SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA

DOCUMENTO DI SICUREZZA NAZIONALE

ALLEGATO ALLA RELAZIONE ANNUALE AL PARLAMENTO

AI SENSI DELL'ART. 38, CO. 1 BIS, LEGGE 124/2007


Crisi cibernetica nazionale
Bot
Distributed Denial of Service (DDoS)
Attribution
Bitsquatting
Web-defacement
Social engineering
Computer Security Incident Response Team (CSIRT)
Confidence Building Measure (CBM)
False flag
SQL Injection
Phishing
Ransomware
Spoofing
Typosquatting
Malware
Computer Security Incident Response Team (CSIRT)
Advanced Persistent Threat (APT)

INDICE

2013-2017: LE TAPPE DELLA *CYBER SECURITY* IN ITALIA

2013	**L. n.133/2012 Modifiche alla l. n.124/2007**
GENNAIO	**Decreto Monti DPCM 24/01/2013** Direttiva che definisce la prima architettura nazionale *cyber*
APRILE	**Tavolo Tecnico *Cyber*** Istituzione del TTC per lo sviluppo dell'architettura nazionale in sede di coordinamento interministeriale
LUGLIO	**Nucleo per la Sicurezza Cibernetica** Prima riunione plenaria
NOVEMBRE	**Tavolo Tecnico Imprese** Vengono avviati i lavori del TTI per dare inizio ad una PPP strutturata
DICEMBRE	**Strategia Nazionale *Cyber*** Adozione del primo Quadro Strategico Nazionale e del Piano Nazionale
2014	**CERT-PA** Il *Computer Emergency Response Team* della Pubblica Amministrazione diventa operativo
OTTOBRE	**Collaborazione con il CINI** Il DIS sigla un accordo di cooperazione con il Consorzio Interuniversitario Nazionale per l'Informatica
NOVEMBRE	**CERT-N** Il *Computer Emergency Response Team* Nazionale diventa operativo
2015	**Direttiva 1° agosto 2015 sul coordinamento interministeriale** volta ad allineare gli assetti difensivi *cyber* del Paese a quelli dei principali partner internazionali
OTTOBRE	**CISR** Con il D.L. 174/2015 vengono attribuiti al CISR compiti di supporto al Presidente del Consiglio in caso di situazioni di crisi che coinvolgono la sicurezza nazionale
2016	**Legge di stabilità 2016** Il Governo stanzia 150 milioni di euro per la *cyber security*
GIUGNO	**Aggiornamento architettura *cyber*** Avvio del processo di aggiornamento dell'architettura
LUGLIO	**Direttiva NIS 2016/1148** Il Parlamento UE vara la Direttiva sulla sicurezza delle reti e dei sistemi informativi dell'Unione, da attuare entro maggio 2018
2017	**Decreto Gentiloni DPCM 17 febbraio 2017** Nuova architettura nazionale *cyber*
MAGGIO	**Aggiornamento del Piano nazionale *cyber*** Pubblicazione del nuovo Piano Nazionale per la sicurezza cibernetica

PREMESSA

In linea con un mondo che continua ad essere sempre più interconnesso e dipendente dall'efficace funzionamento e dalla resilienza di reti, sistemi e dispositivi informatici – che conferiscono natura ubiquitaria ai contenuti da essi trasportati, elaborati e conservati – l'architettura nazionale *cyber* ha conosciuto, nel 2017, interventi di modifica miranti a razionalizzare e potenziare ulteriormente le capacità di difesa cibernetica del Paese. Il 17 febbraio è stato adottato il nuovo Decreto del Presidente del Consiglio dei Ministri "*Direttiva recante gli indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*" (cd. "Decreto Gentiloni") che, nel sostituire quello del 24 gennaio 2013, ha posto il Dipartimento Informazioni per la Sicurezza-DIS al centro della *governance* nazionale in materia di *cyber security*. Il DIS ha, così, assunto la direzione del Nucleo per la Sicurezza Cibernetica-NSC, deputato all'adozione di misure di coordinamento per la gestione di incidenti *cyber* di particolare rilevanza e per la dichiarazione della crisi cibernetica nazionale, rispetto alla quale è chiamato a tenere costantemente informato il Presidente del Consiglio dei Ministri. Nella sua nuova veste, il Nucleo si è riunito per valutare eventi cibernetici con potenziale impatto sistemico - *ransomware WannaCry* e *software* malevolo *NotPetya* – sia per definirne l'effettiva portata, sia per individuare le necessarie contromisure. In tale ambito, gli esiti degli approfondimenti svolti hanno consentito di rilevare, a dispetto del rilievo mediatico che hanno ricevuto i richiamati incidenti, contenute ripercussioni in ambito nazionale.

Tra le ulteriori misure tese ad elevare gli *standard* di sicurezza dei sistemi e delle reti italiane, vanno annoverate quelle che prevedono – anche in vista del recepimento della Direttiva UE 1148/2016 "Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione" – l'unificazione operativa del CERT Nazionale (CERT-N) e del CERT della Pubblica Amministrazione (CERT-PA), al fine di acquisire maggiore capacità di rilevazione, allarme e prima analisi degli incidenti cibernetici, e l'istituzione, presso il Ministero dello Sviluppo Economico, di un Centro di Valutazione e Certificazione Nazionale-CVCN cui sarà affidata la verifica dell'affidabilità delle componenti ICT destinate ad essere impiegate nei sistemi di soggetti sia pubblici che privati nazionali, titolari di funzioni critiche o strategiche.

Tale riorganizzazione è stata formalmente declinata, a marzo, nel nuovo "*Piano nazionale per la protezione cibernetica e la sicurezza informatica*", che ha individuato, nell'annesso Piano d'Azione, le misure ritenute più urgenti per rafforzare gli assetti cibernetici del nostro Paese. L'aggiornamento del documento, frutto di una sinergia che ha coinvolto tutte le componenti dell'architettura nazionale, è stato agevolato da un articolato processo di revisione delle attività svolte a partire dal 2013 e di identificazione delle principali *lesson learned*.

Sul piano generale, la razionalizzazione operata attraverso i richiamati interventi potrà meglio contribuire ad elevare la sicurezza dei nostri sistemi se le molteplici iniziative *cyber* – assunte a livello verticale (nazionale, regionale e locale) e orizzontale (pubblico e privato)

– saranno ancorate alla logica di sistema delineata nel DPCM Gentiloni. Iniziative che dovranno coprire in modo organico le varie dimensioni della minaccia *cyber*, evitando inutili sovrapposizioni. Attraverso la sistematizzazione degli sforzi nazionali sarà inoltre possibile avviare un cambio di passo anche a livello internazionale, *in primis* presso l'Unione Europea, ove è necessario rafforzare il presidio degli esercizi d'interesse, allo scopo di elevare gli *standard* di sicurezza nei prodotti *hardware* e *software* relativi al mercato unico digitale europeo e, allo stesso tempo, garantire agli *asset* strategici pubblici e privati del nostro Paese livelli di sicurezza adeguati alla minaccia.

Sul fronte intelligence, il Comparto ha continuato a tutelare i *target* rilevanti per la sicurezza nazionale (infrastrutture critiche ed *asset* strategici), sia in chiave preventiva che *post incident*.

Lo spionaggio digitale, confermatosi come la minaccia più insidiosa, ha manifestato ancora una volta elevate capacità di rimodulazione rispetto alle misure difensive adottate per ridurre la superfice d'attacco. Riguardo all'incremento segnato dal *cyber-espionage*, sono apparsi stabili l'attivismo digitale e il *cyber*-terrorismo, che non hanno fatto registrare significative evoluzioni in termini sia di capacità che di tecniche impiegate. La ricerca di vulnerabilità nelle infrastrutture digitali di realtà produttive nazionali ha consentito, inoltre, l'implementazione di operazioni di *patching* per scongiurare i rischi di sottrazione di *know-how* pregiato o il blocco di attività.

In linea di continuità con le precedenti edizioni, il Documento di Sicurezza Nazionale è suddiviso in due parti: l'una, dedicata alle dinamiche che hanno interessato l'architettura di sicurezza cibernetica del nostro Paese; l'altra, volta a fornire una fotografia della minaccia *cyber* in Italia.

POTENZIAMENTO DELLE CAPACITÀ CIBERNETICHE NAZIONALI

Nel 2013, con il cd. "Decreto Monti", l'Italia ha delineato, per la prima volta, la sua architettura di sicurezza cibernetica, provvedendo a sistematizzare, sia pure a legislazione vigente, le molteplici competenze di settore distribuite tra diversi attori istituzionali. Ciò ha consentito l'avvio dell'accrescimento delle capacità *cyber* nazionali, opportunamente guidato dagli atti di indirizzo strategico (il "Quadro strategico nazionale") e operativo (il "Piano nazionale *cyber*").

Pur a fronte dei positivi risultati raggiunti, le evoluzioni che hanno interessato la materia – *in primis*, quelle connesse con la Direttiva NIS sulla sicurezza di *network and information system* della UE – hanno imposto una verifica dell'efficacia dell'architettura nazionale a fronte, da un lato, della crescente sofisticazione della minaccia e della rilevanza strategica dei *target* cui la stessa si rivolge e, dall'altro, degli impegni assunti dall'Italia in ambito internazionale, ove i principali Alleati hanno conseguito avanzati assetti difensivi e, non di rado, offensivi.

Gli esiti di tale verifica si sono tradotti nel "DPCM GENTILONI" che, sempre ad invarianza del quadro normativo primario vigente, è intervenuto razionalizzando ulteriormente l'architettura delineata nel 2013. Tale provvedimento ha ridefinito le attribuzioni del Presidente del Consiglio dei Ministri e del CISR nel campo della sicurezza cibernetica, in linea con le funzioni di deliberazione, consulenza e proposta, a supporto del Presidente del Consiglio attribuite al CISR dall'articolo 7-*bis* del Decreto Legge n. 174/2015 in caso di crisi, assegnando al Direttore Generale del DIS un ruolo attivo e centrale nella gestione ordinaria e straordinaria della *cyber security* in Italia. Il DG-DIS, infatti, è chiamato a definire le linee di azione di interesse generale, al fine di innalzare e migliorare i livelli di sicurezza dei sistemi e delle reti nazionali, e ad individuare le più avanzate soluzioni tecnologiche a sostegno delle attività di prevenzione, contrasto e risposta agli incidenti che interessino Amministrazioni, enti pubblici e operatori privati.

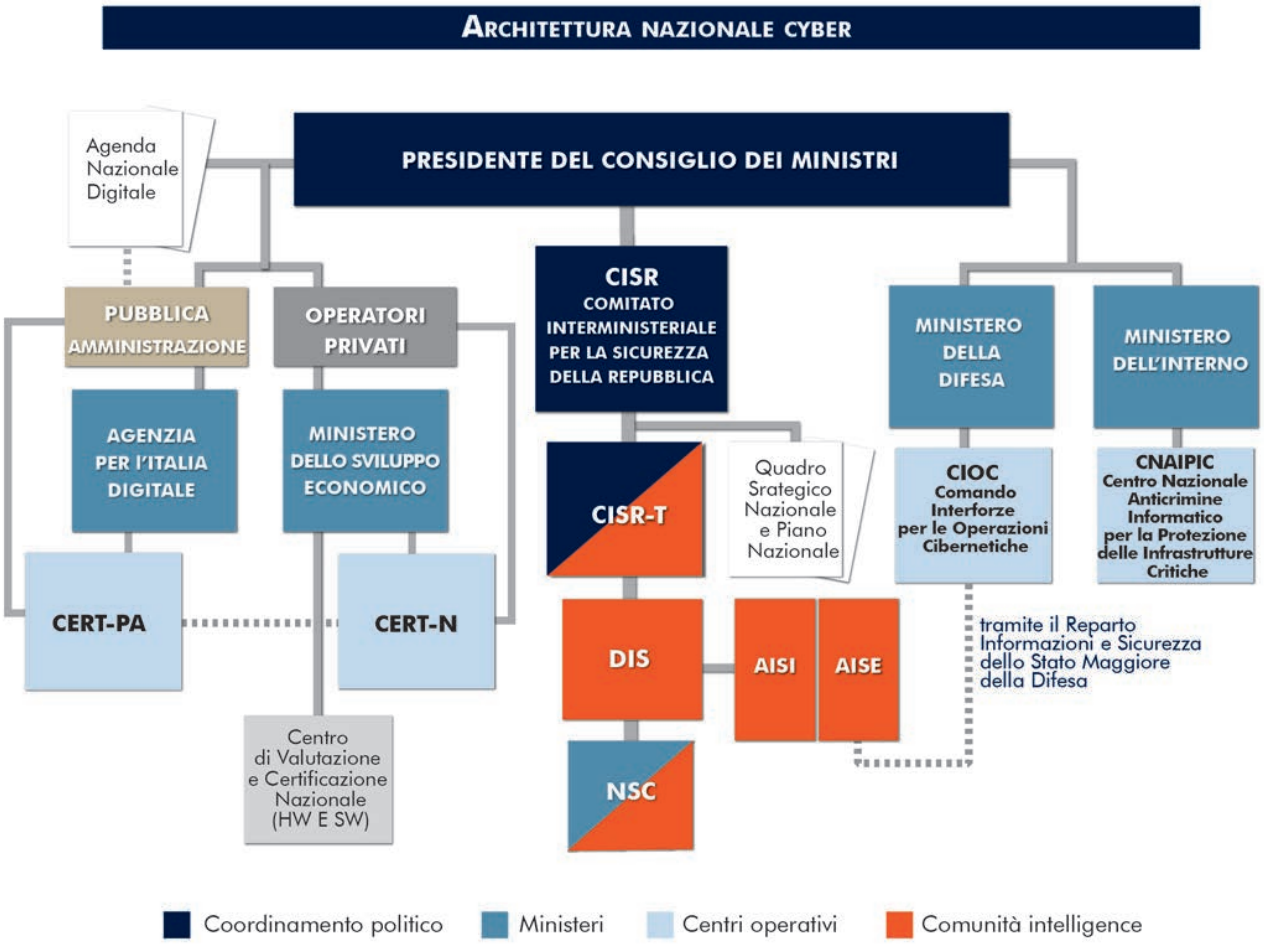
Il Comitato Interministeriale per la Sicurezza della Repubblica-CISR, a livello politico, è presieduto dal Presidente del Consiglio dei Ministri, ed è composto, oltre che dall'Autorità delegata (ove nominata), dai seguenti Ministri:

1. AFFARI ESTERI E COOPERAZIONE INTERNAZIONALE
2. INTERNO
3. GIUSTIZIA
4. DIFESA
5. ECONOMIA E FINANZE
6. SVILUPPO ECONOMICO

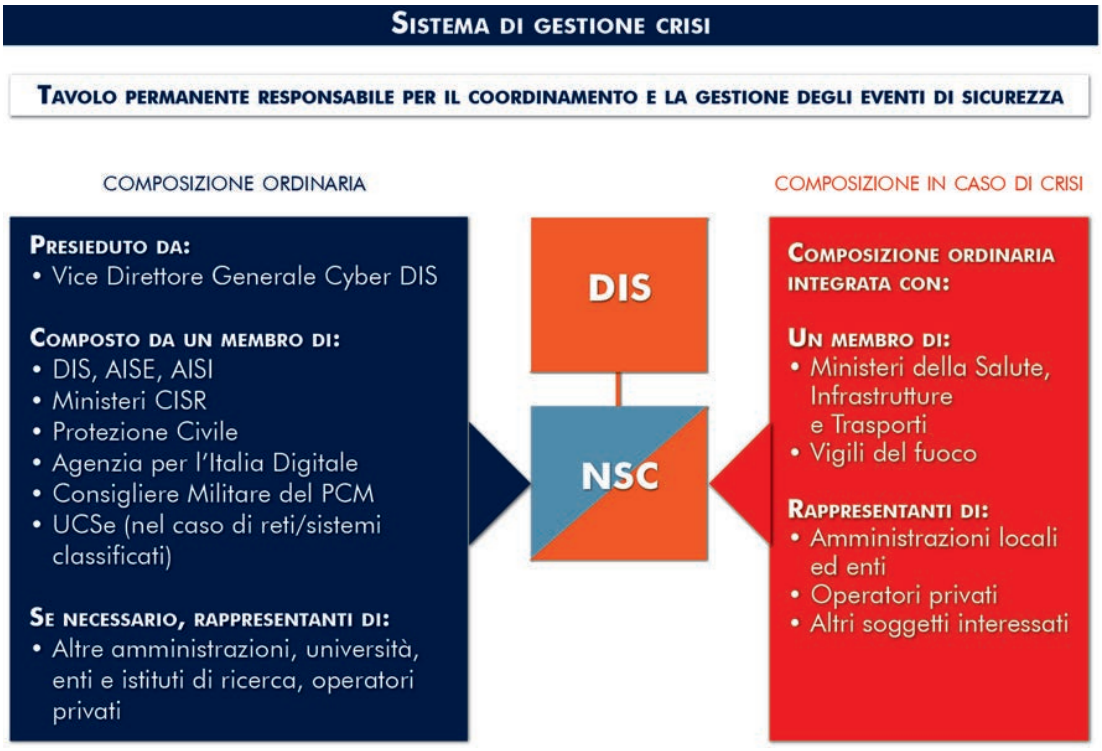
Il Direttore Generale del DIS svolge le funzioni di Segretario del Comitato.

Al Ministero dello Sviluppo Economico è stato, poi, conferito il compito di istituire un Centro di Valutazione e Certificazione Nazionale per la verifica dell'affidabilità della componentistica ICT da impiegare, in particolare, nelle infrastrutture critiche e strategiche.

A seguire una panoramica dei soggetti che compongono l'architettura nazionale *cyber* ai sensi del "DPCM Gentiloni".



Le misure di razionalizzazione dell'architettura e di riposizionamento dell'NSC – chiamato ad operare in chiave sia di prevenzione e preparazione (*prevention & preparedness*) che di risposta e ripristino (*response & recovery*) – sono state accompagnate dalla nomina di un dedicato Vice Direttore Generale del DIS, cui spettano funzioni di raccordo degli attori che compongono il *framework* nazionale. Di seguito una panoramica del nuovo sistema di gestione delle crisi (*v. Glossario*).

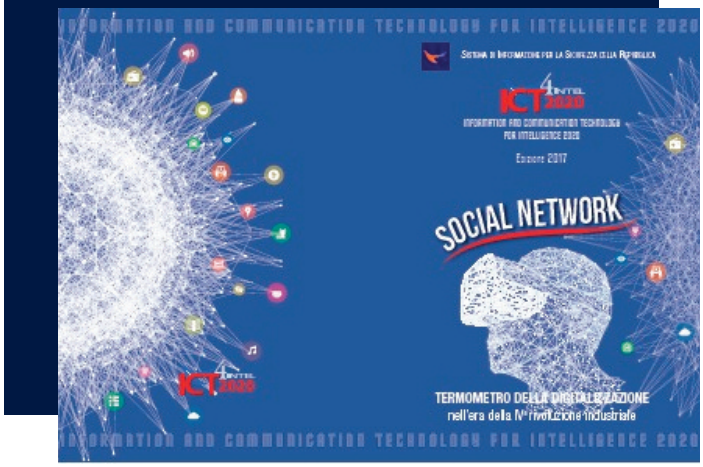


Al Vice Direttore Generale *Cyber* è demandata, altresì, l'attuazione delle misure di potenziamento previste dal Piano d'Azione-PA, annesso al Piano Nazionale, tra cui spiccano la unificazione tra CERT-N e CERT-PA – anche in vista della costituzione del CSIRT nazionale (*v. Glossario*) chiamato ad interfacciarsi, ai sensi della Direttiva NIS, con il CSIRT europeo – e l'avvio di iniziative volte a realizzare un "Centro nazionale di Ricerca e Sviluppo in *Cybersecurity*", nonché un "Centro nazionale di crittografia".

Iniziative, queste ultime, che potranno essere proficuamente sviluppate, in linea con quanto fatto da altri Paesi tecnologicamente avanzati, nell'ambito di una entità istituzionale in grado di fungere da stimolatore, collettore e incubatore. Si tratta, in sostanza, di prevedere la costituzione di una Fondazione per la sicurezza cibernetica, attraverso cui dare vita ad un'effettiva alleanza tra istituzioni, aziende e mondo accademico, così da favorire lo sviluppo di linee di ricerca mirate nell'ottica di delineare appropriate architetture digitali nazionali intorno al concetto di sicurezza. Tali architetture devono rispondere, in un contesto di profonda trasformazione digitale, alla complessità delle minacce presenti e future, assicurando una "continuità di servizio" che possa abilitare un organico sviluppo economico e sociale del Paese.

IL PARTENARIATO PUBBLICO-PRIVATO-PPP, alleanza necessaria in materia di *cyber security*, ha conosciuto un allargamento a nuovi operatori critici e strategici, che hanno sottoscritto convenzioni con il DIS. La collaborazione con tali soggetti ha continuato a sostanziarsi in incontri periodici del TAVOLO TECNICO IMPRESE-TTI, in occasione dei quali sono state trattate

tematiche di *policy*, analizzate minacce *cyber* e fornite raccomandazioni di sicurezza in chiave sia preventiva, sia di *detection*. Gli operatori convenzionati sono stati destinatari, inoltre, di SEMINARI DEDICATI ALLE MINACCE DI TIPO AVANZATO E PERSISTENTE (*v. Glossario*) ed alla CRITTOGRAFIA che, tenuti presso la Scuola di formazione del Comparto, sono stati organizzati dagli afferenti al Comitato Nazionale per la Ricerca in *cyber security*, segnatamente il Consiglio Nazionale delle Ricerche (CNR), le Università parte del Laboratorio nazionale di Cybersecurity del Consorzio Nazionale Interuniversitario per l'Informatica (CINI) ed il Consorzio Nazionale Interuniversitario per le Telecomunicazioni.



In tale contesto, inoltre, nell'ottica di promuovere una integrazione progettuale ed operativa tra Intelligence, Industria ed Università e allo scopo di garantire l'efficace impiego delle capacità *high-tech* nazionali a protezione del nostro Paese, si è tenuta, il 28 e 29 novembre, la quarta edizione dell'ICT4INTEL 2020, dedicata ai *social media*. L'obiettivo dell'edizione 2017 è stato quello di cogliere – a fronte degli impatti prodotti dall'uso massivo dei *social network* sulle tradizionali attività di ricerca, raccolta ed analisi delle informazioni – le potenzialità offerte dalla tecnologia per mitigare i rischi derivanti da tale fenomeno. Nell'occasione, particolare rilievo è stato attribuito alla necessità di un presidio che, proprio attraverso la *partnership* pubblico-privato, garantisca la tutela delle libertà e dei diritti fondamentali dei cittadini nella dimensione digitale.

A supporto di tali libertà, è stata varata la prima campagna nazionale di formazione per la promozione di un utilizzo consapevole delle tecnologie ICT, denominata *"Be Aware. Be Digital"*. Lanciata dal DIS in occasione della celebrazione del decennale della legge di riforma del Comparto, l'iniziativa, coordinata con il Ministero dell'Istruzione, dell'Università e della Ricerca, mira ad aumentare la consapevolezza dei rischi *cyber*, allo scopo di con-

sentire un più sicuro esercizio della libertà nel *web*. Una campagna, quindi, tesa ad accrescere, in un'ottica incrementale, la capacità di discernere le situazioni di reale vantaggio da quelle che privano delle libertà fondamentali. Due le categorie *target*: i giovani, per definizione "nativi digitali", e le PMI, in quanto tessuto produttivo su cui si fonda la parte più significativa della ricchezza nazionale. Vale evidenziare, inoltre, come tale ultima iniziativa sia destinata ad incontrare terreno fertile, considerato che la galassia di medie e piccole imprese nazionali è destinataria, dal 2016, del Framework Nazionale per la Cybersecurity (FNCS)[1] , strumento mediante il quale si è voluta agevolare l'introduzione nell'ambito di quelle realtà imprenditoriali già consapevoli del principio di gestione strutturata del rischio *cyber*. Il rafforzamento delle PMI nazionali consentirà di incrementare la resilienza delle filiere produttive nazionali.

Tuttavia, l'aumento della resilienza di un Paese rispetto ad attacchi di tipo cibernetico può soltanto essere efficacemente affrontato se il Paese si doterà di una *workforce* adeguata. Quindi abbiamo di fronte un problema di formazione molto vasto che include sia i lavoratori attivi che le future generazioni. Formazione che va dalla cultura di base fino alla ricerca dei talenti. Molte iniziative sono in atto a livello locale e nazionale e su di esse anche il Comparto conta per poter incrementare sia il livello generale della sicurezza, sia le capacità operative direttamente gestite.

SUL PIANO INTERNAZIONALE, il presidio di alcuni esercizi (G7, UE, NATO e OSCE) da parte del DIS ha consentito al Ministero degli Affari Esteri e della Cooperazione Internazionale di meglio sostenere gli interessi cibernetici del nostro Paese. Per quel che concerne il G7, in occasione del *Summit* di Taormina del 26-27 maggio, i *leader* dei Paesi membri hanno adottato la *"Declaration on Responsible States Behavior in Cybersapce"*, con la quale è stata riconosciuta la necessità di accrescere la cooperazione internazionale al fine di ridurre l'uso malevolo delle tecnologie ICT da parte di attori statuali e non, ed agevolare l'implementazione di *confidence building measure*-CBM (*v. Glossario*). In ambito OSCE, il DIS ha partecipato alle riunioni dell'*Informal Working Group* incentrate sulla protezione delle infrastrutture critiche. In sede UE, sono state coordinate, attraverso il TAVOLO TECNICO CYBER-TTC, le attività nazionali per la finalizzazione del *Cybersecurity Package* (cd. "Pacchetto Juncker"), lanciato il 13 settembre dalla Commissione e dall'Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza. Tale "pacchetto" – nell'ottica di colmare i *gap* emersi dopo l'adozione, nel 2013, della strategia per la sicurezza cibernetica della UE – mira a rafforzare la resilienza dell'Unione agli attacchi cibernetici, a dotare la stessa di un'efficace deterrenza cibernetica e a rafforzare la cooperazione internazionale. Quanto alle attività NATO, oltre a garantire la partecipazione all'esercitazione di *crisis management* CMX17, il DIS ha partecipato alle iniziative per lo sviluppo del Cyber Defence Pledge.

[1] http://cybersecurityframework.it

Rilevante, infine, l'esperienza maturata nell'ambito delle esercitazioni internazionali che hanno visto impegnato il nostro Paese quale *player*, in sede NATO, del citato *crisis management exercise* CMX17, cui ha partecipato, per la prima volta, la UE, svolgendo in parallelo una esercitazione finalizzata a testare le procedure di gestione delle crisi all'interno delle istituzioni comunitarie.

CYBER DEFENCE PLEDGE

Documento redatto sulla base degli indirizzi definiti dai Capi di Stato e di Governo in occasione del *Summit* di Varsavia del luglio 2016, che mira ad accrescere la resilienza degli Alleati ad attacchi *cyber*, attraverso:

- lo sviluppo delle capacità di difesa delle infrastrutture IT nazionali;
- una adeguata allocazione di risorse da parte dei singoli Paesi;
- il rafforzamento della cooperazione e lo scambio di *best practice*;
- la condivisione di informazioni relative a minacce *cyber*;
- una maggiore consapevolezza in merito a pratiche di cd. *cyber hygiene*;
- una migliore formazione sui temi della *cyber defence* delle Forze Alleate;
- la pronta implementazione degli impegni assunti dai Paesi in ambito NATO.

STATO DELLA MINACCIA CIBERNETICA IN ITALIA E POSSIBILI EVOLUZIONI

UNO SGUARDO AL CONTESTO INTERNAZIONALE

La disamina degli eventi *cyber* occorsi a livello internazionale nel 2017 ha portato all'attenzione due principali filoni di minaccia: il primo, riconducibile al *ransomware* (*v. Glossario*) che, mediante *WannaCry*, ha interessato, nel maggio, centinaia di migliaia di computer a livello globale, bloccando l'operatività di ospedali, banche e aziende; il secondo, da ascrivere alle campagne di influenza che, prendendo avvio con la diffusione *online* di informazioni trafugate mediante attacchi *cyber*, hanno mirato a condizionare l'orientamento ed il *sentiment* delle opinioni pubbliche, specie allorquando queste ultime sono state chiamate alle urne. In particolare, tali campagne hanno dimostrato di saper sfruttare, con l'impiego di tecniche sofisticate e di ingenti risorse finanziarie, sia gli attributi fondanti delle democrazie liberali (dalle libertà civili agli strumenti tecnologici più avanzati), sia le divisioni politiche, economiche e sociali dei contesti d'interesse, con l'obiettivo di introdurre, all'interno degli stessi, elementi di destabilizzazione e di minarne la coesione.

AMBITI E ATTORI DELLA MINACCIA

Nel 2017, il dominio cibernetico ha continuato a costituire spazio privilegiato per attività ostili, di diversa matrice, condotte in danno di *target* nazionali – tanto pubblici che privati, con differente livello di strutturazione, a partire dal singolo individuo fino ad arrivare alla più complessa organizzazione istituzionale o aziendale – la cui esposizione alla minaccia è riconducibile alla crescente pervasività degli strumenti di comunicazione elettronica e di digitalizzazione delle informazioni e dei processi.

La continua evoluzione del dominio cibernetico, quindi, nell'ampliare la superficie di attacco, ha parallelamente comportato una pronunciata diversificazione ed un affinamento dei vettori della minaccia. Tattiche, tecniche e procedure si sono caratterizzate, infatti, per diversi livelli di capacità offensiva: dalla negazione di servizio alla violazione di sistemi ICT, attraverso operazioni, spesso silenti, finalizzate a compromettere risorse di cui assumere il controllo, così da acquisire i dati in esse contenute.

A fronte di ciò, il Comparto ha continuato ad assicurare, mediante dedicate manovre informative, la tutela delle infrastrutture critiche e degli *asset* strategici, specie in occasione di eventi di rilevanza internazionale, tenutisi in territorio nazionale (incluso il G7), rispetto ai quali l'attività intelligence ha permesso di prevenire azioni ostili di matrice sia statuale che hacktivista.

Nell'alveo, poi, della tutela del sistema Paese, sono state poste in essere iniziative tese ad individuare possibili criticità nelle infrastrutture di attori produttivi nazionali a protezione del loro *know-how* tecnologico. L'azione svolta ha consentito di rilevare la presenza di vulnerabilità nei sistemi informativi di rilevanti imprese italiane, suscettibili di esporle ad azioni sia di spionaggio digitale, sia miranti a bloccarne i sistemi e, di conseguenza, l'attività.

Il ricorso al ***cyber* spionaggio** ha continuato ad essere appannaggio quasi esclusivo di attori strutturati globali. Questi ultimi, quando hanno colpito *target* pubblici titolari di funzioni critiche, hanno impiegato armi digitali sempre più silenti e persistenti, articolate infrastrutture di comando e controllo, nonché tecniche di offuscamento volte a celare il codice malevolo e le sue funzionalità. Per la realizzazione delle infrastrutture d'attacco (registrazione di domini e servizi di *hosting*) gli attori ostili hanno privilegiato, in linea di continuità con il passato, servizi commerciali che offrono garanzie di anonimato nei pagamenti, accettando transazioni in criptovalute (*v. Glossario*) come i *Bitcoin*.

Tra le tattiche che hanno conosciuto significativa evoluzione, vanno annoverate le *email* di *spear-phishing* (*v. Glossario*), confermatesi quale principale vettore d'attacco. Qui, il dato emergente è costituito dal fatto che – mentre in passato, l'inoculazione del *malware* prevedeva l'interazione con il titolare dell'*account* di posta elettronica (che veniva spinto a cliccare su un *link* o ad accedere ad un allegato infetto) – oggi, la sola apertura dell'*email* è in grado di infettare la postazione colpita in modalità completamente *stealth*.

Di particolare interesse, inoltre, sono risultate le tecniche di *impersonation*, che hanno consentito all'attaccante di acquisire credenziali di accesso a caselle di posta elettronica (sia istituzionali che private), riferibili spesso a figure apicali di aziende e Amministrazioni di rilevanza strategica. Tale tattica – altro tratto caratterizzante del *cyber-espionage* – è stata funzionale sia all'acquisizione di informazioni sensibili, anche per attività controindicate che si svolgono nel mondo reale, sia all'ulteriore propagazione del *malware* tra i diversi *target*. L'attaccante, infatti, ha fatto leva sul *trust* generato nel destinatario dalla ricezione di messaggistica proveniente da mittente noto o, ancorché non noto, di rango istituzionale. Sempre al fine di rendere le *email* credibili, sono stati usati indirizzi di posta elettronica e domini simili a quelli legittimi (cd. *bitsquatting* o *typosquatting*, *v. Glossario*), correlati al contesto professionale della vittima, ovvero analoghi a quelli impiegati da *media*, *email provider* o società, specie dei settori IT e finanziario.

Al furto di credenziali ha fatto seguito, talvolta, la loro pubblicazione *on-line*, spesso sul *dark web* ovvero su siti impiegati per la condivisione di *leak* con il pubblico. Tali modalità, proprie dell'ecosistema hacktivista, sono state adottate sia da *cyber*-criminali in qualità di *proxy* di entità statuali, sia direttamente da quest'ultime, al fine di rendere maggiormente difficoltosa l'*attribution* dell'attività ostile nell'ambito di operazioni cd. *"false flag"* (*v. Glossario*).

Le azioni di spionaggio digitale registrate nel 2017 sono state finalizzate, più che all'acquisizione di *know-how* pregiato e piani industriali delle eccellenze imprenditoriali nazionali, a guadagnare posizioni di forza in sede di negoziazione di accordi di natura politico-strategica ovvero ad agevolare la conduzione di attività di ingerenza nei processi istituzionali, specie nell'ambito dei principali consessi internazionali.

Quanto al ***cyber* terrorismo**, le sconfitte territoriali progressivamente subite dal *Califfato* nella roccaforte siro-irachena hanno costretto l'organizzazione ad implementare una *web-strategy* per mantenere una certa visibilità, funzionale a proseguire, almeno sul piano vir-

tuale, l'opera di proselitismo, radicalizzazione e reclutamento di nuove leve. In quest'ottica, è continuata la diffusione di materiale informativo-propagandistico attraverso strumenti automatizzati (*bot, v. Glossario*), che hanno consentito sia di accelerare e amplificare la disseminazione di notizie rilasciate dai tradizionali *media center* jihadisti, sia di distribuire massivamente *link* che hanno reindirizzato la navigazione verso piattaforme per lo *storage* temporaneo di contenuti elaborati da DAESH o dai suoi simpatizzanti. Un esempio di ricorso a tali metodiche è stata l'offensiva, lanciata il 30 giugno, mediante l'uso di *bot* su un noto servizio di messaggistica istantanea, con cui DAESH avvisava i propri sostenitori che la notizia della fine del *Califfato*, annunciata dalle autorità irachene a seguito della riconquista di Mosul, era da ritenersi falsa.

In generale, gli strumenti impiegati da DAESH (*bot* e *tool* disponibili in rete per attacchi *cyber*) hanno continuato a caratterizzarsi per bassa sofisticazione tecnica e media capacità offensiva.

Con riguardo, infine, alle attività dell'***hacktivism***, esse sono state prevalentemente orientate alle istanze di contestazione politica e sociale (sanità pubblica, tutela ambientale, occupazione e crisi del settore creditizio) assonanti con quelle dell'antagonismo reale, quale forma di sostegno alle manifestazioni di piazza. In tale ambito, emblematico è stato il rilancio delle operazioni *"OpSafePharma"*, che ha interessato, oltre ad Amministrazioni centrali e locali, anche rilevanti gruppi farmaceutici nazionali e non, ed *"OpGreenRights"* che ha riguardato, a dispetto delle motivazioni addotte dall'organizzazione tra cui quella di protesta contro i tagli alla ricerca sulle fonti rinnovabili, pure realtà impegnate nel fotovoltaico ed in altre forme di energia pulita. Ciò, in un contesto ove hanno trovato conferma sia la natura poco sofisticata degli attacchi condotti dal movimento, sia la scelta di *target*, effettuata in base alla presenza di vulnerabilità di immediata sfruttabilità. Il *modus operandi* adottato ha previsto, innanzitutto, attività preliminari di scansione di vulnerabilità (cd. *bug hunting*) per successivi accessi abusivi in modalità *SQL Injection* (*v. Glossario*), finalizzati all'esfiltrazione di dati da piattaforme *web*, resi, poi, di pubblico dominio, o offensive di negazione del servizio (*Distributed Denial of Service*-DDoS, *v. Glossario*).

SERIE STATISTICHE

A completamento dello scenario descrittivo, anche per questa edizione sono state elaborate statistiche relative agli attacchi condotti contro *target* nazionali di rilevanza strategica sotto il profilo della sicurezza nazionale, ancorché non insistenti sul suolo italiano.

Come di consueto, per maggiore completezza e adesione del dato rappresentato rispetto alla realtà fenomenica, l'analisi è stata condotta sulla base degli elementi informativi forniti da AISE ed AISI, dai Servizi Collegati Esteri, dagli organismi internazionali dedicati alla materia cibernetica, nonché dagli altri soggetti che compongono l'architettura.

Imprescindibili esigenze di riservatezza circa l'entità numerica delle minacce rilevate impongono una trasposizione esclusivamente in termini percentuali del volume degli attacchi registrati.

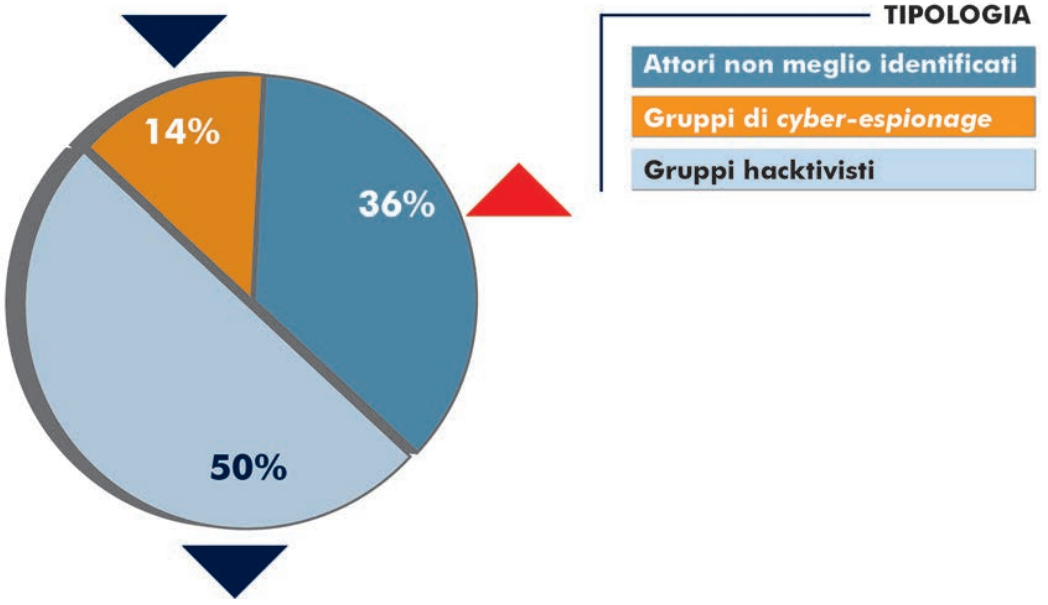
La serie è corredata dai seguenti elementi grafici indicativi dei *trend*, desunti comparando i dati dell'anno di riferimento con quelli del 2016.

▲ Trend in crescita ▼ Trend in diminuzione ▶ Trend stabile

Per quel che concerne la tipologia di **attori ostili**, anche nel 2017 ha trovato conferma il *trend* che vede nei **gruppi hacktivisti** la minaccia più rilevante in termini percentuali, con il 50% degli attacchi a fronte del 14% riferibili a **gruppi di *cyber-espionage***. Entrambe le categorie hanno fatto registrare una flessione (rispettivamente, pari al -2% ed al -5%), a fronte di un aumento dei cd. **"attori non meglio identificati"**, che si sono attestati al 36% delle incursioni *cyber*. Elevato si è mantenuto, infatti, il numero complessivo di eventi per i quali non è stato possibile disporre di elementi univoci in termini di attribuzione e che, pertanto, sono stati inseriti sotto tale categoria.

In merito, poi, ai **gruppi islamisti**, il 2017, a differenza degli anni precedenti, non ha fatto registrate in direzione di *target* italiani azioni così significative da essere prese in considerazione in questa analisi.

ATTACCHI CYBER IN ITALIA IN BASE ALLA TIPOLOGIA DEGLI ATTORI OSTILI
(IN % SUL TOTALE 2017)

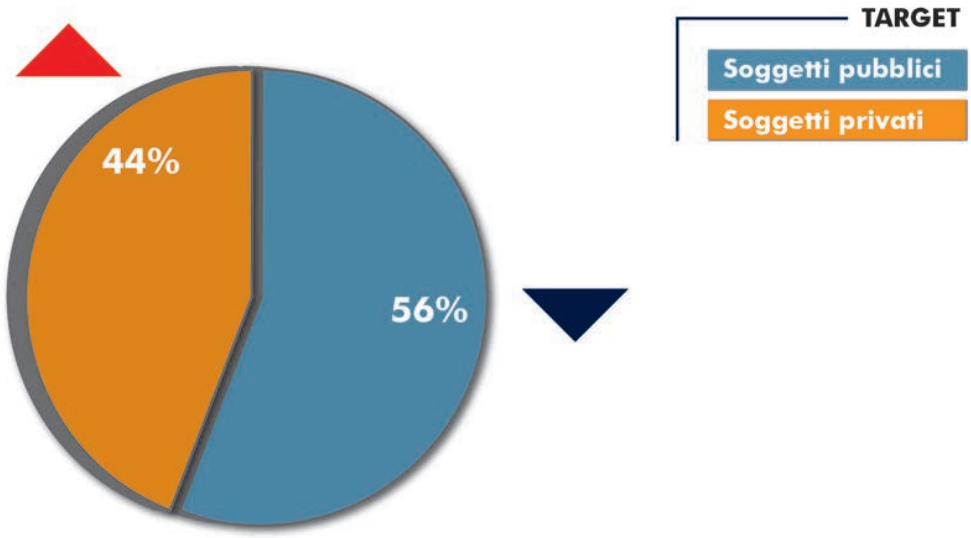


Quanto ai dati in base ai ***target*** è diminuito in maniera rilevante – per la prima volta dal 2015, anno a partire dal quale sono state redatte serie statistiche sulle minacce *cyber* – il divario tra le azioni perpetrate nei confronti di **soggetti pubblici**, che hanno continuato a costituire la maggioranza con il 56%, e quelle in direzione di **soggetti privati**, che hanno

raggiunto il 44%, registrando un aumento di 17 punti percentuali. Sintomo, questo, di una sempre maggiore consapevolezza dei rischi *cyber* e del conseguente aumento delle capacità di rilevazione e di un maggiore *information-sharing*.

Nell'anno di riferimento, inoltre, è venuto meno il dato relativo ai ***target* non meglio identificati o diffusi**, a dimostrazione del fatto che le campagne *cyber* sono state condotte contro obiettivi specifici, anziché in direzione di numeri generalizzati e indistinti di obiettivi.

ATTACCHI *CYBER* IN ITALIA IN BASE ALLA TIPOLOGIA DEI *TARGET*
(IN % SUL TOTALE 2017)



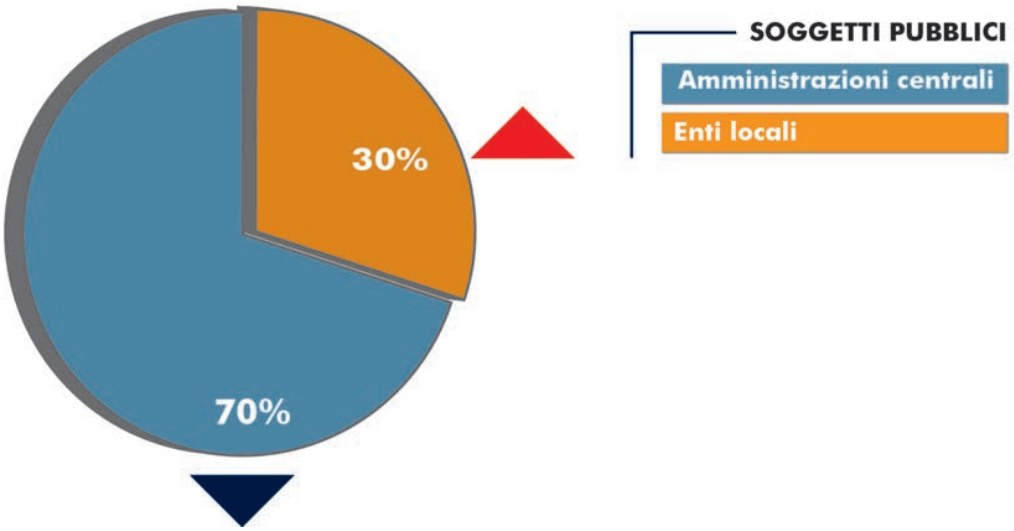
Esplodendo, poi, i dati relativi ai **soggetti pubblici**, si coglie un elemento di novità rispetto agli anni pregressi. Infatti, pur continuando a rilevarsi una netta predominanza delle Amministrazioni centrali (70% degli attacchi *cyber* verso soggetti pubblici) rispetto agli Enti locali (30%), questi ultimi hanno fatto registrare un aumento di 17 punti percentuali rispetto al 2016.

È rimasta invece immutata la differente tipologia di azioni di cui le richiamate categorie sono state vittime, anche in ragione del diverso grado di sensibilità delle informazioni da esse detenute; per tale motivo, le Pubbliche Amministrazioni Centrali-PAC, hanno continuato ad essere *target* privilegiato di attacchi di *cyber*-spionaggio, mentre le Pubbliche Amministrazioni Locali-PAL sono state perlopiù interessate da campagne di attivismo digitale.

Quanto ai **soggetti privati**, il grafico mostra un chiaro incremento degli incidenti registrati da quasi tutti i principali settori, ad eccezione di quello bancario (-11%). È stato rilevato un notevole incremento di eventi che hanno interessato l'industria farmaceutica (+10% rispetto al 2016), obiettivo della campagna *"OpSafePharma"*, di matrice hacktivista. Seguono gli operatori energetici (+4%) e della difesa (+1%).

Attacchi cyber in Italia in base alla tipologia dei target pubblici

(in % sul totale 2017, dati aggregati)

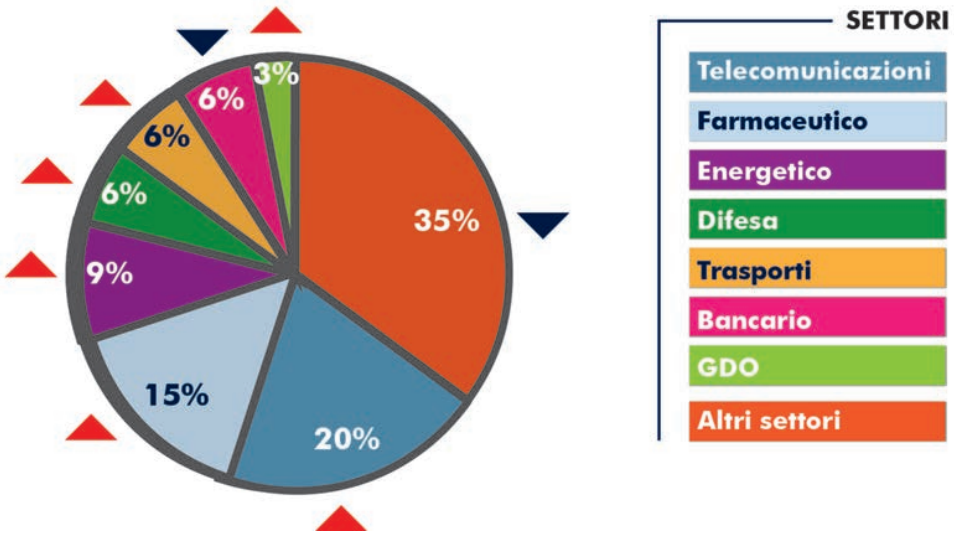


Altro aspetto da evidenziare è il ritorno di attacchi contro i settori delle telecomunicazioni (20%) e dei trasporti (6%) e quelli contro una *"new entry"*, rappresentata dalla grande distribuzione organizzata-GDO (3%).

Sotto la voce "altri settori" (35%) sono state ricomprese aziende diversificate che non assumono, singolarmente considerate, rilevanza sotto il profilo strategico.

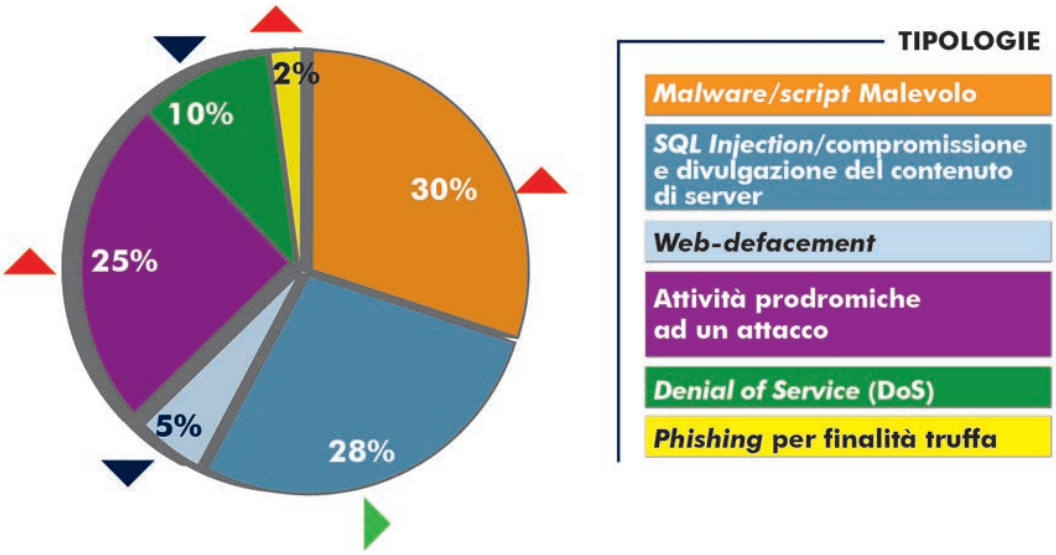
Attacchi cyber in Italia in base alla tipologia dei soggetti privati

target (in % sul totale 2017)



ATTACCHI CYBER IN ITALIA IN BASE ALLA TIPOLOGIA DI ATTACCO IMPIEGATA

(IN % SUL TOTALE 2017)



Con riguardo, infine, alle **tipologie di attacco**, rispetto al 2016 la diffusione di *software* malevolo (*malware*, *v. Glossario*) ha conosciuto un incremento di 19 punti percentuali, attestandosi al 30% degli eventi registrati, benché vi sia stato un sostanziale allineamento con l'*SQL Injection* (28% del totale; stabile rispetto all'anno precedente).

In aumento sono risultate anche le attività prodromiche ad un attacco (25% degli attacchi *cyber*, +2% se confrontato col dato 2016), mentre in diminuzione sono i *Web-defacement* (-8%, *v. Glossario*) ed i *Distributed Denial of Service* (-9%).

Il ricorso al *phishing* (*v. Glossario*) per finalità di truffa (2%) ha interessato in particolare operatori privati di rilevanza strategica, *target*, questi ultimi, di campagne che, attraverso tecniche di *social engineering* (*v. Glossario*), hanno interessato *account email* di personale operante nel settore *Finance*. L'obiettivo è stato quello di ottenere il pagamento di fatture false e/o altri benefici di natura economica, ingannando il destinatario mediante *spoofing* (*v. Glossario*) del mittente.

TREND EVOLUTIVI

Il *cyber* spazio è divenuto, nel tempo, terreno di confronto, se non addirittura di scontro geo-politico tra gli Stati. La disciplina dell'ecosistema che ruota intorno al concetto di "digitale" continua ad essere oggetto di ampio dibattito nei principali consessi internazionali dai quali emerge, in maniera "corale", la necessità di un richiamo al senso di responsabilità degli Stati nello spazio cibernetico, atto ad evitare l'adozione di condotte suscettibili di sfociare in tensioni e conflittualità.

Al fine di scongiurare tale eventualità, una vasta gamma di strumenti – da quelli diplomatici a quelli più prettamente economici – è a disposizione della comunità internazionale, che si è dotata di appositi *toolbox*, come quello relativo alla *"cyber diplomacy"* approvato dall'UE nel mese di ottobre.

L'adozione di tali misure costituisce una significativa presa d'atto dell'esigenza di intervenire nei confronti degli attori statuali ostili – ferme restando le difficoltà della definizione univoca dell'attribuzione degli attacchi – anche laddove gli stessi agiscano mediante l'impiego di *proxy* o secondo modalità tipiche della criminalità informatica e dell'hacktivismo.

In prospettiva, si ritiene possibile un aumento del ricorso, da parte di attori statuali, a modalità operative di offuscamento, anche per conseguire profitti volti a finanziare lo sviluppo di attività sanzionate dalla comunità internazionale.

Al contempo, appare ragionevole ipotizzare la crescita del trend delle minacce ibride. L'impiego di tali strumenti, pur non essendo un fenomeno nuovo, costituisce una realtà sempre più perniciosa, sofisticata e di difficile rilevazione. Gli attacchi di natura ibrida hanno infatti reso più labile la linea di demarcazione tra situazioni caratterizzate da assenza di ostilità e forme di conflittualità diffusa tra gli Stati.

In questo, lo strumento cibernetico è destinato a divenire sempre di più un agevolatore di attività di influenza, realizzate attraverso la manipolazione e la diffusione mirata di informazioni preventivamente acquisite attraverso manovre intrusive nel *cyber*-spazio, così da orientare le opinioni pubbliche, fomentare le tensioni socio-economiche, accrescere l'instabilità politica dei Paesi dell'area occidentale, all'atto dell'adozione di decisioni strategiche, ritenute dall'attore ostile sfavorevoli ai propri interessi.

LE PAROLE DEL *CYBER*

***Advanced Persistent Threat* (APT)**. Minaccia consistente in un attacco mirato, volto ad installare una serie di *malware* all'interno delle reti bersaglio, al fine di riuscire a mantenere attivi i canali impiegati per la fuoriuscita di informazioni pregiate dalle infrastrutture IT del *target*.

Attribution. Termine che identifica l'attribuzione di un attacco *cyber* come, ad esempio, una campagna di *cyber*-spionaggio, ad un determinato attore ostile.

Bitsquatting. Consiste nella registrazione a dominio di un nome molto simile a quello di un dominio noto. La differenza è di solito minima e concepita in maniera tale da non essere graficamente distinguibile dall'utente (ad esempio, la "l" minuscola è spesso sostituita dal numero "1").

Bot. Programmi che sono in grado di riprodurre il comportamento umano *on-line* come, ad esempio, popolare un profilo *social* ed inviare messaggi in una *chat*.

***Confidence Building Measure* (CBM).** Serie di azioni volte a prevenire possibili *escalation* derivanti da operazioni condotte nello spazio cibernetico.

Criptovalute. Valute digitali che si basano sulla crittografia sia per la loro generazione, sia per la convalida delle transazioni.

Crisi cibernetica nazionale. Situazione in cui l'evento assume dimensioni, intensità o natura tali da incidere sulla sicurezza nazionale o da non poter essere fronteggiato dalle singole Amministrazioni competenti in via ordinaria, ma con l'assunzione di decisioni coordinate in sede interministeriale.

***Computer Security Incident Response Team* (CSIRT).** Unità organizzativa deputata a coordinare la risposta ad incidenti informatici, a mitigarne gli effetti ed a prevenire il verificarsi di ulteriori eventi.

***Distributed Denial of Service* (DDoS)**. Attacco DoS lanciato da un gran numero di sistemi compromessi ed infetti (*botnet*), volto a rendere un sistema informatico o una risorsa non disponibile ai legittimi utenti attraverso la saturazione delle risorse ed il sovraccarico delle connessioni di rete dei sistemi *server*.

False flag (operazioni). Si tratta di operazioni, generalmente condotte nello spazio cibernetico ma non solo, poste in essere usando cautele tali da indurre l'avversario in errore circa la reale riconducibilità delle stesse ad uno specifico attore ostile.

Malware. Contrazione di *malicious software*. Programma inserito in un sistema informatico, generalmente in modo clandestino, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo. I *software* malevoli sono divenuti, nel tempo, sempre più sofisticati. Non solo sono adattabili a qualsiasi tipologia di obiettivo, ma sono anche in grado di sfruttare

vulnerabilità non ancora note (cd. *0-day*) per infettare le risorse informatiche dei *target*. Ciò consente a tali *software* di non essere rilevati dai sistemi antivirus e di passare praticamente inosservati. Essi, inoltre, sono in grado di celarsi nell'ambito del sistema-obiettivo, di spostarsi al suo interno, così da poterne effettuare una mappatura e propagare l'infezione. Infine, grazie agli stessi, le informazioni di interesse, prima di essere sottratte, vengono compresse e criptate per celarne l'esfiltrazione con il traffico di rete generato dall'ordinaria attività lavorativa del *target*.

Phishing. Attacco informatico avente, generalmente, l'obiettivo di carpire informazioni sensibili (*userid, password*, numeri di carte di credito, PIN) con l'invio di false *email* generiche a un gran numero di indirizzi. Le *email* sono congegnate per convincere i destinatari ad aprire un allegato o ad accedere a siti *web fake*. Il *phisher* utilizza i dati acquisiti per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Ransomware. *Malware* che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione. I *ransomware* sono, nella maggioranza dei casi, dei *trojan* diffusi tramite siti *web* malevoli o compromessi, ovvero per mezzo della posta elettronica. Questi si presentano come allegati apparentemente innocui (come, ad esempio, file PDF) provenienti da mittenti legittimi (soggetti istituzionali o privati). Tale elemento induce gli ignari utenti ad aprire l'allegato, il quale riporta come oggetto diciture che richiamano fatture, bollette, ingiunzioni di pagamento ed altri oggetti similari.

Social engineering. Arte di manipolare psicologicamente le persone affinché compiano determinate azioni o rivelino informazioni confidenziali, come le credenziali di accesso a sistemi informatici.

Spear-phishing. Attacco informatico di tipo *phishing* condotto contro utenti specifici mediante l'invio di *email* formulate con il fine di carpire informazioni sensibili dal destinatario ovvero di indurlo ad aprire allegati o *link* malevoli.

Spoofing. Manipolazione di dati telematici quali l'indirizzo IP o l'*email* del mittente, così come l'estensione di *file*, tali da farli apparire innocui o, comunque, promananti da soggetti noti o che non generano sospetti.

SQL Injection. Tecnica mirata a colpire applicazioni *web* che si appoggiano su *database* programmati con linguaggio SQL, tramite lo sfruttamento di vulnerabilità quali l'inefficienza dei controlli sui dati ricevuti in *input* e l'inserimento di codice malevolo all'interno delle *query*. Tali attacchi consentono di accedere alle funzioni di amministrazione del sistema oltre che di sottrarre o alterare i dati.

Typosquatting. Vedi la voce *"bitsquatting"*.

Web-defacement. Attacco condotto contro un sito *web* e consistente nel modificare i contenuti dello stesso limitatamente alla *home-page* ovvero includendo anche le sottopagine del sito.