COMMISSIONE IV
DIFESA

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

6.

SEDUTA DI MARTEDÌ 7 GIUGNO 2016

PRESIDENZA DEL PRESIDENTE **FRANCESCO SAVERIO GAROFANI**

INDICE

N. B. Sigle dei gruppi parlamentari: Partito Democratico: PD; MoVimento 5 Stelle: M5S; Forza Italia - Il Popolo della Libertà - Berlusconi Presidente: (FI-PdL); Area Popolare (NCD-UDC): (AP); Sinistra Italiana-Sinistra Ecologia Libertà: SI-SEL; Scelta Civica per l'Italia: (SCpI); Lega Nord e Autonomie - Lega dei Popoli - Noi con Salvini: (LNA); Democrazia Solidale-Centro Democratico: (DeS-CD); Fratelli d'Italia-Alleanza Nazionale: (FdI-AN); Misto: Misto; Misto-Alleanza Liberalpopolare Autonomie ALA-MAIE-Movimento Associativo italiani all'Estero: Misto-ALA-MAIE; Misto-Minoranze Linguistiche: Misto-Min.Ling.; Misto-Partito Socialista Italiano (PSI) - Liberali per l'Italia (PLI): Misto-PSI-PLI; Misto-Alternativa Libera-Possibile: Misto-AL-P; Misto-Conservatori e Riformisti: Misto-CR; Misto-USEI-IDEA (Unione Sudamericana Emigrati Italiani): Misto-USEI-IDEA; Misto-FARE ! - Pri: Misto-FARE ! - Pri.

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE FRANCESCO SAVERIO GAROFANI

La seduta comincia alle 11.30.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche mediante la trasmissione televisiva sul canale satellitare della Camera dei deputati e la trasmissione diretta sulla web-tv della Camera dei deputati.

Audizione della Direttrice generale dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM), dottoressa Rita Forsi, in qualità di Responsabile del CERT Nazionale.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico, l'audizione della Direttrice generale dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM), dottoressa Rita Forsi, Responsabile del CERT nazionale.

Saluto e do il benvenuto alla dottoressa Forsi che ringrazio per la sua presenza. La dottoressa è accompagnata dall'ingegner Sandro Mari, esponente del medesimo Istituto.

Dopo l'intervento della Direttrice generale darò la parola ai colleghi che intendano porre domande o svolgere osservazioni. Successivamente la dottoressa potrà rispondere alle domande. Senza ulteriori indugi do subito la parola alla dottoressa Forsi.

RITA FORSI, *Direttrice generale dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM) e Responsabile del CERT Nazionale*. Buongiorno, presidente e grazie per l'invito e per l'opportunità.

Il tema dell'audizione è sicuramente molto sensibile e importante. Noi, come Istituto superiore delle comunicazioni e delle tecnologie dell'informazione del Ministero dello sviluppo economico, abbiamo in carico lo sviluppo e le attività relative al CERT (*Computer Emergency Response Team*) nazionale. Il CERT è una struttura tecnico-operativa deputata a trattare e a supportare – come vedremo meglio nella presentazione che mi accingo a fare – tutte quelle problematiche relative a minacce, incidenti e attacchi di sicurezza informatica.

Seguirò l'indice riportato nella prima *slide*, quindi, ogni mio elemento o contributo potrà essere ritrovato in modo da rendere un po' più facile seguire tutta la presentazione. Mi accingo a iniziare parlando del contesto europeo, di quello nazionale, di cosa abbiamo fatto in Italia e a quale punto siamo arrivati con il CERT nazionale e, infine, mi soffermerò su qualche sviluppo futuro.

Parlando del contesto europeo, sicuramente dobbiamo fare riferimento al fatto che le tecnologie dell'informazione e delle comunicazioni costituiscono l'elemento portante della crescita economica. Finanza, sanità, energia e trasporti dipendono dal corretto funzionamento di reti e di sistemi informatici. Parallelamente allo sviluppo di nuove tecnologie, anche gli attacchi *cyber* diventano sempre più sofisticati e possono colpire il funzionamento dell'apparato statale o la fornitura dei servizi essenziali per i cittadini, con conseguenti danni econo-

mici e pregiudizio anche alla qualità della vita stessa dei cittadini.

L'Unione europea si confronta con questa problematica ormai da una decina d'anni, quindi noi possiamo partire da un *excursus* che ci mostra i risultati di questa analisi che è stata fatta a livello europeo.

Io parlerei, quindi, dell'ENISA (Agenzia europea per la sicurezza delle reti e dell'informazione) costituita nel 2004 perché già allora l'Unione europea aveva deciso che fosse importante dotarsi di una struttura deputata alla sicurezza delle reti e dell'informazione. L'obiettivo era quello di favorire l'incremento del livello di sicurezza delle reti e dell'informazione nell'Unione europea e, quindi, anche lo sviluppo di una cultura in materia a vantaggio di cittadini, consumatori, imprese e settore pubblico, all'interno dell'Unione europea. L'ENISA agisce come centro di competenza per uno scambio di informazioni e *best practice* fra le istituzioni, le autorità nazionali, le imprese, valutando i rischi attuali e quelli emergenti.

Vorrei ora passare a una sintesi di quella che è stata la presenza europea su questo tema con provvedimenti specifici. Naturalmente farò riferimento anche al noto attacco che nella primavera del 2007 ha colpito l'Estonia e che ha fatto crescere in Europa la consapevolezza dei potenziali rischi e la conseguente necessità di rafforzare le capacità nazionali e il coordinamento a livello europeo. All'inizio, la Commissione europea ha intensificato le attività sulla sicurezza dello spazio *cyber* con una comunicazione del 2009. La tematica di questa comunicazione era quella di rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa da *cyber* attacchi e *cyber* perturbazioni.

Poi, abbiamo avuto nel 2010 l'importante caposaldo dell'Agenda digitale che aveva un capitolo veramente fondamentale e importante, dedicato al *trust and security*. Questo era uno dei *pillar* dell'Agenda digitale.

Successivamente, nel 2011, c'è stata un'altra comunicazione, sempre della Commissione europea, che trattava la realizzazione e le successive tappe verso una sicurezza informatica mondiale (recitava proprio così).

Infine, c'è stata una comunicazione del 2013 che cominciava a essere ancora più stringente, parlando di strategia dell'Unione Europea per la *cyber security* e di un cyberspazio aperto e sicuro – questo era il tema – e, al contempo, attivava la discussione di una proposta di direttiva, recante misure per un livello comune elevato. Ci tengo a sottolineare il termine « elevato » per il livello comune di sicurezza delle reti e dei sistemi informativi dell'Unione europea. Faccio riferimento alla cosiddetta direttiva NIS (*Network and information security*), di cui parleremo più avanti e che è stata approvata dal Consiglio dell'Unione europea lo scorso 17 maggio, anche se era nata già con questa comunicazione.

Nella *slide* denominata « Crescere in sicurezza nell'Unione Europea », sono riportate praticamente le tematiche di ogni atto che ho appena citato.

Facciamo ora un piccolo *assessment* con le parole chiave e soprattutto riferito al fatto che sarebbe impossibile analizzare in dettaglio i contenuti della Commissione. Tuttavia, una delle cose più importanti che emerge da questo tipo di comunicazioni è sicuramente il ruolo dei CERT.

I CERT vengono visti come « catalizzatori nazionali degli interessi e delle capacità delle parti in causa » per realizzare attività di utilità pubblica – come quelle connesse ai sistemi di condivisione delle informazioni e di allarmi destinati ai cittadini, ma anche alle aziende pubbliche e alle piccole e medie imprese – e per impegnarsi attivamente nella cooperazione transnazionale e nello scambio di informazioni.

Nel febbraio 2013, la Commissione europea ha delineato questa strategia e ha preso atto della necessità di assicurare adeguate capacità e un coordinamento efficace. La Commissione ha presentato, quindi, l'ipotesi della direttiva. Nella parte conclusiva del mio intervento dedicherò un po' di spazio allo sviluppo per quanto riguarda il CERT nazionale e relazione con la direttiva.

Le parole chiave, che già delineano grosso modo e per concetti i compiti, sono: preparazione e prevenzione; individuazione e reazione; mitigazione e recupero; cooperazione pubblico-privato, che sarà uno dei temi fondamentali, perché ce ne sono diversi; piani di emergenza; esercitazioni di *cyber security*, quindi di sicurezza informatica, nazionali ed europee; *info sharing*, come elemento trasversale e indispensabile per poter attivare un vero meccanismo dotato di efficacia; un ottimo livello di cooperazione internazionale, altrimenti tutto sarebbe vano.

La strategia europea, per la verità, dava anche delle indicazioni di massima su ruoli e responsabilità. Ho, quindi, preparato anche una *slide*, denominata « Strategia europea: ruoli e responsabilità », in cui si iniziano a vedere come, a livello europeo, vengono identificati i compiti da portare avanti. C'è una sicurezza delle reti e delle informazioni come obiettivo; c'è un'attività di contrasto da realizzare e c'è un'attività essenzialmente di difesa demandata a vari organi che possono ricoprire ruoli di competenze specifiche e specialistiche.

Il livello nazionale prevede, come si vede in basso a sinistra, dei CERT nazionali. Le unità nazionali di lotta al *cyber crime* sono quelle, invece, deputate all'attività di contrasto e alle attività di difesa, che sono facilmente individuabili e con compiti diversi, come è ovvio che sia. Nell'ultima parte a destra si vede un'interazione importante con l'industria, quindi con il mondo del settore privato e il mondo dell'accademia.

Del contesto nazionale, che cosa possiamo dire ? A fronte di numerose sollecitazioni che sono arrivate anche dall'Europa, l'Italia ha colto l'occasione del recepimento della direttiva n. 140 del 2009, che ha modificato il quadro regolamentare in materia di comunicazioni elettroniche, e con il decreto legislativo n. 70 del 2012 ha previsto l'individuazione del CERT nazionale presso il Ministero dello sviluppo economico, al fine di supportare i cittadini e le imprese, avvalendosi delle risorse umane, strumentali e finanziarie disponibili e senza oneri aggiuntivi per il bilancio dello Stato. Successivamente abbiamo avuto il Decreto del Presidente del Consiglio dei ministri del 24 del gennaio 2013. Questo, che ha delineato l'architettura nazionale per la protezione cibernetica e la sicurezza informatica, ha affidato al CERT nazionale la funzione di supporto al tavolo tecnico NISP (Nucleo interministeriale situazione e pianificazione) che agisce come tavolo interministeriale di crisi cibernetica. In caso di crisi, dunque, il CERT nazionale deve praticamente mettersi a disposizione e a supporto di tale importante organo.

Il CERT nazionale è stato affidato all'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione con il Decreto del Presidente del Consiglio dei ministri del 5 dicembre 2103 (quindi, prima al MISE e, poi, direttamente all'Istituto superiore che è una direzione generale del Ministero dello sviluppo economico) che concerne appunto il regolamento di organizzazione del nostro Ministero.

Riguardo ad alcune riflessioni sulle motivazioni per cui il CERT nazionale ha trovato luogo presso l'Istituto superiore, direi che c'era sicuramente un'esperienza in questo organo tecnico-scientifico dell'ex Ministero delle comunicazioni, poi confluito nel Ministero dello sviluppo economico, in termini di esperienza e professionalità nel settore della *cyber security*.

C'era, infatti, già operativo dal 2003, l'OCSI, ovvero l'Organo di certificazione della sicurezza informatica. C'era una partecipazione al *management board* dell'agenzia ENISA dal 2004 e poi, dal 2009, con la rappresentanza governativa, fra l'altro in capo alla mia persona. Inoltre, c'era un'esperienza di esercitazioni di sicurezza informatica a livello europeo e anche a livello nazionale. La prima a livello europeo – lo dico per notizia – è stata svolta nel 2010, quando l'Italia ha partecipato e l'Istituto superiore aveva coordinato un tavolo di lavoro per la partecipazione a questo importante appuntamento.

Per entrare nel cuore dell'argomento e del tema dell'audizione, l'inserimento del CERT nazionale nell'architettura di *cyber security* è riassunto in modo semplice, ma anche molto chiaro nella *slide* denominata

« Il CERT nazionale nell'architettura di cyber security », dove si vedono i tre livelli essenziali di funzionamento che stanno alla base dell'architettura, cioè il livello politico-strategico, il livello di coordinamento e il livello operativo.

Il CERT nazionale si colloca naturalmente nel livello operativo, quindi è bene aggiungere che, nell'architettura generale di *cyber security*, il Nucleo per la sicurezza cibernetica (NSC) ricopre il livello di coordinamento, mentre il Comitato interministeriale per la sicurezza della Repubblica (CISR) ricopre il livello politico-strategico con altri tavoli e altre strutture che sono a sostegno dei veri e propri livelli alti e decisionali.

Il quadro strategico nazionale è una delle risultanze del lavoro di quest'anni, seguiti appunto all'emissione del citato decreto del 24 gennaio 2013. Nel quadro strategico nazionale, gli obiettivi del CERT nazionale vengono ben definiti.

Viene ovviamente posta, fra gli obiettivi del CERT nazionale, la realizzazione della piena operatività, per potenziare ovviamente gli strumenti di rilevazione e di contrasto e i meccanismi di risposta agli incidenti. È importante notare che questo avviene tramite un sistema sicuro e riservato di condivisione delle informazioni.

Il CERT nazionale, inoltre, definisce un modello di comunicazione condiviso con gli altri CERT perché, come ho già accennato, la condivisione, l'*info sharing* e lo scambio di informazioni con altri CERT a livello europeo e internazionale è uno degli *asset* fondamentali. Viene definito anche uno schema di accreditamento al fine di individuare i ruoli, i domini di competenza e i punti di contatto, supportando la costruzione di un'adeguata *community* per la sicurezza nazionale. Pertanto, il fatto che il CERT deve supportare vuol dire che è un anello importante di una catena che funziona, se ben raccordata.

Lo sviluppo del CERT nazionale è sulla base di un modello cooperativo pubblico-privato, che naturalmente dovrà avere come scopo il supporto ai cittadini e alle imprese, tramite iniziative e azioni che possono essere di sensibilizzazione, di prevenzione e di coordinamento delle risposte, non solo su piccoli eventi o piccoli incidenti, ma anche su eventi cibernetici su vasta scala.

L'attivazione di meccanismi di cooperazione, sia nell'ambito del nostro Paese, sia a livello internazionale, compete ancora al CERT nazionale, così come tutti i collegamenti.

Inoltre, c'è lo sviluppo di una piattaforma di coordinamento tecnico funzionale perché è importante che il flusso informativo possa scorrere in modo sicuro e protetto, non solo a livello nazionale, ma anche a livello internazionale.

Passo adesso a declinare, un po' più nel dettaglio, quelle che sono le caratteristiche del CERT nazionale italiano.

La nostra *mission* è quella di supportare i cittadini e le imprese attraverso azioni di sensibilizzazione per la crescita della cultura della sicurezza e di prevenzione, nonché attraverso azioni di prevenzione e di coordinamento della risposta a eventi cibernetici su vasta scala.

Tale *mission* si realizza provvedendo a informare tempestivamente, circa le potenziali minacce informatiche che possono essere veramente dannose e di cui veniamo a conoscenza, e con la cooperazione con istituzioni analoghe a qualsiasi livello e con altri attori pubblici e privati, coinvolti nella sicurezza informatica, promuovendo l'interazione fra questi attori. Inoltre, la nostra *mission* si realizza facilitando la risposta a incidenti informatici su larga scala e, questo, è uno snodo importante. Infine, la nostra *mission* si realizza fornendo il supporto nel processo di soluzione di crisi cibernetica.

Le attività, per poter raggiungere quest'obiettivo, si possono riassumere in tre capisaldi: attività di tipo tecnico-operativo; attività di rapporti con istituzioni e imprese; attività di formazione e di sensibilizzazione.

Definiamo, ancora più in dettaglio, le attività tecnico-operative perché un grande lavoro fatto ha bisogno di essere anche descritto più in dettaglio.

Le operazioni, che vengono condotte giornalmente, si riassumono in un monito-

raggio e in un'analisi di fonti di informazione, in una gestione della piattaforma di *info sharing* che è stata costituita, nella predisposizione di contenuti per il sito *web* – che è fatto essenzialmente di *news*, quindi di notizie molto aggiornate, e di bollettini che sono, invece, notizie più mirate – e di linee guida di varia natura e difficoltà. Una gestione delle segnalazioni viene condotta giornalmente. Vengono attivate e mantenute campagne di informazione e vengono aggiornati i contenuti del sito *web* perché sia un riferimento effettivo anche per i cittadini che non ne avrebbero altri. Inoltre, c'è una gestione e una manutenzione della infrastruttura tecnologica.

Per quanto riguarda i rapporti con le istituzioni e le imprese è stato attivato un tavolo tecnico con gli operatori. Noi lo chiamiamo « tavolo tecnico con gli operatori », ma vedremo bene quali sono in particolare. Si tratta di soggetti privati che sono stati in qualche modo coinvolti dal primo momento dell'attivazione del CERT nazionale. A questo tavolo siedono la maggior parte delle infrastrutture critiche e le più grandi aziende.

Poi, con esse sono stati attivati dei rapporti, sia con i più grandi sia con le piccole e medie imprese, e sono stati fatti accordi di collaborazione specifici. Inoltre, vengono gestiti rapporti con i CERT istituzionali in ambito nazionale e internazionale. A livello nazionale, come vedremo, c'è il CERT della pubblica amministrazione, il CERT Difesa ed altri.

Vengono gestiti i progetti di ricerca in ambito nazionale ed europeo e viene gestita un'attività internazionale di carattere più generale per i rapporti con qualsiasi altro soggetto che si occupi di questa materia.

Poi, ci sono la formazione e la programmazione dei corsi specialistici nonché l'organizzazione di eventi, nei quali siamo in qualche modo obbligati a divulgare la cultura della sicurezza, e l'organizzazione di campagne di sensibilizzazione.

Ecco, le interazioni del CERT nazionale sono riassunte velocemente per l'Italia nella *slide* a pagina 36. Potete vedere il CERT Difesa, il CERT della pubblica amministrazione, il CNAIPIC, le università e gli enti di ricerca, i CERT internazionali e poi quelli che rappresentano il *core constituency*, cioè i cittadini e le imprese.

Per le collaborazioni con il settore pubblico abbiamo protocolli d'intesa come CERT nazionale, quindi come Istituto che sorregge il CERT nazionale, con il settore pubblico, in particolare con l'Agenzia per l'Italia digitale (AgID) e col Ministero della difesa. Abbiamo protocolli d'intesa con università ed enti di ricerca, in particolare con il CNR, con il Consorzio Interuniversitario nazionale per l'informatica (CINI) e con il consorzio GARR che, com'è noto, è la rete italiana dell'università e della ricerca.

La *slide* a pagina 38 mostra alcune immagini per riportare le collaborazioni con il settore privato. Come vedete ci sono operatori di comunicazione elettronica, operatori del settore Energia, Poste italiane. Ci sono *vendor* di sicurezza, associazioni come Anitec, che raggruppa veramente molte decine di imprese ad alto livello, e c'è un accordo con le Assicurazioni Generali, come nuova frontiera, in sostanza, delle problematiche che vengono trattate dal CERT nazionale.

Con il settore privato l'Associazione Anitec raggruppa circa 50 aziende del settore *Information technology*. Il Consorzio ABI Lab, invece, raggruppa 160 banche associate; poi, ci sono anche contatti con singole banche. Inoltre, c'è il tavolo tecnico permanente, di cui ho già parlato che vede un contatto diretto della maggior parte di queste aziende con la funzionalità del CERT nazionale.

La *slide* a pagina 39 dà l'impressione visiva dei rapporti già attivati con tutti i CERT dell'Unione europea. Come vedete, ormai ne mancano veramente pochissimi perché siamo oltre la ventina e giornalmente ci scambiamo molte informazioni.

In particolare, ci tengo a sottolineare il rapporto con il CERT EU, il CERT delle istituzioni europee, che per noi è un riferimento molto importante. Esiste un rapporto diretto che ha consentito l'instaurarsi di relazioni fiduciarie essenziali per abilitare lo scambio di informazioni sensibili. Un'intensa attività di cooperazione è stata

avviata anche con i CERT di: Austria; Belgio; Bulgaria; Croazia; Germania; Irlanda; Finlandia; Francia; Ungheria; Repubblica Ceca; Lituania; Lettonia; Lussemburgo; Olanda; Polonia; Portogallo; Regno Unito; Romania; Spagna; Slovacchia e Svezia.

Tra l'altro, questa cooperazione è stata sperimentata – questo è un altro dato fondamentale – dal CERT nazionale, anche durante le esercitazioni paneuropee, organizzate dall'agenzia ENISA, e in particolare durante la Cyber Europe 2014. Adesso, è in corso la fase tecnica dell'esercitazione Cyber Europe 2016, che vede il CERT nazionale impegnato a risolvere problematiche tecniche.

La *slide* a pagina 40 si riferisce, invece, ai rapporti attivati con alcuni dei CERT internazionali. Teniamo moltissimo ovviamente al CERT degli Stati Uniti d'America, al CERT del Brasile e cerchiamo di attivare rapporti fiduciari perché questo è lo spirito che guida ogni tipo di cooperazione fra i CERT. Infatti è importante attivare relazioni fiduciarie perché anche la condivisione delle informazioni sia più efficace possibile.

Passo adesso a parlare dei sistemi di accreditamento. Il *Trusted introducer* è appunto un servizio offerto dall'associazione che ha l'obiettivo di favorire e rendere efficace la cooperazione fra i CERT pubblici e privati, alimentando una rete di fiducia con servizi specializzati aggiuntivi, per aumentare la capacità di analisi e la capacità di informazione anche alle nostre *costituency* nazionali.

L'accreditamento presso questo soggetto segue un altro riconoscimento ottenuto dalla Carnegie Mellon, l'università americana che deve autorizzare l'utilizzo del marchio CERT. Questo marchio, infatti, è stato registrato da questa università nella quale fu realizzato il primo CERT. Adesso sono in corso azioni per il conseguimento dell'ulteriore certificazione presso il FIRST *(Forum of Incident Response and Security Teams)*.

Passo ad alcuni dettagli e mi avvio alla conclusione in modo da poter, poi, essere disponibile per qualsiasi richiesta.

Mi preme dare alcune informazioni sulle tipologie e sui volumi delle attività svolte nello scorso anno e nei primi quattro mesi dell'anno in corso che abbiamo ritenuto più significative, anche se devo dire e ricordare che il CERT nazionale è nato a giugno del 2014, quindi, tutti questi dati sono raccolti e disponibili presso di noi. I più significativi per quanto riguarda i *trend* di crescita credo che siano quelli che sto per dare.

In particolare mi soffermerò sulle attività di maggior peso, originate dalla collaborazione con i CERT internazionali, e poi dal centro Anti-Botnet. Il centro Anti-Botnet è un'ulteriore realizzazione, attivata presso l'Istituto superiore e nata nell'ambito del progetto europeo Advanced Cyber Defence Center (ACDC). Infine, concluderò con una breve panoramica sulle campagne informative, sia preventive che reattive, che sono state realizzate, che sono campagne destinate a operatori e a *internet service provider* in primo luogo.

Le attività quotidiane del CERT nazionale prevedono, appunto perché il CERT è l'unico punto di contatto internazionale, la ricezione di informazioni e relative minacce e vulnerabilità riscontrate in rete da parte degli omologhi colleghi dei CERT europei e internazionali.

Che cosa dobbiamo fare su queste segnalazioni ? Dobbiamo verificare la segnalazione, storicizzare l'informazione per eventuali correlazioni con incidenti analoghi e interfacciarci con i soggetti italiani eventualmente coinvolti che, tipicamente, sono operatori e *internet service provider* che poi forniscono il servizio agli utenti finali.

Alcuni flussi sono ormai consolidati. Per esempio, il CERT EU fornisce, fra le altre informazioni relative a indicatori di compromissione rilevati dai propri *stakeholder*, dati di particolare interesse per l'aggiornamento dei sistemi perimetrali di difesa dell'organizzazione. Il CERT nazionale provvede alla loro immediata diffusione ai soggetti italiani, con i quali sono stati stipulati gli accordi di collaborazione, e agli altri CERT istituzionali italiani, quindi c'è una

rete ben coesa di condivisione delle informazioni.

Con molti CERT internazionali, principalmente europei, sono inoltre avviati già altri meccanismi di comunicazione periodica, tipicamente settimanale, ma a volte anche giornaliera, relativa a compromissioni particolari. Il CERT nazionale, in questo caso, si fa carico di verificare la segnalazione, di allertare ancora prontamente gli operatori e gli *internet service provider*, perché si facciano a loro volta promotori di azioni informative ai loro clienti finali colpiti da queste problematiche.

Attualmente, sono oltre 500 i soggetti, tra operatori e *internet service provider* di varia dimensione, contattati dal CERT nazionale nel corso del tempo, con una copertura di oltre il 95 per cento dello spazio di indirizzamento italiano. Direi che questo è uno dei risultati più importanti e anche di grande spessore e impegno, conseguiti dal CERT nazionale.

A titolo di esempio, posso dirvi che il CERT tedesco (CERT-Bund) ha fornito indicazioni relative a compromissioni legate, per esempio, al famigerato *malware*, noto come « Ebury », particolarmente pericoloso in quanto consente all'attaccante di acquisire il controllo completo della macchina compromessa. Grazie all'azione informativa del CERT nazionale nei confronti degli operatori coinvolti, il numero di infezioni si è ridotto, fino quasi ad annullarsi.

Analoghe informazioni sono state diffuse relativamente a infezioni di tipo *botnet* ovvero alle reti di computer infetti (« *botnet* » significa appunto questo), per lo più appartenenti a ignari cittadini. Si tratta di *computer* comandati a distanza da centri di comando e controllo per scopi illegali. Il danno potenziale che le *botnet* possono causare le rende una delle principali fonti di reddito illegale su *internet*.

In particolare, alcune informazioni relative a Ramnit, che è un'altra *botnet* smantellata dall'Interpol nel febbraio 2015 e che continua ancora a far sentire i suoi effetti, oppure a Mumblehard, un'altra pericolosa *botnet*, sono state disseminate ai soggetti interessati, grazie all'attività di *info sharing* internazionale del nostro CERT.

A queste si vanno a sommare le numerose segnalazioni in costante aumento – dato degno di nota – e relative a compromissioni di singole macchine sul territorio nazionale che ospitano, per esempio, pagine di *phishing*, fenomeno rilevato dal CERT nazionale appunto in aumento.

Abbiamo anche un contributo importante, come vedete dalla *slide* a pagina 43 che si riferisce in particolare al progetto ACDC. Si notano alcuni dati significativi, come il numero di eventi raccolti durante il giorno e provenienti da tutto il mondo oppure la piattaforma, relativa a questo progetto (quanti eventi è riuscita in qualche modo raccogliere dal 2015). C'è un dato interessante anche per il primo quadrimestre del 2016: il numero dei *report* inviati nel 2015 è di 4.300, mentre è di circa 1.600 già nel primo quadrimestre 2016; quindi, come si può notare, si tratta di numeri molto interessanti.

Passerei adesso alla questione delle campagne informative perché si tratta di uno dei compiti fondamentali del CERT nazionale. Nell'ambito delle proprie attività di monitoraggio, il CERT nazionale ha avviato un certo numero di campagne informative. Inoltre, tramite anche accordi con terze parti affidabili, è in possesso di informazioni relative a vulnerabilità o compromissioni di macchine appartenenti a reti nazionali.

Questo è uno snodo importante perché la raccolta di informazioni può provenire da molte fonti. La cosa importante è che queste fonti siano affidabili. Inoltre, il fatto che il CERT nazionale sia inserito in questa rete di accreditamento, di cui ho parlato prima, fa sì che aumenti il numero delle fonti che possono fornire informazioni importanti.

Le campagne si dividono in due grandi categorie: quelle preventive, che sono relative a configurazioni scorrette di macchine o comunque a vulnerabilità riscontrabili in rete con semplici procedure d'interrogazione; oppure quelle reattive, che sono relative a compromissioni vere e proprie ri-

levabili tipicamente attraverso misure di traffico anomalo.

Il CERT nazionale ha pertanto ritenuto utile, dopo un'attenta analisi dei dati rilevati, di inoltrare periodicamente questa informazione agli oltre 500 operatori.

Le campagne preventive hanno riguardato principalmente, tanto per dare qualche dato tecnico, protocolli aperti all'esterno, dove si utilizzavano gli scopi malevoli, per esempio, attacchi di DDoS (*Distributed Denial of Service*) che hanno l'obiettivo di determinare un fuori servizio delle macchine colpite. In questo caso, l'obiettivo è quello di evitare che le macchine italiane possano essere utilizzate come mezzo per attacchi di questo tipo a terze parti, siano esse italiane o meno. Quindi, la gestione di questo tipo di fenomeno ha molti aspetti che vengono curati dal CERT nazionale.

In altri casi, l'apertura impropria di protocolli all'esterno, sconsigliata dalle migliori pratiche internazionali, rappresenta un rischio vero e proprio per l'integrità della macchina stessa. Stiamo ricevendo numerosi riscontri da parte degli operatori e degli amministratori di rete che ci testimoniano l'utilità del servizio che stiamo loro fornendo.

Per quanto riguarda le campagne reattive, anch'esse avviate dal 2015, posso dirvi che queste si sono arricchite nel corso del tempo di nuove fonti informative affidabili e hanno riguardato siti *web* o singole macchine compromesse.

In particolare, le compromissioni più ricorrenti sono quelle relative a *botnet* note o dal *target* specifico, come Cutwail, Kelihos, Asprox e Lethic, che sono *botnet* utilizzate per inviare *spam* di vario genere, in molti casi vettori di *phishing* o di altro *malware* più specifico, per esempio, per il furto di credenziali nel settore bancario.

Altro tema molto sensibile è quello delle azioni di sensibilizzazione condotte dal CERT nazionale sulla diffusione del *ransomware*, perché il *ransomware* è riconosciuto da tutti come una delle minacce più pericolose del momento attuale. Il fenomeno è drammaticamente in crescita e colpisce indifferentemente vari tipi di utenza. La soluzione più efficace è la prevenzione, cui aggiungerei anche la formazione, in modo che i soggetti siano sempre più preparati. Quindi azioni di sensibilizzazione e informazione possono migliorare la prevenzione.

Vorrei fare una piccola osservazione. Fra le molte *news* pubblicate sul sito *web* del CERT nazionale, circa 40 sono dedicate al *ransomware* e alle numerose varianti perché, come è noto, questo *malware* si replica, cambiando natura, con una velocità impressionante.

Ultimamente, è stata pubblicata anche una linea guida dedicata a questo tema e ispirata a principi di semplicità che ne consentano un utilizzo efficace anche da parte della generalità dei cittadini. La guida ha lo scopo di fornire informazioni essenziali sulle caratteristiche di tale famigerata categoria di *malware*, sulle sue varianti, sulle modalità di diffusione e soprattutto – questo è lo scopo del sito *web* – sulle opportune contromisure da prendere e sui comportamenti consigliati da tenere, al fine di prevenire la possibilità di cadere vittima del *malware*.

Mi avvio davvero alla conclusione con alcuni degli ultimi sviluppi operativi, sui quali il CERT si misurerà. In particolare, mi riferisco alla recente approvazione della direttiva NIS e a certe iniziative che abbiamo recentemente attivato anche in ambito G7. Lo dico solo per esemplificare come gli impegni del CERT nazionale, in termini di cultura e in termini di azione, si aprano man mano che aumenta la capacità operativa.

Per quanto riguarda la proposta di direttiva NIS, il suo studio è durato tre anni. La formale approvazione è stata raggiunta solo lo scorso 17 maggio. Adesso, ne attendiamo la pubblicazione nella *Gazzetta Ufficiale*.

Come inciderà la nuova direttiva sul panorama attuale ? Le nuove disposizioni prevedono, fra l'altro, l'adozione di misure di sicurezza e l'obbligo di notifica degli incidenti significativi per gli operatori di servizi essenziali. Questo è un punto molto importante e interessante che è stato oggetto di un lungo dibattito.

I settori interessati dalla nuova normativa sono: quelli dell'energia, quindi elettricità il settore dell'*oil and gas*; i trasporti (aereo marittimo, stradale e ferroviario); il settore bancario e infrastrutture dei mercati finanziari, quindi gli istituti di credito e gli operatori dei servizi di *trading*; il settore della salute, con ospedali e cliniche private; il settore idrico, con i fornitori di servizi di acqua per il consumo umano; le infrastrutture digitali, *internet exchange point*, *domain name system*, *service provider*, *top level domain registrered*, quindi tutto il settore specialistico che rappresenta un punto veramente sensibile e delicato nel panorama delle tecnologie dell'informazione e degli accessi alla rete internet.

Scendendo maggiormente nel dettaglio, la cooperazione fra i CERT, altro caposaldo della nuova direttiva, prevede l'armonizzazione delle procedure operative dei diversi centri, allo scopo di abilitare un efficace scambio di informazioni su minacce incidenti, attraverso l'utilizzo di strumenti opportuni. L'aspetto di rilievo sul quale il CERT nazionale si è già dovuto confrontare riguarda la cooperazione nella gestione della risposta agli incidenti di natura transfrontaliera. Sul punto la direttiva NIS imporrà l'adozione di misure sempre più efficaci.

I requisiti di base che verranno stabiliti – già previsti per i CERT – sono di tipo tecnico e organizzativo, oltre che di base, e permettono di creare e di partecipare in modo sempre più efficace alla rete dei CERT. Tra questi, si segnalano la disponibilità dei servizi di comunicazione ridondanti, la sicurezza fisica dell'infrastruttura logistica e la continuità operativa H24. Un ulteriore requisito raccomandato dalla direttiva è la disponibilità di risorse umane e materiali per la partecipazione alla rete di cooperazione internazionale.

La nuova normativa definisce, fra l'altro, anche i compiti dei CERT, che sono la cooperazione con il settore privato, il monitoraggio degli incidenti, l'emissione di preallarme, l'intervento in caso di incidente, l'analisi dinamica dei rischi e degli incidenti e la partecipazione alla rete dei CERT. Lo sottolineo ancora una volta perché questa è una raccomandazione importante della nuova direttiva.

Ancora, è prevista la promozione di prassi comuni o standardizzate per il trattamento degli incidenti e dei rischi. Si tratta – apro una parentesi – di un compito che ci stiamo dando ormai anche nelle esercitazioni di sicurezza informatica.

Poi c'è la promozione di procedure standard per l'adozione di sistemi di classificazione degli incidenti, dei rischi e delle informazioni, perché anche su questo, quanto più saremo capaci di migliorare la capacità di intenderci sulla tipologia dell'incidente, sulla tipologia del rischio, sulla gravità e sulla leggibilità delle informazioni, tanto migliore sarà l'efficacia dell'azione di ogni singolo CERT e della rete in generale.

Infine, vorrei precisare che l'Unione europea ha avviato un progetto con il fine di supportare la realizzazione di una piattaforma (*core service platform*) per l'implementazione di meccanismi di cooperazione che incrementeranno la capacità dei CERT europei in termini di scambio di informazioni. Il progetto trova fondamento nella citata direttiva NIS e rientra in un più vasto programma avviato dalla Commissione europea e denominato « *Connecting Europe Facility* », in modo semplicistico. Tale programma ha l'obiettivo di uniformare le dotazioni di reti e infrastrutture degli Stati membri nei settori di telecomunicazioni, energia e trasporti. Il CERT nazionale partecipa al progetto ed è membro del *governance board* per la realizzazione del *core service platform*.

Termino con un'informazione relativa all'azione portata avanti in ambito G7 perché il tema della *cyber security* è entrato prepotentemente anche nell'agenda dei lavori del G7 Energia.

La dipendenza sempre maggiore delle reti energetiche dalle tecnologie dell'informazione e della comunicazione ha evidenziato come la sicurezza energetica, anche nello spazio informatico, debba diventare un impegno trasversale che si traduce nella necessità di una stretta cooperazione per mettere a fattor comune le conoscenze tecniche, le migliori pratiche e le informa-

zioni; sempre con lo stesso obiettivo di fronteggiare in modo più consapevole e coordinato i rischi e gli attacchi di natura informatica.

In tal senso, una più stretta collaborazione fra i CERT dei Paesi del G7 rappresenta un importante obiettivo da conseguire nel breve termine e sono già state poste le basi per la creazione di un profilo tecnico *cyber* in gruppi di lavoro dei Paesi appartenenti al G7.

Da questo punto di vista, è stata avviata un'ulteriore sfida che sicuramente comporterà dell'altro impegno, ma anche un altro elemento – speriamo – di sicurezza negli altri settori. Ho citato anche l'ICT, di *default*, ma devo dire che non possono esistere a questo punto famiglie che rimangono escluse, vista l'informatizzazione nonché la globalizzazione delle informazioni.

Mi fermerei qui e vi ringrazio dell'attenzione.

PRESIDENTE. Grazie a lei, dottoressa Forsi, per questa articolata relazione che ha proposto alla Commissione.

Do la parola ai colleghi che intendono intervenire per porre quesiti o formulare osservazioni.

MASSIMO ARTINI. Grazie, dottoressa Forsi. Sono rimasto molto colpito dalla presentazione che ha fatto perché ci sono molti spunti che fanno vedere un'evoluzione assai positiva del lavoro che sta svolgendo il CERT nazionale. Avrei, ma la evito al Presidente e ai colleghi, una montagna di domande che sono più prettamente di curiosità personale e che riservo per un momento diverso. Tuttavia, le chiedo uno spunto che è più di visione rispetto a questo argomento.

Lei ci ha dato una serie di spunti rispetto alle ultime direttive, anche da un punto di vista europeo e di capacità di saper sopportare un carico di lavoro che riguarda la scoperta o comunque la prevenzione di determinati tipi di problemi.

Le faccio due domande. In primo luogo cosa suggerirebbe, rispetto alla normativa attuale, per promuovere quel coordinamento tra i CERT e per promuovere quella capacità di prevenzione, di scoperta e di formazione ? L'altra domanda si riferisce al punto fondamentale costituito dai servizi ridondanti e risorse umane e materiali. Ebbene, vorrei – lei ha la consapevolezza dello stato attuale, almeno per quanto riguarda il Ministero dello sviluppo economico – comprendere quale sarebbe l'impatto finanziario necessario per avere un livello che sia soddisfacente per le vostre aspettative.

Lo chiedo perché il punto è comprendere dove si può arrivare, che tipo di lavoro si vuol fare e quanto sarebbe l'impatto finanziario per le casse dello Stato. A mio modesto parere, questo è un percorso che va seguito e fatto in ogni caso. Sarebbe quindi importante avere la consapevolezza, come decisori – almeno per quanto riguarda la parte di stanziamenti, non parlo di come investirli –, perché il ragionamento è comprendere qual è l'impatto finanziario, almeno nella parte più civile. Poi, ritengo che anche il coordinamento con i servizi di *intelligence* e di difesa sia necessario perché alcuni settori sono coperti da un livello di classifica completamente diverso.

Siccome vedo, anche rispetto ad analisi fatte in passato, che c'è stato un forte incremento del lavoro da parte del CERT nazionale – soprattutto con riguardo ai dati di prevenzione e ne sono veramente molto felice – le chiedo se mi può dare un'idea di quanto potrebbe essere l'ammontare delle risorse economiche necessarie. Grazie.

DINO SECCO. Vorrei fare una domanda ad integrazione dell'intervento del collega Artini.

La relazione egregiamente ha delineato un quadro delle attività e delle collaborazioni. Per questo tipo di lavoro ho alcune curiosità. Quante persone compongono la struttura ? Quella attuale è sufficiente ? Vorrei anche sapere quali sono le collaborazioni esterne, con enti o società private, per questa attività che viene svolta.

PRESIDENTE. Se non ci sono altre richieste, do la parola alla dottoressa Forsi per la replica.

RITA FORSI, *Direttrice generale dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM) e Responsabile del CERT Nazionale*. Faccio riferimento alla prima domanda dell'onorevole Artini.

Il lavoro che si presenta è notevole, non lo nascondiamo. Infatti, l'abbiamo evidenziato e direttamente collegato alla capacità che giornalmente viene maturata perché più si lavora e più si intravedono possibilità e capacità da raggiungere.

Lei ha parlato di che cosa potrebbe essere suggerito per favorire il coordinamento dei CERT. Io farei riferimento a un'iniziativa che l'Italia aveva adottato nel semestre di presidenza europea.

Noi avevamo attivato, come Italia, la prima riunione dei CERT nazionali e governativi europei. Tale riunione si è svolta a Venezia l'8 luglio 2014. Quest'iniziativa aveva lo scopo di far conoscere le persone che lavorano direttamente in ogni CERT per creare un coordinamento efficace, ma soprattutto basato sul rapporto fiduciario e di conoscenza personale.

Questo è un percorso che è stato riconosciuto come molto valido dalla Commissione europea ed è stato gestito appunto dalla presidenza italiana in collaborazione con la Commissione stessa e con l'ENISA. Si tratta di un percorso – ripeto – che è stato riconosciuto, a livello di Commissione europea come molto importante, tant'è che è stato sempre replicato, per ogni ulteriore semestre che si è succeduto. Quindi, questo percorso è sicuramente il primo obiettivo da continuare a coltivare, ossia il rapporto fiduciario e di conoscenza personale con i soggetti che fanno lo stesso lavoro in omologhe strutture.

Questo è valido per migliorare l'affidabilità. Poi, naturalmente, la stessa direttiva NIS pone degli obblighi e impone di raggiungere altri risultati nei termini di una piattaforma che possa essere sempre più efficace a livello europeo, come si vedeva in una delle ultime *slide* che ho presentato.

L'Italia partecipa a questo *governance board* e intende farsi parte attiva per confermare la necessità di un coordinamento efficace fra questi CERT.

I CERT sono di diversa natura. Poi, magari passerò la parola mio collaboratore che, essendo un referente tecnico del CERT nazionale e un nostro collaboratore presente su alcune di queste realtà anche a livello europeo, può aggiungere qualche elemento di dettaglio da questo punto di vista.

Volevo soltanto dire che il fatto di avere varie tipologie di CERT in ogni Paese, anche europeo, ci ha imposto un grande lavoro – che abbiamo fatto volentieri – di conoscerci e riconoscerci con le strutture omologhe per attivare quei meccanismi che portassero allo stesso risultato, a partire anche da strutture che, pur essendo omologhe, sono un po' diverse.

Da un DNA diverso, si voleva arrivare a uno stesso risultato perché la condivisione delle informazioni e la tipologia di classificazione che la NIS ci imporrà ci chiederanno di parlare sempre più lo stesso linguaggio. Quindi questo sarà il percorso da effettuare per migliorare in sostanza il coordinamento dei CERT, ossia: i rapporti fiduciari, la conoscenza della materia, gli scambi interpersonali e la consuetudine a scambi e rapporti attraverso mezzi affidabili e sicuri che garantiscano l'efficacia delle comunicazioni e soprattutto – non l'ho detto, ma mi fa piacere dirlo ora – la tempestività dell'azione.

Aggiungo che il fatto che ogni nazione ha comunque strutture diverse per raggiungere sia il settore pubblico sia quello privato.

Per quanto riguarda l'altra domanda dell'onorevole Artini, vorrei dire che, se avessi questa capacità, ne sarei molto contenta, ma non sono in grado di rispondere con precisione per un motivo.

Voglio premettere a questo che il fatto di raggiungere certi obiettivi, secondo me, non deve essere visto come un obbligo a carico di un singolo soggetto, bensì a carico di una *community* ben funzionante. In Italia abbiamo una *community* stabilita dal decreto del 24 gennaio 2013 e abbiamo un sistema di responsabilità distribuite, quindi ognuno ha dei compiti; in particolare, il Ministero dello sviluppo economico ha il compito del CERT nazionale. Tuttavia, con

gli esempi che ho fatto degli accordi di collaborazione a livello pubblico e a livello privato, in effetti c'è questo problema di come, a partire da risorse sicuramente scarse, raggiungere degli obiettivi accettabili e poi sempre migliori.

Dal punto di vista della partenza, questo era stato possibile – lo ripeto volentieri – perché c'era un *know-how* di partenza. L'Istituto superiore delle comunicazioni è un organo di tipo tecnico con personale tecnico, quindi è stata fatta la scelta di coinvolgere il più possibile il personale a disposizione.

Naturalmente, le problematiche che si è trovato ad affrontare il CERT nazionale hanno richiesto sempre più specializzazione, quindi questo sarà un percorso continuo, anche di formazione degli stessi tecnici e dello stesso personale del CERT nazionale.

Noi abbiamo deciso di intraprendere anche delle sinergie, per esempio, con il Consiglio nazionale delle ricerche e con il GARR per quanto riguarda la rete della ricerca, che ha un *know-how* elevato in termini di sicurezza informatica e di tecnologie abilitanti per quanto riguarda anche l'organizzazione logistica delle strutture che servono.

Soprattutto, abbiamo un ottimo rapporto di collaborazione tecnico con il CNR e con la parte che riguarda la sicurezza dell'*information technology* del CNR. Grazie a questa collaborazione, riusciamo al momento a superare quelle limitazioni che potrebbero essere una difficoltà a garantire un orario o un altro.

In questo modo, con certe strutture e certi meccanismi di risorse all'interno del nostro Ministero che sono stati tutti utilizzati, al momento è stato possibile raggiungere questi risultati. I numeri sono sinceramente importanti.

Per il futuro ovviamente serviranno degli investimenti. Su questo, mi sento di dire che è un po' difficile cercare di individuare bene le cifre che servono e il numero delle persone perché dipende dal modello che vogliamo adottare. Ovviamente, un modello che funzioni H24, con grande disponibilità, che può prevedere disponibilità a viaggiare o altro, comporterebbe numeri superiori. Noi siamo sulla decina. L'assetto è variabile appunto perché io cerco di impegnare tutto il mio personale.

Non ho portato una *slide* organizzativa, ma si può recuperare dal decreto di riorganizzazione del Ministero dello sviluppo economico, per capire che il CERT nazionale è *a latere* della direzione per poter beneficiare di tutte le collaborazioni con le divisioni all'interno dell'Istituto superiore. Questa è stata la scelta finora effettuata. Vedremo se sarà riconfermata o meno.

Certamente, per lo sviluppo futuro, se vogliamo potenziare, posso solo dire che un certo investimento serve. Al momento, noi supportiamo molte iniziative con azioni di ricerca, distribuendo il peso sugli altri capisaldi che noi abbiamo. Concordo, tuttavia, sul fatto che per avanzare servano comunque degli investimenti.

Tali investimenti dovranno essere in qualche modo misurati sia per il personale sia per le risorse sia per le collaborazioni.

Al momento, i progetti di ricerca ci stanno aiutando molto – questo mi sento di dirlo – e abbiamo appena vinto anche un altro progetto di ricerca a livello europeo.

Inoltre, stiamo seguendo molto l'eCall e, soprattutto, seguiamo anche un'altra iniziativa che è la costituzione di una associazione pubblico-privato a livello europeo che si richiama alla sigla *Contractual public-private partnerships* e che è un partenariato pubblico-privato che dovrà sostenere l'azione di ogni singolo Stato e, poi, a livello europeo prevederà la costituzione di un'associazione pubblico-privato che sarà la controparte della Commissione europea, soprattutto per quanto riguarda i progetti di Horizon 2020. In base a quello ci sarà una forte interazione con i *topics* dell'eCall successive che verranno fatte, perché l'Italia sta lavorando molto su questo. Ovviamente anche il CERT nazionale potrebbe beneficiare di certi impegni che magari potremmo riuscire a portare a casa in modo favorevole.

La cosa importante è, a nostro avviso, quella di proseguire con un'apertura della ricerca di fonti di finanziamento che sia

anche rispondente alle nuove esigenze, perché molti sono i profili nuovi ed emergenti.

La domanda dell'onorevole Secco riguarda i rapporti con il settore privato. La costruzione di quel partenariato è stata il nostro argomento principale, toccato fin dall'inizio.

Le audizioni fatte prima dell'avvio del CERT nazionale, in realtà prevedevano anche una sinergia ancora più stretta. Poi, anche su richiesta di alcuni soggetti, è stato suggerito e previsto che il CERT nazionale fosse gestito esclusivamente da personale della pubblica amministrazione.

Questo in qualche modo ha « penalizzato », fin dal primo momento forse, le potenzialità. Abbiamo, però, cercato di arricchirlo e di superare questa difficoltà con la costituzione di un tavolo tecnico permanente. Faccio riferimento a quegli accordi di collaborazione di cui parlavo nella presentazione. Abbiamo deciso appunto di attivare, fin da subito, un tavolo tecnico permanente con gli operatori, con cui con modalità sicure ci scambiamo informazioni e che si riunisce periodicamente. Quindi il supporto che arriva al CERT nazionale dai soggetti privati adesso è veramente in crescita e in aumento, specialmente per quanto riguarda alcuni settori particolari.

È un po' più complicato il rapporto con alcuni settori nei quali la concorrenza è molto attiva fra i vari soggetti, per cui la condivisione di informazioni viene vista come un elemento non sempre positivo. Da questo punto di vista, si cerca di ovviare a questa situazione con un rapporto diretto tra il CERT nazionale e il singolo soggetto, per cui abbiamo dato questa disponibilità in modo tale da aumentare il clima di fiducia e arrivare a portare quei contributi che effettivamente possono essere utili.

Ci tengo a ribadire il ruolo del CERT. Il CERT è un *hub* ed è un unico *focal point* nazionale che raccoglie, dall'Italia verso l'estero e dall'estero verso l'Italia, ragione per cui quanto più siamo efficaci ed efficienti in questo tipo di contribuzione verso gli altri colleghi, tanto più ci aspettiamo di ricevere in un clima di fiducia costruito.

Non so se ho risposto alla sua domanda, altrimenti posso aggiungere dell'altro.

DINO SECCO. Io intendevo riferirmi ad un altro aspetto: siccome questa è un'attività estremamente specifica, complicata e professionale, volevo sapere se voi avete tutta la professionalità interna e tutti i macchinari che servono per dare risposte o avete bisogno anche di strutture esterne soprattutto per alcuni servizi.

RITA FORSI, *Direttrice generale dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM) e Responsabile del CERT Nazionale*. Per quanto riguarda la funzionalità, a oggi il CERT nazionale ha le strutture che servono. Che cosa è prevedibile per il futuro ? Il futuro probabilmente ci porterà un aumento indescrivibile del numero dei dati che dovremmo trattare, quindi dovremo veramente valutare il potenziamento di questi nostri sistemi e lo stiamo appunto facendo.

Parallelamente, è molto interessante la possibilità – nella risposta appunto che le sto per dare – di fare cenno alla necessità di aumentare sempre la nostra capacità delle analisi e delle verifiche tecniche, prima dell'utilizzo e dell'invio di certe informazioni. La capacità di analisi e di correlazione naturalmente può avvenire sia internamente al CERT sia in collaborazione con gli organi di Polizia, con gli organi dell'*intelligence* e con lo stesso CERT della pubblica amministrazione, quindi con tutti gli altri organi che hanno comunque dei profili di particolare importanza.

Ci tengo a dire appunto che questa necessità di correlazione dovrà vedere comunque un approfondimento di natura tecnica non indifferente. Noi, su questo, come Istituto superiore, abbiamo una tradizione di studio e di ricerca e faremo certamente la nostra parte, ma, da questo punto di vista, io vedo favorevolmente un'interlocuzione, un dialogo e un'apertura totale. Non a caso avevo citato anche la collaborazione con il CINI e con il laboratorio nazionale di *cyber security*. In particolare, con alcune università sono già attivi scambi effettivi e scambi efficaci di discussioni tecniche su particolari tipi di *malware* e su particolari caratteristiche tecniche perché, in quella fase, veramente ognuno

potrebbe portare il proprio contributo anche per l'attività del CERT nazionale.

Ecco, se s'immagina un mondo in cui tutto deve essere fatto solo e soltanto entro il CERT nazionale, allora è una previsione di ipotesi – per ritornare alla domanda dell'onorevole Artini – perché, altrimenti, se riusciamo a far parte di una *community* dalla quale possano arrivare contributi specialistici, ancorché non classificati e certamente di natura non delicata, secondo me la *community* può avere uno sviluppo anche globale in modo tale che poi ne beneficino tutte le componenti che partecipano all'architettura nazionale, che può essere questa o può essere diversa, però è il principio di come si vuole affrontare questo discorso.

Da questi primi due anni di lavoro abbiamo capito che il coinvolgimento massimo è un elemento fondamentale perché, quanti più soggetti sono consapevoli, tanto più possiamo avere dei contributi effettivi. Mi riferisco a contributi al sistema contributi e alla creazione di una cultura di sicurezza e di protezione.

Cambiano anche dentro il nostro Ministero, come vediamo giornalmente, le percezioni delle pericolosità dei virus informatici. Anche il personale del nostro Ministero è tutto sommato, come dico sempre, costituito da cittadini comuni, quindi più riusciamo a far avere questa consapevolezza, più riusciamo a colpire i nostri obiettivi, ossia quelli che non solo ci siamo posti, ma anche quelli che ci vengono posti dalle normative nazionali e internazionali.

Siamo in una comunità globale e non possiamo non accorgerci che ogni anello deve essere molto saldo e che la debolezza di un anello fa la debolezza della catena generale, come spesso sentiamo dire. Dobbiamo tendere a migliorare totalmente e globalmente, come società e come nazione.

PRESIDENTE. Ringrazio moltissimo la dottoressa Forsi per gli elementi e le informazioni che ha portato nella sua relazione e nelle sue risposte, nonché per la presentazione informatica che ci ha illustrato, di cui autorizzo la pubblicazione in allegato al resoconto stenografico dell'audizione odierna *(vedi allegato)*. La consideriamo a disposizione per eventuali ulteriori richieste, anche in forma scritta, e per chiarimenti che potrebbero essere richiesti dai colleghi deputati.

Dichiaro conclusa l'audizione.

La seduta termina alle 12.45.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI
ESTENSORE DEL PROCESSO VERBALE

DOTT. RENZO DICKMANN

Licenziato per la stampa
il 14 settembre 2016

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

MINISTERO DELLO SVILUPPO ECONOMICO

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Audizione
Commissione Difesa
Camera dei Deputati

Roma, 7 giugno 2016

MINISTERO DELLO SVILUPPO ECONOMICO

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Indice

- **Il Contesto Europeo**
- **Il Contesto Nazionale**
- **Il CERT Nazionale**
  - **Mission, Organizzazione**
  - **Attività**
  - **Collaborazione settore pubblico, privato, Accademia e Enti di ricerca**
  - **Interazioni a livello nazionale e con i CERT internazionali**
  - **Dati sulle attività ed esempi**
- **Alcuni nuovi sviluppi**
  - **Direttiva «Network and Information Security»**
  - **G7**

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Il Contesto Europeo

enisa

MINISTERO DELLO SVILUPPO ECONOMICO

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

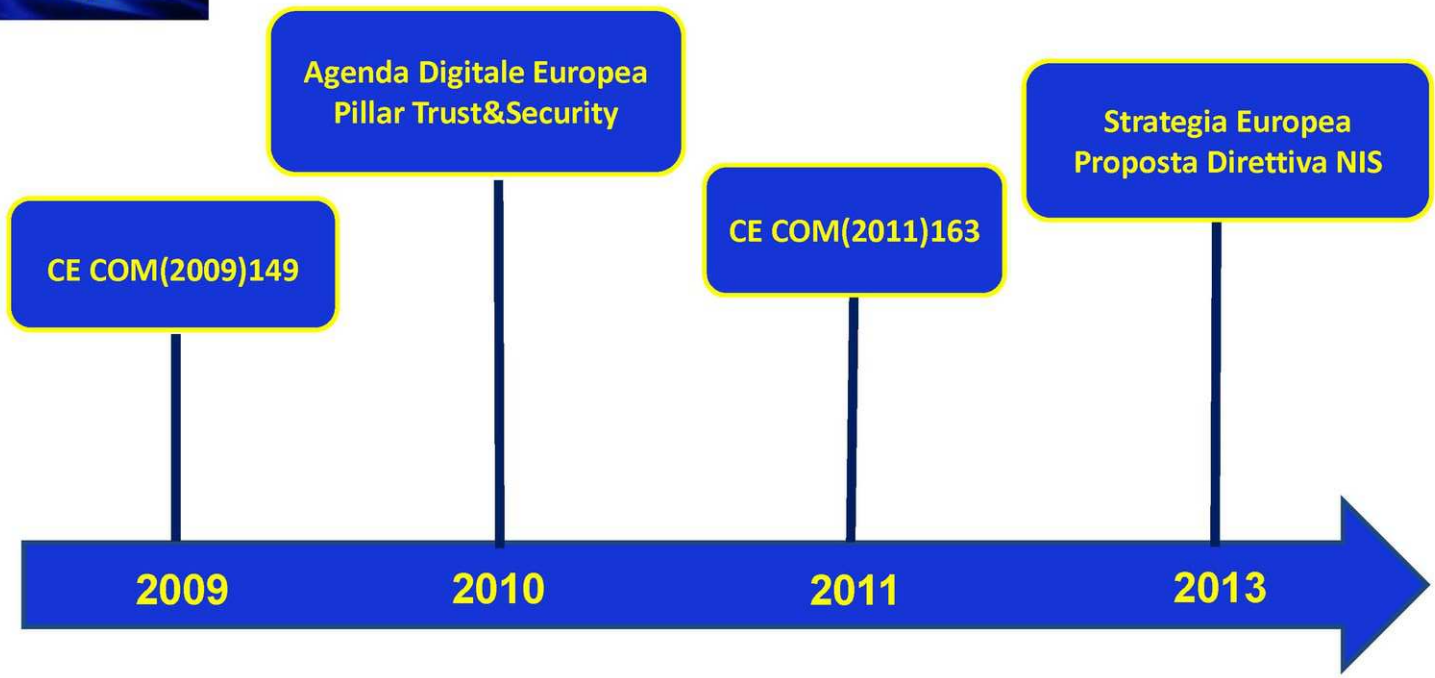
ENISA - European Union Agency for Network and Information Security

- Costituita nel 2004 per assicurare un **elevato livello di sicurezza delle reti e dell'informazione nell'UE** nonché di sviluppare una **cultura in materia di sicurezza delle reti e dell'informazione** a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico nell'Unione europea

- Agisce come **piattaforma di scambio di informazioni e best practice** tra le istituzioni UE, le autorità nazionali e le imprese

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione
CERT nazionale Italia

Il contesto europeo: Timeline



MINISTERO DELLO SVILUPPO ECONOMICO

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Crescere in sicurezza nell'UE

- COM (2009) 149 - Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai cyber attacchi e dalle cyber perturbazioni
- COM (2010) 245 - Agenda Digitale Europea - Pillar Trust and Security
- COM (2011) 163 - Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale
- Strategia dell'Unione europea per la Cybersecurity: un ciberspazio aperto e sicuro
- COM(2013) 48 - POPOSTA DI DIRETTIVA: misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Le parole chiave nell'UE

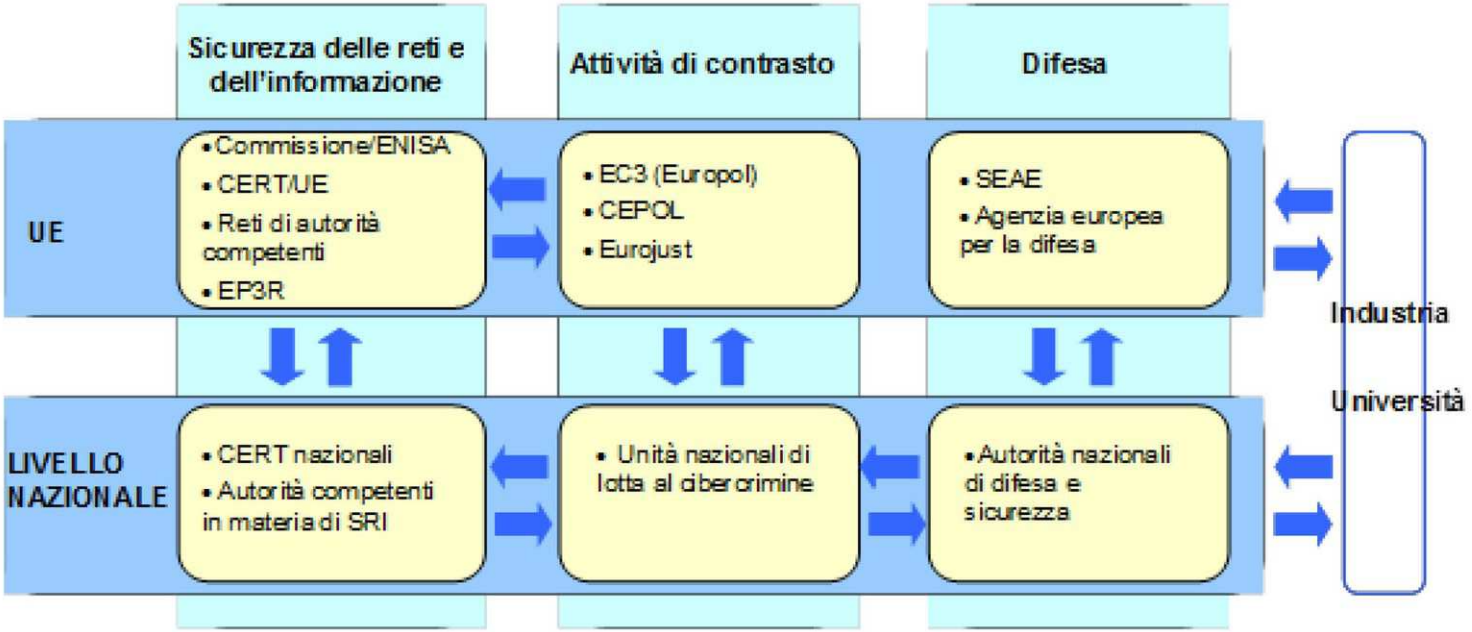
- Preparazione e prevenzione
- Individuazione e reazione
- Mitigazione e recupero
- Cooperazione pubblico-privato
- Piani di emergenza
- Esercitazioni nazionali ed europee
- Infosharing
- Cooperazione internazionale

CERT

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Strategia europea: ruoli e responsabilità



MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Il contesto nazionale

Normativa di riferimento

MINISTERO DELLO SVILUPPO ECONOMICO

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

CERT nazionale: riferimenti normativi

D. Lgs. 70/2012

Individuazione del CERT Nazionale presso il Ministero dello Sviluppo Economico

DPCM 24 Gennaio 2013

IL CERT Nazionale supporta il tavolo interministeriale di crisi cibernetica

DPCM 158 /2013

Il CERT Nazionale è affidato all' Istituto Superiore CTI

28 Maggio 2012 — 24 Gennaio 2013 — 5 dicembre 2013

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Il CERT Nazionale presso il MiSE – ISCTI
Motivazioni

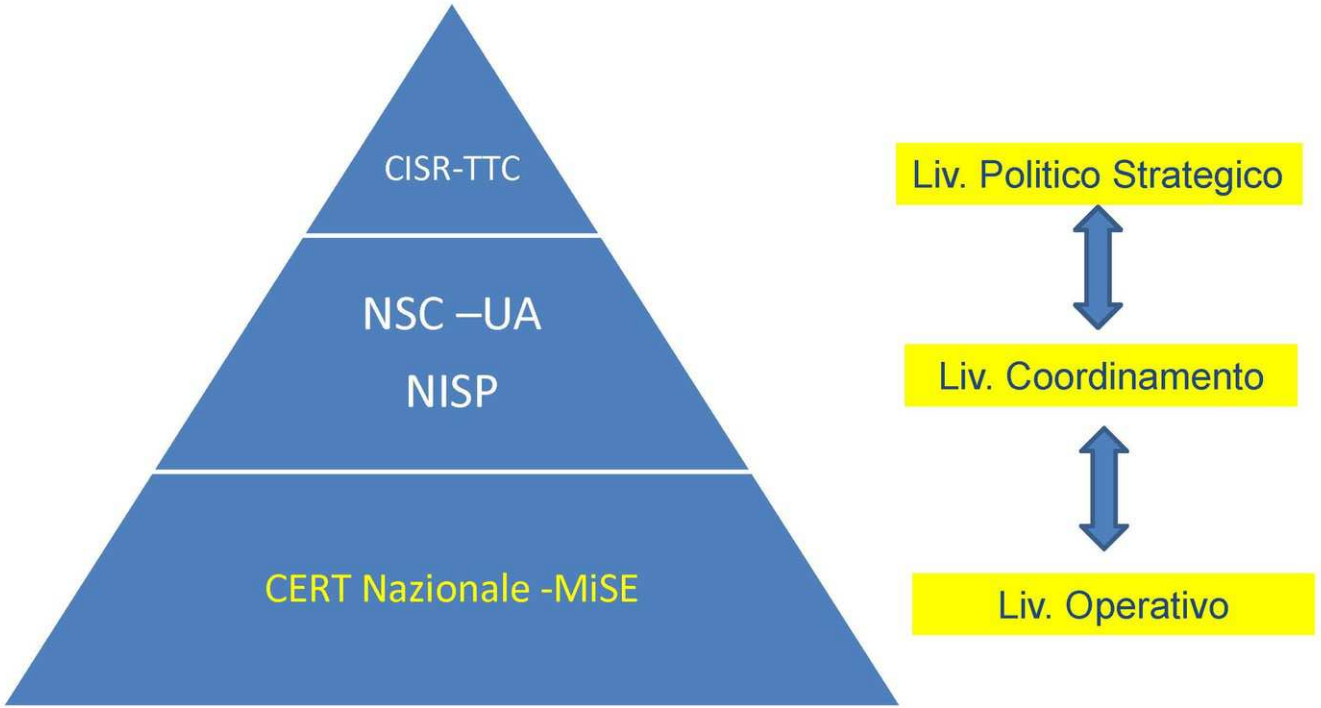
- Esperienze e professionalità nel settore della cyber security
- Organismo di certificazione della sicurezza informatica OCSI
- Partecipazione al MB dell'Agenzia ENISA dal 2004
- Esercitazioni di sicurezza informatica europee e nazionali

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Il CERT Nazionale nell'Architettura di cyber security

Presidente del Consiglio dei Ministri



QSN: Obiettivi del CERT Nazionale

- Realizzazione della **piena operatività del CERT nazionale** per potenziare gli strumenti di rilevazione e contrasto delle minacce ed i meccanismi di risposta agli incidenti, tramite un sistema sicuro e riservato di condivisione delle informazioni
- Il CERT nazionale definisce un **modello di comunicazione condiviso con gli altri CERT** ed uno schema di accreditamento al fine di individuare ruoli, domini di competenza e punti di contatto supportando la costruzione di un'adeguata *community per la sicurezza nazionale*
- Sviluppo del CERT nazionale sulla base di un **modello cooperativo pubblico-privato** finalizzato a supportare cittadini e imprese tramite azioni di sensibilizzazione, di prevenzione e di coordinamento della risposta ad eventi cibernetici su vasta scala
- Attivazione di **meccanismi di cooperazione in ambito nazionale e internazionale**, individuando nel CERT nazionale le funzioni di collegamento con altri CERT pubblici e privati operanti sul territorio e di interfaccia verso il CERT europeo e verso i CERT di altri Stati
- Sviluppo di una **piattaforma di coordinamento tecnico e funzionale** tra tutti i CERT esistenti che permetta il flusso informativo necessario all'attività di prevenzione e risposta

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

IL CERT Nazionale

- **Mission**
- **Organizzazione**
- **Attività**
- **Collaborazione settore pubblico, privato, Accademia e Enti di ricerca**
- **Relazioni con i CERT internazionali**

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

CERT Nazionale

Mission

Supportare cittadini e imprese attraverso azioni di **sensibilizzazione** per la crescita della cultura della sicurezza, di **prevenzione** e di **coordinamento** della risposta ad eventi cibernetici su vasta scala

Fornire informazioni tempestive su potenziali minacce informatiche che possano recare danno a imprese e cittadini

Cooperare con istituzioni analoghe, nazionali ed internazionali, e con altri attori pubblici e privati coinvolti nella sicurezza informatica promuovendo la loro interazione

Facilitare la risposta ad incidenti informatici su larga scala

Fornire supporto nel processo di soluzione di crisi cibernetica


MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione
CERT nazionale Italia
Attività del CERT Nazionale
• Tecnico-operative
• Rapporti con Istituzioni e Imprese
• Formazione e sensibilizzazione
13/06/2016
15

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione
CERT nazionale Italia

Attività tecnico – operative

- Monitoraggio e analisi di fonti di informazione
- Gestione della piattaforma di infosharing
- Predisposizione di contenuti per il sito web (news, bollettini e linee guida)
- Gestione delle segnalazioni
- Campagne di informazione
- Aggiornamento dei contenuti del sito web
- Gestione e manutenzione dell'infrastruttura tecnologica

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Rapporti con Istituzioni e Imprese

- Gestione Tavolo Tecnico operatori
- Rapporti con le Imprese
- Accordi di collaborazione
- Rapporti con CERT istituzionali in ambito nazionale ed internazionale
- Progetti di ricerca in ambito nazionale ed europeo
- Attività internazionale

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione
CERT nazionale Italia

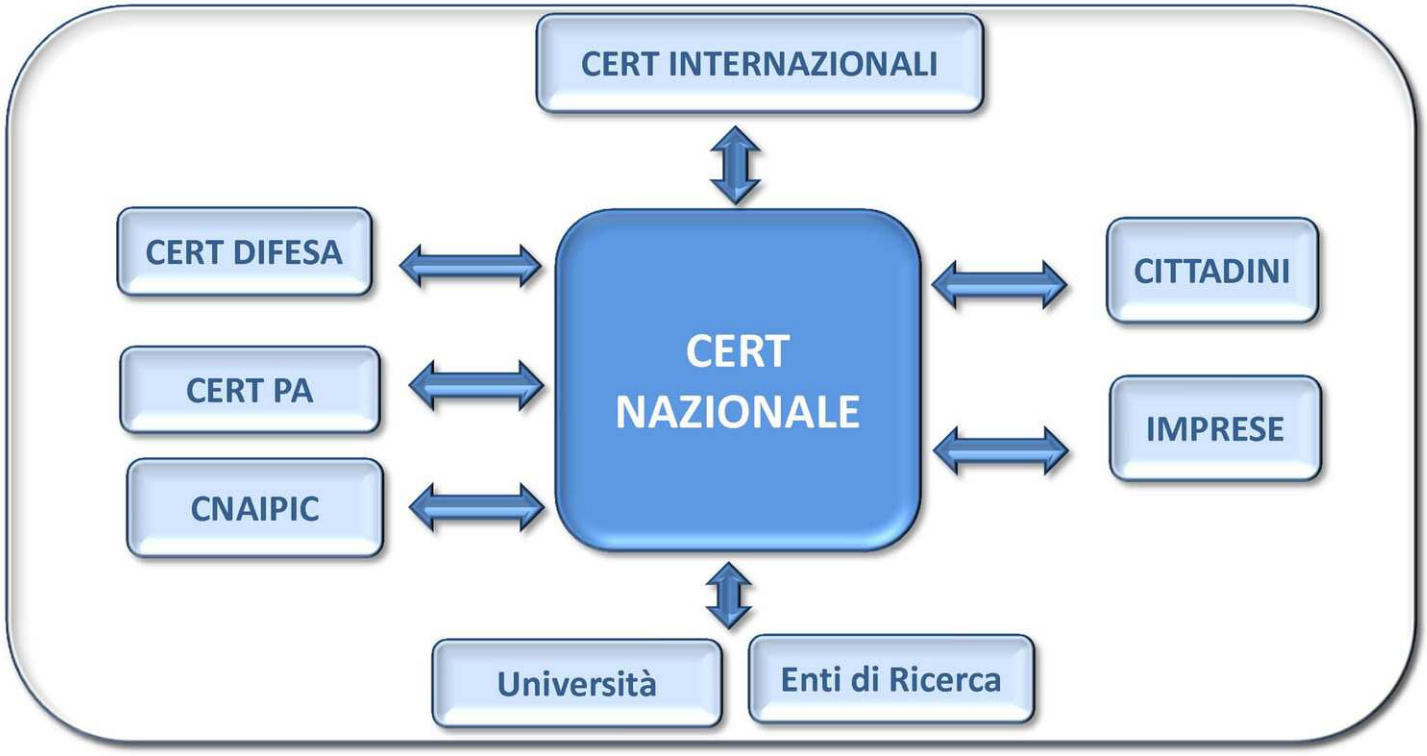
Formazione e sensibilizzazione

- Programmazione corsi specialistici sulle materie della sicurezza informatica
- Organizzazione di eventi per l'incremento della cultura della sicurezza
- Organizzazione di campagne di sensibilizzazione rivolte a cittadini e imprese

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Le interazioni del CERT



Collaborazioni con il settore pubblico

Protocolli d'intesa con il settore pubblico

- Agenzia per l'Italia Digitale – **AgID**
- Ministero della Difesa

Protocolli d'intesa con Università e Enti di Ricerca

- Centro nazionale Ricerche - **CNR**
- Consorzio Interuniversitario Nazionale per l' Informatica – **CINI**
- Consorzio **GARR** - Rete Italiana dell'Università e della Ricerca

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Collaborazioni con il settore privato

Accordi SETTORE PRIVATO

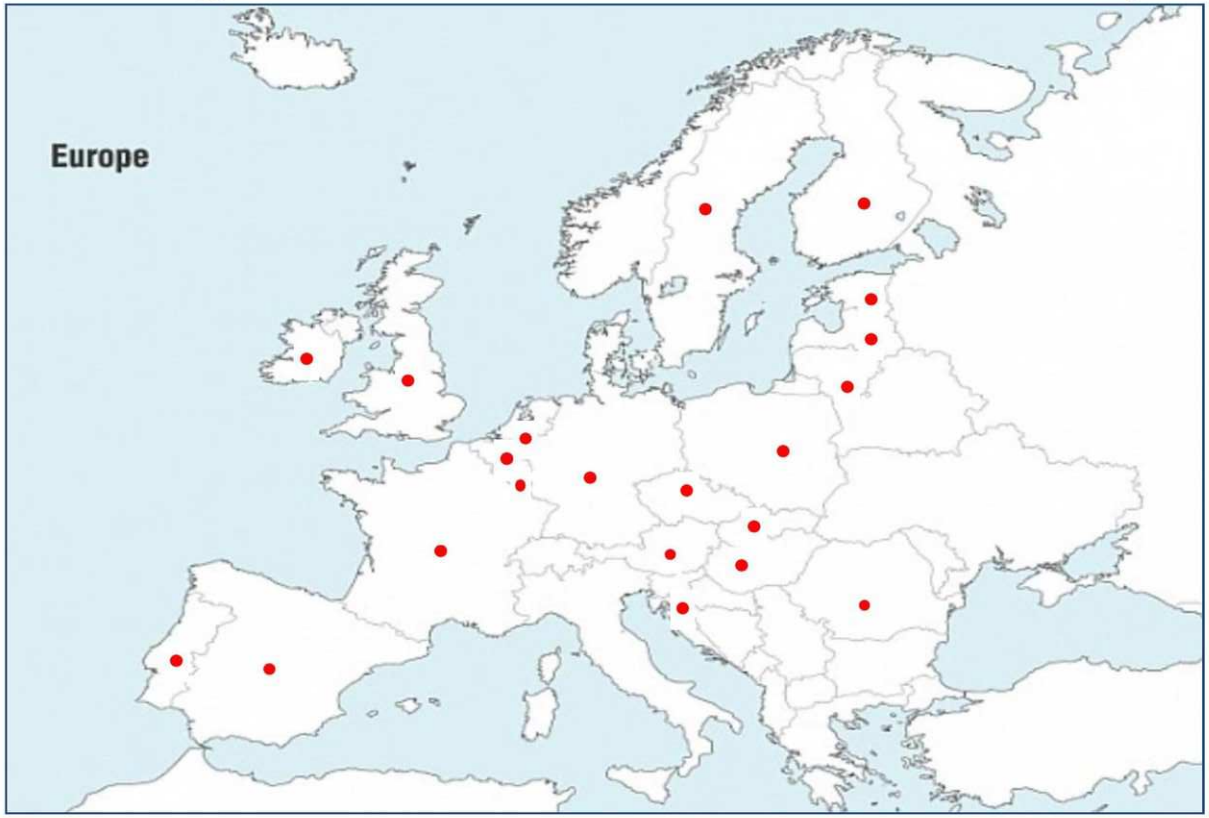
SNAM
TIM
ERG
ABI Lab Tecnologia utile
Posteitaliane
Terna
Symantec
FASTWEB
vodafone
ANITEC ASSOCIAZIONE NAZIONALE INDUSTRIE INFORMATICA, TELECOMUNICAZIONI ED ELETTRONICA DI CONSUMO
GENERALI
WIND
enel
3
Microsoft

MINISTERO DELLO SVILUPPO ECONOMICO

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Infosharing con i CERT dell'Unione Europea



MINISTERO DELLO SVILUPPO ECONOMICO

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Infosharing con CERT extra-UE

Cert Australia

cert.br 15 anos — Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

US-CERT — United States Computer Emergency Readiness Team

CERT-IL

JPCERT CC® — Japan Computer Emergency Response Team Coordination Center — JPCERTコーディネーションセンター

Communications Authority of Kenya

Sri Lanka CERT|CC

CuCERT — Equipo de Respuesta a Incidentes Computacionales de Cuba

Government of Canada / Gouvernement du Canada — Canada

certim — Handling Computer Security Incidents

RU-CERT

MyCERT — Malaysia Computer Emergency Response Team

Equipo de Respuestas ante Emergencias Cibernéticas

BTK — Bilgi Teknolojileri ve İletişim Kurumu

TN CERT — Coordination Center

CERT-UA — Computer Emergency Response Team of Ukraine

MINISTERO DELLO SVILUPPO ECONOMICO

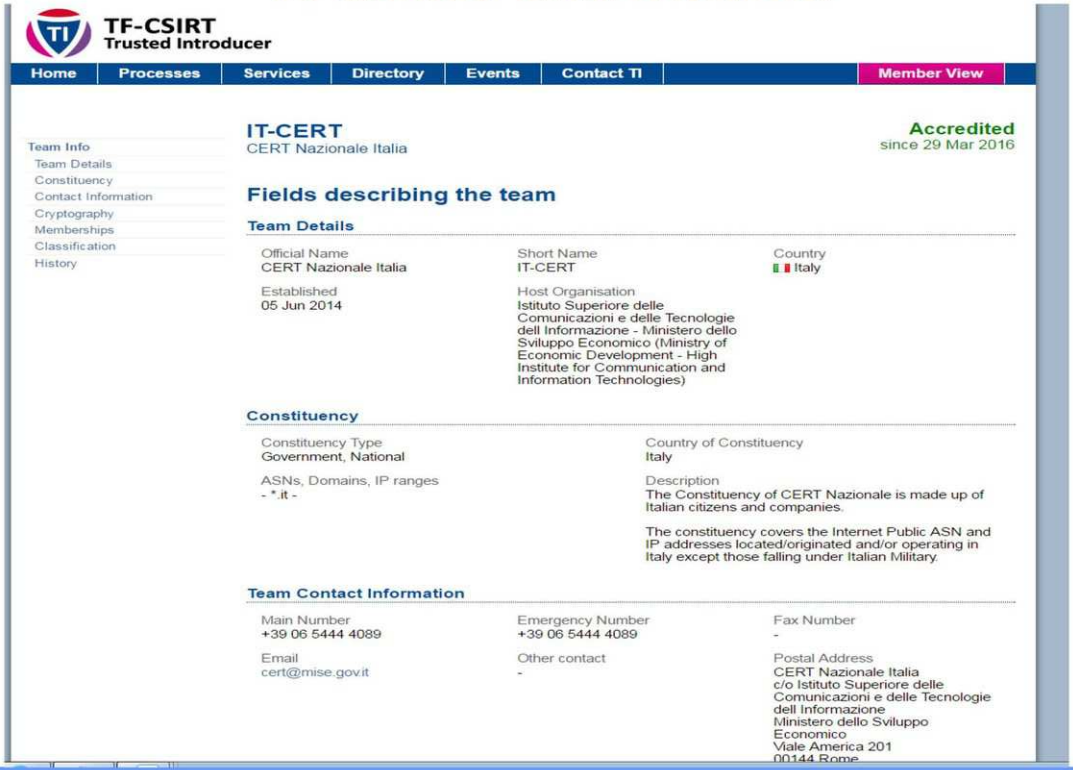
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

TF-CSIRT Trusted Introducer

Certificazione

Trusted Introducer



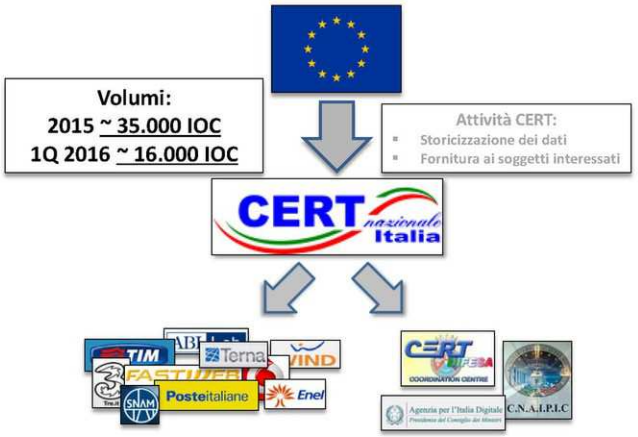
MINISTERO DELLO SVILUPPO ECONOMICO

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

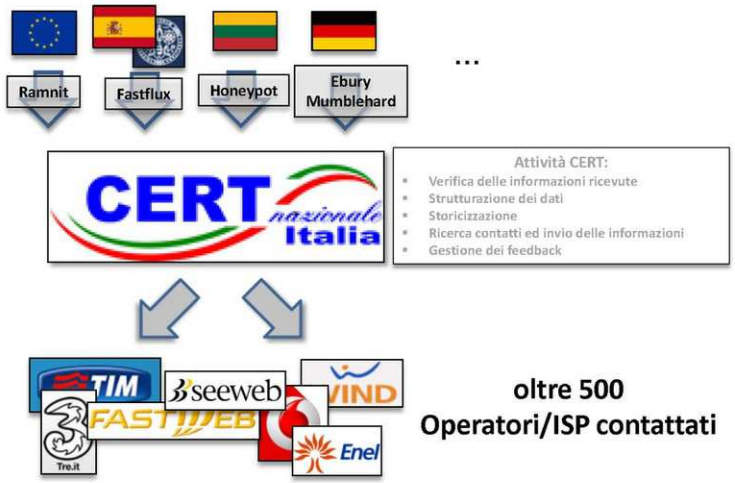
CERT nazionale Italia

Dati 2015 e 1Q 2016

Infosharing Internazionale



- Punto di contatto internazionale per la ricezione di segnalazioni
- Dati ricevuti principalmente dagli omologhi CERT europei ed internazionali



oltre 500 Operatori/ISP contattati

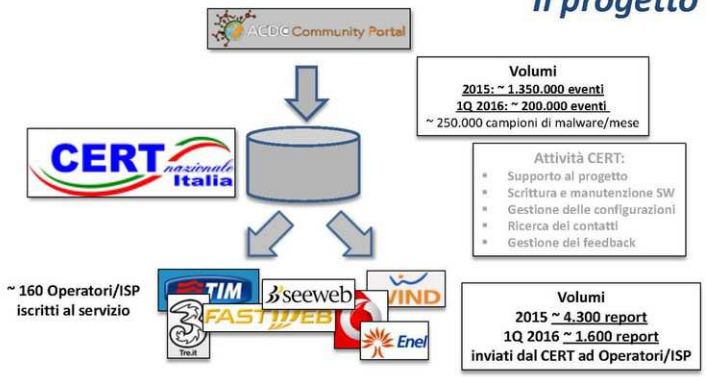
- Dati storicizzati ed inviati agli Operatori/ISP interessati
- Gestione dei feedback e correlazione tra incidenti

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

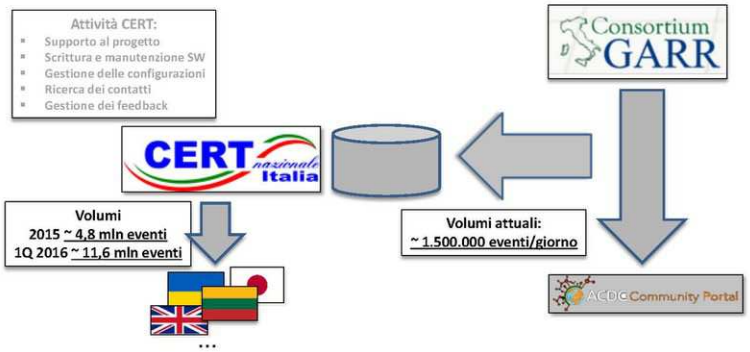
Dati 2015 e 1Q 2016 (2/5)

Il progetto europeo ACDC



- Piattaforma ACDC: collezionati circa 1.350.000 eventi di sicurezza relativi a reti italiane nel 2015 e 200.000 nel 1Q 2016
- Inviati nel 2015 circa 4.300 report agli Operatori/ISP coinvolti e circa 1.600 nel 1Q 2016

- Il sistema di *honeypot* colleziona circa 1.500.000 eventi al giorno (tentativi di connessione/attacco) provenienti da tutto il mondo



MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

CAMPAGNE INFORMATIVE

INFORMAZIONI DA FONTI SEMI-APERTE SU ***VULNERABILITA'*** **o COMPROMISSIONI**

- **REATTIVE** - vulnerabilità riscontrate in rete (per esempio macchine non correttamente configurate, con servizi "aperti" e potenzialmente utilizzabili per attacchi DDoS
- **PREVENTIVE -** segnalazione di compromissione di macchine, appartenenti a diversi tipi di «*botnet*» per la verifica dei sistemi, bonifica e messa in sicurezza

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Dati 2015 e 1Q 2016

Le campagne informative preventive (2/3)

Riguardano la comunicazione agli Operatori/ISP di vulnerabilità riscontrate nelle rispettive reti: macchine non correttamente configurate, con servizi "aperti" e potenzialmente utilizzabili per attacchi DDoS a terze parti o per accessi non autorizzati alle macchine stesse

- Nel 2015 (da aprile) avviate 25 campagne per circa **60.000 macchine** segnalate ai rispettivi Operatori/ISP
- Nel primo quadrimestre 2016 avviate 11 campagne per circa **60.000 macchine** segnalate ai rispettivi Operatori/ISP

Campagna	Data	Numero Macchine Segnalate	ISP Coinvolti
QOTD	21/04/2015	86	26
Chargen	28/04/2015	832	42
Chargen	12/06/2015	539	33
Chargen	20/07/2015	547	30
QOTD	20/07/2015	67	18
Memcached	28/07/2015	319	59
Redis	31/08/2015	60	26
Memcached	31/08/2015	279	47
QOTD	02/09/2015	99	24
Chargen	02/09/2015	731	35
NTP (Monitor)	11/09/2015	516	43
IPMI	16/09/2015	1.181	73
Portmapper	23/09/2015	17.785	262
QOTD	06/10/2015	92	23
Chargen	06/10/2015	687	34
Elasticsearch	07/10/2015	35	17
NAT-PMP	13/10/2015	8.577	109
NTP (Monitor)	22/10/2015	466	41
Redis	23/10/2015	60	28
Memcached	23/10/2015	264	47
QOTD	09/11/2015	102	26
Chargen	09/11/2015	754	34
NAT-PMP	17/11/2015	7.047	106
NTP (Monitor)	04/12/2015	518	44
Portmapper	23/12/2015	17.370	256
IPMI	13/01/2016	1.058	72
QOTD	25/01/2016	105	28
Chargen	25/01/2016	837	32
MC-SQLR	27/01/2016	4.048	160
Redis	23/02/2016	51	17
Memcached	23/02/2016	325	53
NAT-PMP	25/02/2016	6.889	109
NTP (Monitor)	16/03/2016	503	44
Portmapper	23/03/2016	16.011	242
TFTP	12/04/2016	30.435	215
Elasticsearch	13/04/2016	41	16

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Dati 2015 e 1Q 2016

Le campagne informative reattive (3/3)

Riguardano la comunicazione agli Operatori/ISP di effettive compromissioni riscontrate nelle rispettive reti: siti web compromessi o macchine infettate da particolari malware e facenti parte di specifiche «botnet»

- Nel 2015 (da novembre) avviate 12 campagne per circa **70.000 macchine compromesse** da *malware* specifici ed appartenenti a diverse «*botnet*» segnalate ai rispettivi Operatori/ISP
- Nel primo quadrimestre 2016 avviate 13 campagne analoghe per circa **115.000 macchine** segnalate

Campagna (numero)	Data	Numero Eventi Segnalati	ISP Coinvolti
Expiro	09/11/2015	123	10
Gozi(1)	12/11/2015	8.184	129
Palevo	13/11/2015	4.473	63
Cutwail	16/11/2015	1.513	93
Tinba(1)	19/11/2015	4.020	63
Zeroaccess	20/11/2015	30.456	131
Ponmocup(1)	03/12/2015	4.920	116
Dyre(1)	09/12/2015	1.814	45
Kelihos	11/12/2015	10.639	151
Slenfbot	14/12/2015	868	24
Lethic	15/12/2015	161	37
Asprox	24/12/2015	2.676	60
Tinba(2)	12/01/2016	663	29
Dyre(2)	18/01/2016	1.770	37
Vawtrak	19/01/2016	24	9
Ponmocup(2)	09/02/2016	3.341	73
Torpig	11/02/2016	6.026	85
Dorkbot	17/02/2016	620	44
Conficker	22/02/2016	95.253	273
Gootkit	15/03/2016	1.130	29
Matsnu	17/03/2016	37	5
Fleercivet	24/03/2016	630	18
Gozi(2)	11/04/2016	3.830	96
Torrentlocker	14/04/2016	530	50
Tinba(3)	19/04/2016	973	31

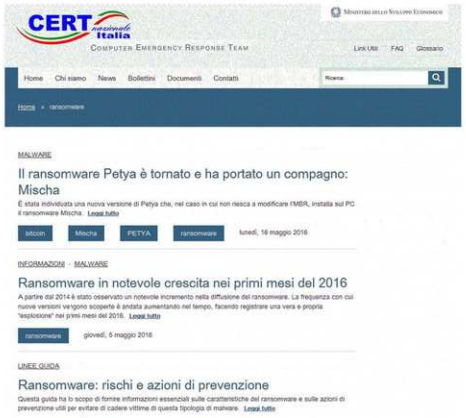
MINISTERO DELLO SVILUPPO ECONOMICO

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Azione di sensibilizzazione sulla diffusione *ransomware*

- Il ***ransomware*** è riconosciuto da tutti come una delle principali minacce informatiche attuali
- Il fenomeno è in crescita
- Colpisce indifferentemente sia l'utenza «*business*» che quella «*retail*»
- La soluzione più efficace è la **prevenzione**
- Solo azioni di sensibilizzazione ed informazione mirate possono migliorare la prevenzione



Delle oltre 200 news pubblicate sul sito del CERT Nazionale (https://www.certnazionale.it) circa 40 sono dedicate al ***ransomware*** ed alle numerose varianti

Pubblicata sul sito del CERT Nazionale una linea guida dedicata

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Alcuni nuovi sviluppi
Direttiva NIS e G7

❑ Direttiva NIS – Network and Information Security

Il **17 maggio 2016** il Consiglio UE ha adottato formalmente nuove norme volte ad aumentare la sicurezza delle reti e dei sistemi informativi in tutta l'UE.

❑ Due sono i pilastri della direttiva

Adozione di misure di sicurezza e **notifica** degli incidenti per gli operatori di **servizi essenziali**

Cooperazione tra i CERT

❑ G7

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

La Direttiva NIS - 1

Cooperazione tra i CERT

- **Costituzione di una rete dei CERT a livello europeo**
- **Armonizzazione delle procedure operative**
- **Scambio di informazioni su minacce ed incidenti**
- **Cooperazione nella risoluzione di incidenti**

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

La Direttiva NIS - 2

Requisiti di base dei CERT

- **Disponibilità dei servizi di comunicazione**
- **Sicurezza fisica**
- **Continuità operativa h24**
- **Partecipazione alla rete di cooperazione internazionale**

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

La Direttiva NIS - 3

Compiti dei CERT

- **Cooperazione con il settore privato**
- Monitoraggio degli incidenti a livello nazionale
- Emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti
- Intervento in caso di incidente
- Analisi dinamica dei rischi e degli incidenti, nonché sensibilizzazione situazionale
- Partecipazione alla rete dei CERT

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

La Direttiva NIS - 4

Compiti dei CERT

- Promozione di prassi comuni o standardizzate per il trattamento degli incidenti e dei rischi
- Promozione di procedure standard per l'adozione di sistemi di classificazione degli incidenti, dei rischi e delle informazioni

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

CSP - Core Service Platform
CEF - Connecting European Facilities

CSP è un progetto nel quadro del programma **CEF** della Commissione Europea.

- È un progetto per la realizzazione di una piattaforma di scambio informazioni
- Prevede l'implementazione di meccanismi di cooperazione
- Ha l'obiettivo di incrementare le capacità dei CERTs europei in termini di scambio informazioni, di coordinamento e di risposta alle minacce "cyber"

Il CERT Nazionale partecipa al progetto

MINISTERO DELLO SVILUPPO ECONOMICO
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione

CERT nazionale Italia

Gruppo dei Sette – G7
Cooperazione tra i CERT nel settore energia

- Rafforzamento della sicurezza nei settori energia e ICT
- Condivisione delle informazioni per il miglioramento dei meccanismi di prevenzione e di risposta ad attacchi di natura informatica
- Stretta collaborazione tra i CERT dei Paesi del G7 Energia

PAGINA BIANCA

Stampato su carta riciclata ecologica

17STC0018380