "Perimetro di sicurezza nazionale cibernetica" e operatori di telecomunicazioni (cd. Telco) – che si differenziano in ragione del tipo di informazioni trattate e della loro sensibilità. Al riguardo, a partire dal mese di ottobre, è stato avviato un portale di "collaboration", riservato ai membri della constituency. Quest'ultimo rappresenta lo strumento privilegiato per favorire lo scambio di informazioni tecniche specifiche con i soggetti accreditati.



Al fine di supportare i compiti di sensibilizzazione su tematiche di sicurezza informatica e disseminare contenuti di rilevanza pubblica, sin dall'avvio dei lavori dello CSIRT è stato realizzato un portale pubblicamente accessibile, disponibile all'indirizzo web https://csirt.gov.it, che offre anche ai cittadini la possibilità di segnalare eventi cibernetici significativi. In particolare, esso contiene notizie, allerte, bollettini di approfondimento, analisi, infografiche e pubblicazioni di interesse, suddivisi per tipologia e destinatari. Nell'ottica di promozione dei servizi offerti e di potenziamento delle attività di divulgazione dello CSIRT, è stato, anche, creato l'account ufficiale Twitter @CSIRT_it.

Portale pubblico

Portale di collaboration

Portale Twitter

Lo CSIRT ha, altresì, attivato numerosi contatti, in occasione di incidenti, con le strutture IT delle organizzazioni interessate, offrendo loro piena collaborazione anche al fine di individuare, in accordo con le controparti, opportune strategie di mitigazione dei relativi effetti e di risposta.

Infine, nel quadro del rapporto di collaborazione tra il DIS e il Garante per la protezione dei dati personali, si annovera la sottoscrizione, avvenuta il 1° dicembre 2020, di un Addendum per l'attuazione del "Protocollo d'intenti sulla protezione dei dati personali nelle attività di sicurezza cibernetica", rinnovato nel marzo 2019. Al riguardo, il documento attuativo mira a definire le modalità con cui lo CSIRT, in occasione di data-breach, possa ricevere gli elementi tecnici rilevanti sotto il profilo della cybersecurity, al fine di prevenire ulteriori simili incidenti.

Segnalazioni

Dall'avvio delle sue attività, lo CSIRT ha trattato oltre 25.000 segnalazioni provenienti sia da società di sicurezza ed omologhi esteri, sia da soggetti nazionali attraverso i canali messi a disposizione della constituency. Di questi, oltre 3.500, pari al 13,8% circa, sono stati classificati quali incidenti e conseguentemente gestiti nel dettaglio, nonché in buona parte inviati, per successiva valorizzazione, al NSC.

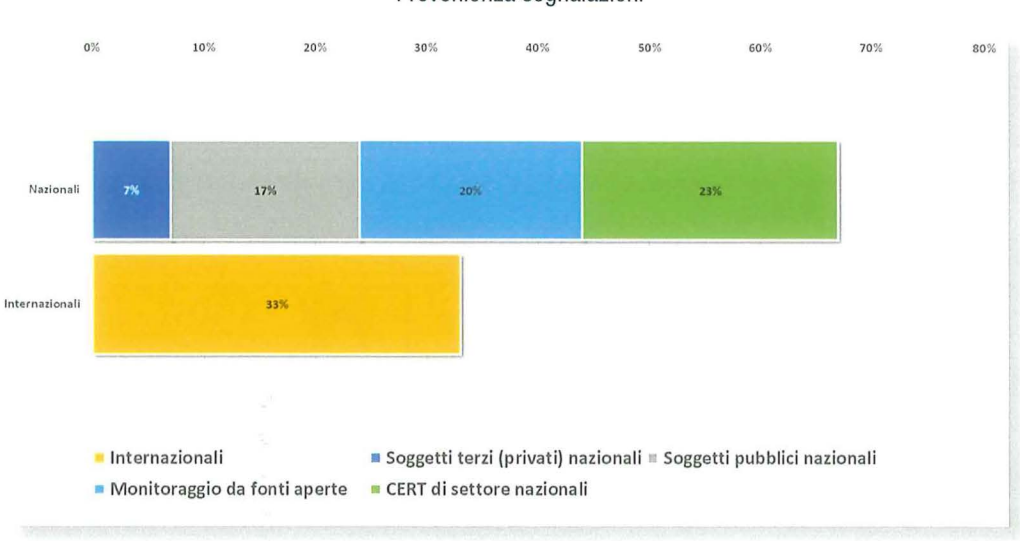
25.845 segnalazioni | **3.558** incidenti | **117** incidenti critici | **273** vulnerabilità critiche

Periodo 06/05/2020 - 31/12/2020

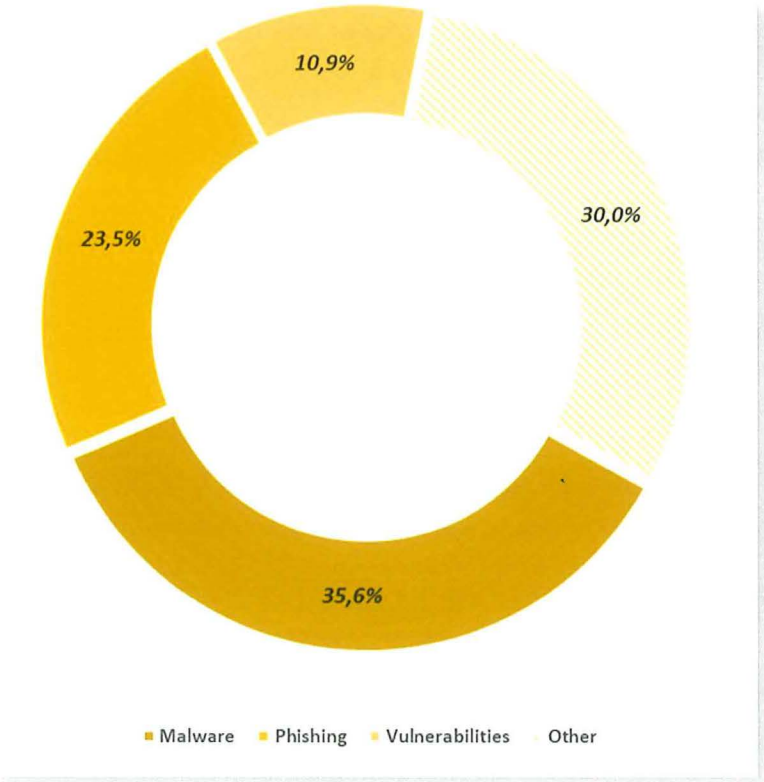
Le suddette attività sono state espletate nel rispetto delle best practice internazionali (e.g. Trusted Introducer, FIRST) e delle linee guida stabilite dall'Agenzia dell'UE per la Cybersercurity (ENISA), attraverso un processo di gestione delle segnalazioni opportunamente strutturato.

Con riferimento alla provenienza geografica delle segnalazioni, si rileva la preponderanza delle attivazioni originate in ambito nazionale. Al riguardo, dalla loro ripartizione effettuata sulla base dei soggetti segnalanti, emerge la prevalenza di quelle provenienti dai CERT di settore nazionali. Per quanto riguarda, invece, il

contesto internazionale, le segnalazioni pervengono principalmente da omologhe articolazioni governative e CERT commerciali, aderenti alla rete UE degli CSIRT.



Per quanto concerne le categorie di rischio, si evidenzia la prevalenza di malware e phishing, seguiti dalle vulnerabilità individuate in prodotti e sistemi e altre casistiche che includono ad esempio data-breach, DDoS, etc.



Con riferimento ai settori maggiormente colpiti, registrati nella prima fase di operatività dello CSIRT, emerge la prevalenza dei soggetti appartenenti alla Pubblica Amministrazione e al settore finanziario.

Nell'ambito della trattazione delle segnalazioni, sono stati emessi preallarmi, allerte, annunci e divulgate informazioni alle parti interessate in merito a rischi e incidenti. Le funzioni di allertamento e divulgazione a favore di singoli soggetti della constituency vengono effettuate attraverso comunicazioni dirette. Nello specifico, dall'avvio delle attività dello CSIRT al 31 dicembre 2020 sono state inviate oltre 3.000 comunicazioni ai soggetti a rischio interessati, tese alla loro sensibilizzazione o allertamento.

3.072 comunicazioni dirette | **379** comunicazioni sul portale pubblico | **79** comunicazioni sul portale di "collaboration"

Periodo 06/05/2020 - 31/12/2020

Analisi tecniche

Considerando gli incidenti legati ad agenti malevoli, lo CSIRT ha pubblicato le seguenti monografie tecniche, realizzate sulla base delle analisi esperite:

- Agent Tesla: nato come infostealer, ha aggiunto nel tempo capacità di injection e diffusione molto più avanzate oltre alla capacità di sottrarre dettagli delle reti e credenziali di accesso;

- Emotet: trojan modulare distribuito come first stage che, dopo aver infettato con successo un sistema, distribuisce infostealer o ransomware;
- Netwalker: ransomware as-a-service che usa tecniche di tipo fileless;
- ModiLoader: dropper multi-stage sfruttato per eseguire un Remote Access Tool (RAT, tool di accesso remoto) sulla macchina vittima;

- Sunburst: trojan osservato per la prima volta nel mese di dicembre 2020 a seguito dall'evento cibernetico che ha riguardato la piattaforma Solarwinds Orion.

ATTIVITA' DI FORMAZIONE E CONSAPEVOLEZZA

Il DIS, proseguendo le attività avviate dal 2018, continuerà a promuovere, nell'ambito del NSC, iniziative volte a favorire una maggiore consapevolezza dei rischi connessi alla cibersicurezza, il rispetto delle pratiche di cyber-hygiene e la formazione, a beneficio di target diversificati, operanti a diversi livelli, dalle Pubbliche