Perché l'Italia deve investire in cybersecurity?

Rischi e opportunità per l'Italia



Redatto da:

Alessandra Fiorani - Senior Researcher Area Difesa & Sicurezza
Valentina De Consoli - Junior Researcher Area Cultura & Società

Mondo Internazionale
Associazione culturale
Gallarate, Via Marco Polo 31
21013 - VA, Italia
C.F. 91071700123
P.IVA 03727710125

Mail: segreteria@mondointernazionale.com

DIFESA E SICUREZZA & CULTURA E SOCIETA’
Perché l’Italia deve investire in Cybersecurity? Rischi e opportunità per l’Italia.

ABSTRACT

La gestione del cyber spazio è una delle più importanti sfide, a livello nazionale e internazionale, del nostro tempo. Si tratta di uno spazio completamente artificiale e questo lo rende ancora più complicato da governare e amministrare. Infatti, non presenta una netta divisione in confini territoriali perciò, alla base della gestione di questo spazio e quindi anche di difesa dalle sue minacce, c’è la cooperazione tra Stati.[1] Quest’ultima è resa ancora più difficile dal fatto che si tratta di cooperare in uno spazio nuovo rispetto al consueto territorio delle relazioni internazionali, territorio contenente minacce anche di tipo extra-statale aventi un forte potere d’azione. Il processo di digitalizzazione dei settori della nostra società sta portando ad un aumento di rischi di attacco cibernetico: questo prevede che gli Stati, le aziende e tutti gli enti interessati studino una strategia di prevenzione e di risposta. La pandemia da Covid-19 ha accelerato il processo e ha portato la popolazione mondiale a trascorrere più tempo online, sia per svago che per lavoro. Conseguentemente il problema di gestire al meglio il cyber spazio e le sue minacce è divenuto ancora più prioritario, proprio perché tutte le debolezze e l’impreparazione dei vari settori si sono manifestate. È questa quindi l’occasione per dare il giusto peso alla problematica e per investire nella cybersecurity colmando le lacune che si sono presentate fino ad ora.

INDICE

1. Ruolo e consigli dell'Unione Europea
2. Cybersecurity e Smart Working
3. La Cybersecurity rende più competitivi
4. Cybersecurity nel settore sanitario: perché gli ospedali sono così violabili?
5. Lotta al Terrorismo
6. Prevenire i reati finanziari

Conclusioni



Perché l'Italia deve investire in Cybersecurity?

1. Ruolo e consigli dell'Unione Europea

L'entità del problema e l'esigenza di trovare una risposta efficace è sentita non solo a livello nazionale, ma anche europeo, Bruxelles infatti si è spesa molto nell'elaborare direttive e una strategia per una efficace risposta comune al problema. L'emergenza sanitaria ha aumentato i rischi a livello cibernetico, fondamentale diventava inserire i temi di digitalizzazione e sicurezza cibernetica nel piano di ripresa europeo. Infatti, tra le principali raccomandazione della Commissione Europea ai paesi riceventi fondi del RF, c'è l'impegno a digitalizzare vari settori del paese.[1] Inoltre, secondo la strategia elaborata nel dicembre 2020, saranno stanziati 4,5 miliardi, specificatamente per azioni di cyber security. La stessa strategia ha visto proporre una Joint Cyber Unit: considerata fondamentale per migliorare la cornice di gestione delle *cybersecurity crisis* a livello di Unione, dove facilitare le operazioni tecnologiche e la cooperazione tra paesi membri.[2]

Così come è necessaria un'agenzia interamente dedicata alla sicurezza cibernetica a Bruxelles, lo è anche a Roma. Una conseguenza molto importante degli ultimi 12 mesi sono le lacune emerse nell'ambito della risposta e prevenzione di attacchi cyber: secondo uno studio condotto da WMware Carbon Black con un campione di 252 interviste, il 38% ha affermato esserci "lacune molto significative nella visibilità relativa alle minacce alla sicurezza informatica".[3] Infatti, poiché in Italia si era già assistito a problemi legati alla digitalizzazione del settore privato o ad attacchi cyber all'amministrazione pubblica, vi è stato un rafforzamento delle politiche di cyber security. Un esempio è la creazione del Perimetro per la Sicurezza Informatica.[4]

---

[1] "Commission Staff Working Document: Guidance to member states Recovery and Resiliance plans", European Commission, 17/09/2020: "The Commission proposes that each recovery and resilience plan includes a minimum level of 20% of expenditure related to digital": https://ec.europa.eu/info/sites/info/files/3_en_document_travail_service_part1_v3_en_0.pdf;

[2] "Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade", European Commission – High Representative of the Union for Foreing Affairs and Security Council, 16/12/2020: JointCommunicationTheEUsCybersecurityStrategyfortheDigitalDecadepdf.pdf;

[3] "Italia – Threat Report", **WM**ware Carbon Black, giugno 2020: https://d110erj175o600.cloudfront.net/wp-content/uploads/2020/07/VMware-Carbon-Black-ItalianThreatReport.pdf;

[4] "Allegato alla Relazione Annuale al Parlamento – Documento di Sicurezza Nazionale", Sistema di Informazione per la Sicurezza della Repubblica, 2019: RELAZIONE-ANNUALE-2019-4.pdf;

Tuttavia, gli sforzi fatti fino a questo momento non sono stati sufficienti e per questo motivo, ora più che mai, è necessario creare una struttura interamente dedicata alla cyber security dove studiare una strategia per: aumentare il prestigio italiano in questo settore, accrescere la *cyber awareness* dei cittadini e creare interconnessione tra pubblico e privato a beneficio di ambedue i settori. [5]

2. Cybersecurity e Smart Working

In seguito alla pandemia il numero di persone in Italia che sono passate da lavorare *in loco* a lavorare da remoto è aumentato di quasi 3 milioni, raggiungendo la cifra di 4 milioni ad aprile.[6] Questa situazione ha colto tantissime aziende impreparate ad una rapida transizione allo *smart working* e nella velocità dell'emergenza è stato sottovalutato l'aspetto della sicurezza cibernetica. Infatti, molti lavoratori hanno dovuto acquistare strumenti di telelavoro e conseguentemente all'eccesso di domanda ne sono stati creati di nuovi; questo ha fatto sì che molte aziende abbiano scelto prodotti recenti e poco adatti allo smart working, cosa che li ha resi più suscettibili ad attacchi. Barbara Poggiali, direttrice della sezione di Cybersecurity di Leonardo, ha affermato che su 230mila campagne di malaspam sul coronavirus lanciate nei primi due mesi di pandemia, il 6% ha riguardato l'Italia,[7] inoltre uno studio ha stimato un aumento del 47% degli attacchi alle reti aziendali a livello mondiale[8]. Le conseguenze di un cyber attacco per un'azienda sarebbero catastrofiche: si parla di danni fisici all'industria, ma soprattutto di danni alla reputazione. Un aspetto su cui si deve prestare maggiore attenzione è la gestione dei dispositivi di lavoro: molte aziende autorizzano i dipendenti ad utilizzare i dispositivi personali per lavorare. Questo comporta un forte rischio perché può capitare che lo stesso dispositivo venga utilizzato anche

[5] "Cybersecurity: Unione europea e Italia Prospettive a Confronto", Claudia Cencetti, Quaderni IAI, 08/2014: Cybersecurity UE e Italia - IAI.pdf;

[6] "Cybersecurity: l'anno che sta finendo e l'anno che verrà", Marcello Fausti, ICT Security Magazine, 14/12/2020: Cybersecurity: l'anno che sta finendo e l'anno che verrà - ICT Security Magazine;

[7] "L'Italia spende 1,3 miliardi per la cybersecurity, ma ancora non bastano", Antonio Piemontese, Wired, 3/7/2020: Cybersecurity, l'Italia spende 1,3 miliardi, ma ancora non bastano - Wired;

[8] "Smart Working, cresciuti del 47% gli attacchi informatici alle reti aziendali", Chiara Sottocorona, Corriere della Sera – Economia, 20/7/2020: https://www.corriere.it/economia/professionisti/20_luglio_20/smart-working-cresciuti-47percento-attacchi-informatici-reti-aziendali-6d7001c4-ca78-11ea-b15c-cd9b33ddf899.shtml;

da familiari, magari da bambini, che possono navigare anche su siti non sicuri e mettere a rischio la sicurezza del dispositivo e le informazioni contenute. Poiché estendere le policy di sicurezza aziendale ai dispositivi personali può apparire come un'intrusione della privacy, molte aziende si limitano a dare delle linee guida, questo però mantiene una forte incertezza in termini di sicurezza. Per questo motivo la soluzione migliore è fornire uno strumento aziendale ad ogni dipendente, dove è possibile eliminare tutti i dati in maniera istantanea di fronte ad un attacco, limitando un furto di dati per esempio, cosa non fattibile con un dispositivo personale. Un ulteriore problema è legato alle reti wireless utilizzate, infatti onde evitare rischi è consigliabile fornire ai dipendenti una connessione sicura tra il dispositivo di lavoro e la rete aziendale, magari tramite installazione di un software apposito. Infine, si può consigliare di aggiornare costantemente le policies aziendali in termini di sicurezza cibernetica e di *smart working* per prevenire ed elaborare una pronta risposta in caso di attacchi. [9]

3. La Cybersecurity rende più competitivi

Al giorno d'oggi l'utilizzo di nuove tecnologie digitali porta ad una maggiore esposizione ai rischi cibernetici. La sicurezza informatica di una rete o infrastruttura è uno degli obiettivi principali che i *Risk Manager* devono considerare e perseguire, sia a livello aziendale che rispetto una amministrazione pubblica. Prendiamo in considerazione un attacco hacker finalizzato al furto di dati, che ha come bersaglio una grande impresa industriale, per questa azienda oltre al danno economico dovuto alla sottrazione dei dati, sorgerà anche un danno reputazionale data la scarsa capacità di difesa. Le stesse conseguenze che un attacco informatico ha per un'impresa, valgono anche per il sistema statale. Un possibile attacco hacker ad una infrastruttura pubblica creerebbe un problema di credibilità. Per spiegare meglio il concetto si riporta di seguito un estratto di un articolo del 2019 del giornale *Scienza in Rete*[10]*.*

"Un attacco informatico di successo potrebbe rappresentare un momento di non ritorno per la

[9] "Smart Working e Cyber Security – Difendere I dati aziendali e i propri dati personali", Vincenzo Calabrò, ICT Security Magazine, 2020: *Guida Pratica per uno Smart Working Sicuro.pdf;

[10] Scienza in rete è un giornale di attualità e cultura scientifica. Scienza in rete è un progetto editoriale dell'Agenzia Zadig condiviso con il Gruppo 2003 per la ricerca scientifica, un'associazione di ricercatori italiani nata per promuovere la cultura scientifica in Italia. https://www.scienzainrete.it/

credibilità di un'azienda, lo sviluppo del suo business e la capacità di vendere prodotti in un regime di sana concorrenza. Ugualmente, un attacco informatico riuscito potrebbe destabilizzare il mercato azionario facendo sprofondare interi Paesi nel caos, oppure bloccare i rifornimenti di gas in inverno o la gestione del ciclo dei rifiuti urbani."[11]

La cybersecurity quindi è fondamentale sia per un sistema aziendale che per quello pubblico-statale. Alcuni Paesi hanno già provveduto al miglioramento delle loro strutture informatiche per la protezione dei propri sistemi, per esempio la Danimarca. Secondo quanto emerso da una ricerca[12] condotta a giugno 2020 dalla società *Comparitech*, tra 76 Stati analizzati in base al livello di cybersecurity, la Danimarca si conferma il Paese più sicuro al mondo, mentre l'Italia si posiziona al 31° posto, quasi a metà classifica. Questo significa che l'Italia deve implementare la messa in sicurezza delle reti informatiche della pubblica amministrazione e delle reti essenziali -c.d. infrastrutture critiche- di uno Stato. La sicurezza e la continuità operativa delle reti critiche ed essenziali diventano un imprescindibile parametro di **vantaggio competitivo**, necessario per assicurare prosperità economica, sviluppo tecnologico, stabilità e indipendenza a tutto il suo sistema. Questo fattore porterebbe il Paese ad essere più competitivo[13] e ad ottenere maggiori rendimenti economici e non: **un Paese maggiormente preparato** ad affrontare attacchi informatici è anche un Paese che **attira più investitori**.

Aumentare i fondi per implementare la cybersecurity statale si dimostra quindi un fattore chiave sia per la tutela dei propri cittadini, sia per elevare il proprio rilievo economico.

4. Cybersecurity nel settore sanitario: perché gli ospedali sono così violabili?

Il settore sanitario è uno dei più colpiti da attacchi cyber: i dispositivi degli ospedali contengono

[11] *L'impatto della cybersecurity sull'economia e la democrazia del Paese: il ruolo della ricerca scientifica*; di Marco Conti, Rocco De Nicola, Paolo Prinetto; pubblicato il 22/07/2019

[12]; *Which countries have the worst (and best) cybersecurity?*, Paul Bischoff, Comparitech, 03/2020, https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

[13] Giugno 2018; Laboratorio Nazionale di Cybersecurity CINI - Consorzio Interuniversitario Nazionale per l'Informatica*;* Roberto Baldoni, Rocco De Nicola, Paolo Prinetto; *Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici Progetti e Azioni per difendere al meglio il Paese dagli attacchi informatici.*

informazioni dei pazienti e i fascicoli contenenti tutti i dati di un individuo vengono rivendute nel dark web ad acquirenti che li utilizzano per furto d'identità o frode. Come evidenziato nel rapporto Clusit 2020[14] gli ospedali non possono permettersi di fermare i lavori quando subiscono un attacco hacker, quindi piuttosto pagano un riscatto pur di tornare ad appropriarsi dei propri dati e far riattivare i loro dispositivi. Questa situazione si è ancora più sentita in piena emergenza sanitaria e gli aggressori hanno imparato a sfruttarla ancora di più: il report Healthcare Threat Landscape ha riportato che a fine marzo le organizzazioni nel settore sanitario avevano ricevuto circa il 16% in più di messaggi pericolosi.[15] Come per altri settori, il motivo per il quale gli ospedali sono così fortemente attaccabili è una carenza di investimenti per la cybersecurity e una mancata strategia di prevenzione di questi attacchi. Infatti, i budget indirizzati alla sanità sono alquanto ristretti e questo non va a favorire investimenti in un settore che non genera profitti; inoltre, molti ospedali hanno a disposizione dispositivi datati con sistema di difesa tradizionali, in altri casi c'è reticenza a dotare questi dispositivi di porzioni di software che ne migliorino le prestazioni, proprio per timore di danneggiarli e renderlo inattivo per un periodo di tempo. Questo fa sì che non ci sia evoluzione nella sicurezza ospedaliera, ma allo stesso tempo i numerosi incidenti informatici hanno un importante costo. Per risolvere questo problema bisognerebbe dare priorità a questa tematica in termini di amministrazione sanitaria e fare maggior training a tutto il personale ospedaliero: può capitare, soprattutto grazie all'aumento di *smart working* a cui abbiamo assistito quest'anno, anche nel settore ospedaliero, che i dipendenti trasferiscano dati su loro chiavette, oppure siano vittime di campagne di *pishing;* perciò è fondamentale che ci sia maggiore prudenza e attenzione da parte di tutti i dipendenti coinvolti, ma anche maggiori competenze in termini di sicurezza cibernetica. Servirebbe anche aggiornare i dispositivi elettronici e dotarli di efficienti sistemi di sicurezza, implementare i controlli, specialmente quelli inerenti alla gestione dei dati e informazioni dei pazienti e infine, come per tutti gli altri settori, creare policies ad hoc, sia per lo *smart working*, sia per il corretto utilizzo dei sistemi informativi, ed effettuare e aggiornare continuamente un R*isk Assessment* e

[14]"Rapporto Clusit 2020 sulla Sicurezza ICT", Clusit, 03/2020, Focus On – Sicurezza nel settore sanitario: *Rapporto_Clusit_2020_web_marzo.pdf;

[15] "Cybersecurity e pandemia: gli attacchi alla sanità continuano", 01health, 09/11/2020: https://www.01health.it/tecnologie/sicurezza/cybersecurity-pandemia-attacchi-sanita-continuano/;

un R*isk Management.* [16]

5. Lotta al Terrorismo

Il tema difesa e cybersecurity combacia su più fronti. Il cyberspazio, da anni ormai, viene considerato come prossimo terreno della conflittualità e dominio operativo in cui competeranno le grandi potenze. La cybersecurity si dimostra essenziale non solo per prevenire guerre cibernetiche ma anche nuove forme "ibride" di minacce, una tra tutte è il **cyberterrorismo**[17].

Rispetto al terrorismo tradizionale questa nuova tipologia sfrutta il web come terreno dove reclutare nuovi seguaci e per una diffusione della ideologia. Nel caso del terrorismo di matrice islamica-radicale la Polizia Postale Italiana ha svolto- e continua tutt'ora- continui controlli di piattaforme web. Questa attività preventiva di controllo ha portato al monitoraggio di oltre 36.000 website. Ciò che si evince da questa vicenda è la continua opera di propaganda e influenza mediatica che i gruppi terroristici pongono in atto. Le attività di cyberterrorismo utilizzano le reti web come:

* strumento di propaganda di operazioni terroristiche;
* strumento di rivendicazione;
* spazio di reclutamento;
* strumenti di finanziamento del terrorismo;
* luogo di vendita e scambio di armi, e tanto altro ancora.

Nel novembre 2019 la Polizia Postale Italiana ha partecipato in collaborazione con l'EUROPOL e altre forze di polizia europee all'Action Day[18], alla chiusura di molti siti Internet dedicati a queste attività illecite.

Sulla base delle precedenti considerazioni e tenendo presente che il terrorismo è di per sé un fenomeno transnazionale, condannato dall'Unione Europea e inserito nell'elenco dei 32 reati sempre perseguibili all'interno dell'UE; appare evidente come anche il cyberterrorismo sia da

[16] "Cyber Security nel settore sanitario: scenari, minacce e consigli di cyber hygiene", Salvatore Lazzari, CyberSecurity360, 16/04/2020: https://www.cybersecurity360.it/soluzioni-aziendali/cyber-security-nel-settore-sanitario-scenari-minacce-e-consigli-di-cyber-hygiene/;

[17] Rapporto Clusit 2020 sulla Sicurezza ICT", Clusit, 03/2020: *Rapporto_Clusit_2020_web_marzo.pdf;

[18] *REFERRAL ACTION DAY AGAINST ISLAMIC STATE ONLINE TERRORIST PROPAGANDA*, EUROPOL; https://www.europol.europa.eu/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda

considerare una muova minaccia. Per far fronte a questa nuova tipologia di rischio transnazionale e cibernetico, si ritiene sia necessario sviluppare efficaci e efficienti strategie di difesa e contrasto, coordinando azioni condivise tra Stati membri e tra agenzie di sicurezza nazionali.

6. Prevenire i reati finanziari

Il settore della finanza è uno dei più esposto a rischi cyber [19], spesso infatti gli attacchi hacker sono rivolti a danni di banche e finanziarie.

Tra i dati del 2019 della Polizia Postale troviamo *"circa 5 mila casi di* ***financial cybercrime*** *registrati con un recupero di quasi 14 milioni di euro su una movimentazione di poco meno di 19 milioni"*[20]*.*

Uno dei più frequenti reati registrato è il *phishing:* tecnica per cui si invia al bersaglio un'"esca", per esempio una mail falsificata da parte dell'istituto bancario di appartenenza, in cui si invita a comunicare credenziali e codici; il tutto finalizzato al furto dei dati sensibili. Ma il phishing non si ferma alle mail, con lo sviluppo delle nuove modalità di comunicazione, SMS e messaggi vocali, questa tecnica di truffa si è evoluta: in *vishing* e *smishing*.

L'elenco dei *financial cybercrimes* comprende ampie fattispecie, tra cui: furto di informazioni sulle carte di pagamento, l'accesso a conti finanziari per avviare transazioni non autorizzate, l'estorsione, la frode di identità per richiedere prodotti finanziari, e così via.

Questi attacchi informatici possono impattare tutto il sistema economico e finanziario. Per far fronte ai crimini finanziari di stampo informatico già dal 2018 alcuni Stati membri dell'UE, compresa l'Italia, hanno avviato una cooperazione di intelligence e forze di polizia che ha dato vita al progetto EU-OF2CEN, lo scopo del progetto è quello di anticipare e bloccare o intercettare frodi già in corso recuperando le somme.[21]

Dal 2018 questo programma si è rivelato sì prezioso per lo scambio informativo tra i vari Paesi europei, però non completamente efficace per contrastare questi crimini.

---

[19] Fonti: statistiche e grafici del Rapporto Clusit 2020 sulla sicurezza ICT in Italia, Clusit, 03/2020: *Rapporto_Clusit_2020_web_marzo.pdf;

[20] https://www.poliziadistato.it/articolo/385e10452a28e24560815120 Polizia Postale; *I dati del 2019*.

[21] *Financial cybercrime: cresce la prevenzione con EU-OF2CEN,* Ministero dell'Interno, 04/2018, https://www.interno.gov.it/it/notizie/financial-cybercrime-cresce-prevenzione-eu-of2cen

Infatti risale al 2018 il più grande attacco informatico finanziario che ha colpito l'Italia; si tratta di un attacco alla piattaforma online di scambio di criptovalute *Bitgrail,* consistente in una frode informatica con cui sono stati rubati 120 milioni di euro in criptovaluta, nello specifico in moneta virtuale NANO XRP.

In questo caso, trattandosi di una piattaforma di *exchange*, ritenuta dalla direttiva NIS dell'Unione Europea[22] un servizio essenziale, è necessario "*un potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema-paese; rafforzamento delle capacità di contrasto alla diffusione di attività e contenuti illegali online; rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica*"[23].

[22] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[23] *Cybersecurity: Unione europea e Italia- Prospettive a confronto;* Quaderni IAI; Claudia Cencetti; Edizioni Nuova Cultura; 08/2014.

Conclusioni

Alla luce di quanto emerso finora, basandoci sulle aree d'interesse in cui si ritiene sia fondamentale incrementare gli investimenti in sicurezza cibernetica, sono state elaborate una serie di proposte o suggerimenti per migliorare il livello di cybersecurity in Italia. Le principali raccomandazioni che si propone di seguire sono:

- **Cyber Awareness:** molti attacchi cyber sono causati dall'errore degli utenti, l'ignoranza della popolazione italiana in termini di *cyber Hygiene* e prevenzione dalle minacce cyber deve essere uno dei primi ostacoli da superare. Questo problema si estende a utenti giovani che usano il cyber spazio per svago, ma anche ad aziende che sottovalutano i rischi di un attacco cibernetico e non agiscono per prevenirlo. Quindi sono raccomandate campagne di sensibilizzazione rivolte ad un vastissimo pubblico l'introduzione di una formazione alla cybersecurity nelle scuole primarie ed una più specifica rivolta ad università ed aziende. [24]

- **Recepimento Direttiva NIS e Perimetro di Sicurezza Nazionale:** la Direttiva NIS (EU-2016/1148)[25] - *Network and Information Security*- interviene sul piano della sicurezza delle reti cibernetiche e, nello specifico, ha l'obiettivo di stabilire un elevato livello di sicurezza della rete e dei sistemi informativi. La Direttiva emanata nel 2016 dalla Commissione e Parlamento EU ha l'obbligo di essere recepita e applicata da tutti gli Stati Membri.

  In Italia la Direttiva è stata recepita attraverso il decreto legislativo n. 65 del maggio 2018 e successivamente, a complemento di questo recepimento, con il decreto-legge n. 105 del 2019. Quest'ultimo istituisce il Perimetro di Sicurezza Nazionale Cibernetica, con il fine di assicurare la sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una

[24] Giugno 2018; Laboratorio Nazionale di Cybersecurity CINI - Consorzio Interuniversitario Nazionale per l'Informatica*;* Roberto Baldoni, Rocco De Nicola, Paolo Prinetto; *Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici Progetti e Azioni per difendere al meglio il Paese dagli attacchi informatici.*

[25] Direttiva (Ue) 2016/1148 del Parlamento Europeo e Del Consiglio, del 06 Luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

sede nel territorio nazionale. Ad un anno circa dall'emanazione del decreto-legge n.105, il percorso per il completamento dell'istituzione di tale perimetro è stato rallentato dagli effetti della pandemia. Tuttavia, il governo Conte II, tramite una serie di DPCM ha provveduto al completamento del Perimetro. Il primo, il DPCM n. 131 del 30 luglio 2020[26] (relativo all'art. 1, comma 2 del decreto-legge[27]) si occupa sia dell'elencazione dei criteri procedurali con cui individuare amministrazioni pubbliche, operatori ed enti pubblici e privati (i soggetti) da includere nel Perimetro.

A seguire, si ritiene necessario contemplare il secondo DPCM, risalente al 25 novembre 2020 e contenente una lista secretata di tutti i soggetti in un primo momento inclusi nell'architettura cibernetica[28]. Per finire, è importante citare il il DPR n. 54 del 5 febbraio 2021[29], pubblicato in Gazzetta Ufficiale[30] in attuazione dell'art. 1 comma 6 del decreto legge e definisce le procedure, le modalità, i termini e i criteri tecnici da seguire ai fini delle valutazioni da parte del Centro di valutazione e certificazione nazionale.

Inoltre, si consiglia di monitorare il processo di revisione della Direttiva; difatti, la Commissione Europea ha elaborato la proposta di revisione della Direttiva NIS, presentando il 16 2021 febbraio in il documento "*Proposed directive on measures for a high common level of cybersecurity across the Union*"[31]

- Sicurezza partecipata: nel settore privato diverse aziende hanno una conoscenza e delle tecniche in termini di cybersecurity molto affinate. Una collaborazione col settore

[26] DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 30 luglio 2020, n. 131
Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. (20G00150) (GU Serie Generale n.261 del 21-10-2020)

[27] Decreto-legge n. 105/2019.

[28] https://formiche.net/2020/12/secondo-dpcm-perimetro-cyber/

[29] Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. (21G00060) (GU Serie Generale n.97 del 23-04-2021)

[30] https://www.gazzettaufficiale.it/eli/id/2021/04/23/21G00060/sg

[31] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, Brussels, 16.12.2020. https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

pubblico per condividere questa conoscenza sarebbe ottimale, infatti le minacce che riguardano la PA o settori come quello sanitario vanno ad incidere sull'intera popolazione. Allo stesso tempo, dotare le nostre aziende di ottimi sistemi di sicurezza cibernetica migliorerebbe la reputazione del *Made in Italy* nel mondo, cosa che andrebbe a beneficio di tutte le nostre aziende. Quindi una sicurezza partecipata tra settore pubblico e privato e tra aziende del settore privato permetterebbe di ottimizzare i livelli di cybersecurity nazionali senza sforzi aggiuntivi e con spese limitate. [32]

- Strategia di Sicurezza Nazionale: Sia alcuni degli Stati membri che i Paesi extraeuropei hanno elaborato delle Strategie di Sicurezza Informatica Nazionale (NCSS). Un insieme di guide e *best practices* da seguire per l'ammodernamento delle proprie strategie di difesa cibernetica. In particolare per elaborare una efficiente *cyber-strategy* si consiglia di perseguire i 13 pilastri principali in tema di cybersecurity elaborati dal Sistema di informazione per la sicurezza della Repubblica; essi sono:

  1. identificare e classificare le infrastrutture critiche da proteggere;
  2. stabilire trattati, leggi e regole di condotta nazionali e/o internazionali ad hoc;
  3. sviluppare i rapporti diplomatici e rafforzare le partnership internazionali;
  4. focus sulla protezione dei diritti fondamentali, sulla privacy e/o sulla libertà di espressione;
  5. focus sul cyber-crime;
  6. trattare il cyber-spazio come dominio di warfare;
  7. creare apposite strutture politiche e decisionali per far fronte alla minaccia;
  8. sviluppare deterrenza per la prevenzione dei conflitti nel cyber-spazio;
  9. incrementare i livelli di sicurezza, affidabilità e resilienza delle reti e dei sistemi informatici;
  10. rafforzare la condivisione delle informazioni (anche tra pubblico e privato), l'early warning e le capacità di incident response;

[32] "*Cybersecurity: Unione europea e Italia Prospettive a Confronto",* Claudia Cencetti, Quaderni IAI, 08/2014: Cybersecurity UE e Italia - IAI.pdf;

11. aumentare la consapevolezza pubblica della minaccia e l'importanza della cyber-security;
12. creare e/o incrementare il numero delle figure professionali ad hoc;
13. incoraggiare l'innovazione, la ricerca e lo sviluppo.[33]

- Aumentare i tecnici: il nostro paese soffre di una scarsa offerta di esperti di informatica e di cybersecurity, infatti tra i professionisti che l'Italia forma molti migrano all'estero attratti da salari più vantaggiosi. La carenza di personale esperto in cybersecurity rende l'Italia un bersaglio più facile da colpire. Il Bel Paese deve lavorare sull'attrattività degli studi di informatica sia a livello di scuola secondaria di primo grado che a livello di università. Inoltre, deve impegnarsi nel limitare l'esodo, creando posti di lavoro nel settore pubblico per queste figure professionali, per esempio e costruendo la cultura dell'esperto di cybersecurity come figura fondamentale nelle aziende.

[33] *I principi strategici delle politiche di cybersecurity*, Stefano Mele, Sistema di informazione per la sicurezza della Repubblica, 12/2013, https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-delle-politiche-di-cyber-security.html

BIBLIOGRAFIA

- *"Commission Staff Working Document: Guidance to member states Recovery and Resiliance plans", European Commission, 17/09/2020: "The Commission proposes that each recovery and resilience plan includes a minimum level of 20% of expenditure related to digital":*

- *Commissione Europea, 07 febbraio 2013, Comunicazione Congiunta al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato Delle Regioni, Strategia dell'Unione europea per la cibersicurezza.*

- *Claudia Cencetti, "Cybersecurity: Unione Europea e Italia. Prospettive a confronto", Quaderni IAI, 08/2014: "Il dibattito sulla natura dello spazio cibernetico è tutt'altro che teorico, essendo alla base della cooperazione internazionale.":Cybersecurity UE e Italia - IAI.pdf;*

- *Direttiva (Ue) 2016/1148 del Parlamento Europeo e Del Consiglio, del 06 Luglio 2016, recante*

  misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

- *DECRETO LEGISLATIVO 18 maggio 2018, n. 65. Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.*

- *DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 30 luglio 2020, n. 131*
  Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133

- *EUROPOL; Referral Action Day Against Islamic State Online Terrorist Propaganda,*

- *"Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade", European Commission – High Representative of the Union for Foreing Affairs and Security Council, 16/12/2020;*

- *Laboratorio Nazionale di Cybersecurity CINI - Consorzio Interuniversitario Nazionale per l'Informatica; Roberto Baldoni, Rocco De Nicola, Paolo Prinetto; "Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici Progetti e Azioni per difendere al meglio il Paese dagli attacchiinformatici"; Giugno 2018*

- *L'impatto della cybersecurity sull'economia e la democrazia del Paese: il ruolo della ricerca scientifica; di Marco Conti, Rocco De Nicola, Paolo Prinetto; pubblicato il 22/07/2019*

- *Marcello Fausti, "Cybersecurity: l'anno che sta finendo e l'anno che verrà", ICT Security Magazine,14/12/2020;*

- *Ministero dell'Interno, Financial cybercrime: cresce la prevenzione con EU-OF2CEN, 04/2018*

- Paul Bischoff, *Which countries have the worst (and best) cybersecurity?*, Comparitech, 03/2020,

- *"Rapporto Clusit 2020 sulla Sicurezza ICT", Clusit, 03/2020,*

- *Sistema di informazione per la sicurezza della Repubblica. RELAZIONE SULLA POLITICA DELL'INFORMAZIONE PER LA SICUREZZA 2020. Relazione al Parlamento.*

- Stefano Mele, *I principi strategici delle politiche di cybersecurity*, Sistema di informazione per lasicurezza della Repubblica, 12/2013

- Vincenzo Calabrò, "Smart Working e Cyber Security – Difendere I dati aziendali e i propri dati personali", ICT Security Magazine, 2020

- *WMware Carbon Black, "Italia – Threat Report", giugno 2020.*

SITOGRAFIA

- Cybersecurity UE e Italia - IAI.pdf;
- https://ec.europa.eu/info/sites/info/files/3_en_document_travail_service_part1_v3_en_0.pdf;
- JointCommunicationTheEUsCybersecurityStrategyfortheDigitalDecadepdf.pdf;
- RELAZIONE-ANNUALE-2019-4.pdf
- https://d110erj175o600.cloudfront.net/wp-content/uploads/2020/07/VMware-Carbon-Black-ItalianThreatReport.pdf;
- Cybersecurity: l'anno che sta finendo e l'anno che verrà - ICT Security Magazine;
- Cybersecurity, l'Italia spende 1,3 miliardi, ma ancora non bastano - Wired
- https://www.corriere.it/economia/professionisti/20_luglio_20/smart-working-cresciuti-47percento-attacchi-informatici-reti-aziendali-6d7001c4-ca78-11ea-b15c-cd9b33ddf899.shtml
- *Guida Pratica per uno Smart Working Sicuro.pdf
- https://www.scienzainrete.it/
- https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/
- *Rapporto_Clusit_2020_web_marzo.pdf
- https://www.01health.it/tecnologie/sicurezza/cybersecurity-pandemia-attacchi-sanita-continuano/
- https://www.cybersecurity360.it/soluzioni-aziendali/cyber-security-nel-settore-sanitario-scenari-minacce-e-consigli-di-cyber-hygiene/
- https://www.europol.europa.eu/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda
- https://www.poliziadistato.it/articolo/385e10452a28e24560815120
- https://www.interno.gov.it/it/notizie/financial-cybercrime-cresce-prevenzione-eu-of2cen

- https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-delle- politiche-di-cyber-security.html