Innovative Legal & ICT Counsel

DirICTo

Diritto & Information and Communication Technology

Rivista di approfondimento nell'ambito delle tematiche di interesse comune per il mondo giuridico e informatico

Fondato e diretto da Massimo Farina

www.diricto.it

info@diricto.it

Il Network raggruppa esperti e studiosi, di tutta l'Italia, in materia di Diritto dell'Informatica e di Informatica Giuridica, con il fine di sviluppare attività di studio, ricerca e approfondimento nell'ambito delle tematiche di interesse comune per il mondo giuridico e informatico.

Sommario

DirICTo
Diritto & Information and Communication Technology

Il malware WannaCry: aspetti penali e le regole AgID/CERT-PA sulla sicurezza informatica

A cura di Gianluca Satta e Alessandro Bonu

Cosa è successo?

L'evento relativo all'ondata del malware denominato WannaCry verificatosi nello scorso mese di maggio è stato di fondamentale importanza per far emergere le criticità che ad oggi sono ancora presenti nell'attività di sviluppo del software. WanaCrypt0r (noto anche come WannaCry o WCry), infatti è un Trojan che si è diffuso velocemente grazie alla possibilità di trasmettersi utilizzando un exploit, accedendo attraverso una nota vulnerabilità di Windows senza bisogno di intervento da parte dell'utente. Una volta che il computer viene infettato, il malware prova a diffondersi in tutti gli altri sistemi della rete locale. L'offensività del malware è stata agevolata notevolmente dal suo particolare funzionamento in grado di sfruttare i privilegi di amministratore con i quali, spesso, si opera nella gran parte dei nostri PC.

WannaCry è stato riconosciuto per la prima volta a febbraio di quest'anno in una variante, meno offensiva dell'attuale, denominata Ransom_WCRY.C. e veicolato tramite alcune tradizionali tecniche di phishing che, anche per la sua scarsa diffusione, hanno portato a sottovalutarne l'effettiva portata e pericolosità. L'attacco del periodo più recente, nella variante WanaCryptor 2.0, ha coinvolto oltre 75.000 computer di 99 paesi diversi in tutto il mondo, causando la criptazione dei file in essi contenuti.

Nella sua ultima versione, quindi, il virus è inquadrabile sia nella categoria dei ransomware che in quella dei cosiddetti worm, poiché è in grado di replicarsi rapidamente sfruttando le debolezze strutturali della rete.

La particolarità di questo attacco riguarda l'utilizzo di una vulnerabilità nota come EternalBlue/DoublePulsar: un sistema exploit sviluppato dall'Intelligence americana della National Security Agency (NSA). Ebbene, EternalBlue, costruito dall'NSA come arma informatica, è tra i codici sottratti all'Agenzia ad opera di un misterioso gruppo di pirati informatici noto come "Shadow Broker": un'attività iniziata la scorsa estate, con la diffusione online di altre armi digitali, che sono poi finite anche in mano di alcuni criminali, poi recentemente utilizzate per potenziare la famiglia dei famigerati ransomware. È così che, alcune settimane fa, il codice offensivo EternalBlue è stato pubblicato online e si è potuto scoprire che la sua modalità di funzionamento sfrutta proprio una vulnerabilità interna ai sistemi Windows prima sconosciuta, ma che Microsoft aveva risolto il 14 marzo 2017 con l'aggiornamento di sicurezza MS17-010.

In Italia, sembrerebbe che non vi siano state importanti evidenze di riscontro, a parte qualche caso isolato, mentre in Inghilterra e Scozia si è verificata una situazione molto più preoccupante: si pensi, a titolo d'esempio, all'accesso bloccato alle cartelle cliniche digitali

dei pazienti o alle ambulanze in emergenza che hanno dovuto invertire la rotta a causa di riferimenti errati sulla destinazione da raggiungere. Il National Health Service (NHS), l'agenzia statale che gestisce la sanità in Gran Bretagna, ha fatto sapere che in alcuni casi è stata addirittura necessaria la sospensione dei servizi sanitari. In Spagna, le principali fonti di cronaca hanno riferito di infezioni importanti anche in aziende di telecomunicazioni e legate a linee di credito.

Come funziona WannaCry

In genere l'infezione avviene attraverso l'apertura di un link malevolo presente su una mail che in qualche modo cerca di riprodurre un sito noto (vedi una banca) o che presenta in allegato una fattura che dev'essere ancora saldata. Si gioca molto sull'istinto umano che in balia del dubbio verso qualcosa che lo riguarda è portato a consultare un link o ad aprire un allegato, ignorando i pericoli del caso.

Il virus in questione, per poter funzionare correttamente e potersi poi diffondere, richiede che l'utente con il quale si accede al sistema operativo infettato sia abilitato con i cosiddetti privilegi amministrativi.

Una volta cliccato sul link presente all'interno della mail o aver aperto l'allegato presente, tutto ha inizio e in poco tempo i dati vengono cifrati e messi sotto chiave. Una volta terminata questa attività di cifratura il virus si preoccupa di notificare al malcapitato un chiaro e ben articolato messaggio su come poter ottenere nuovamente la disponibilità dei propri dati, banalmente attraverso il pagamento di una somma di denaro in valuta bitcoin.

Essendo una valuta poco nota alla maggior parte delle vittime, vengono descritti minuziosamente tutti i passi da compiere per procedere al pagamento. Il soggetto criminale in questo contesto punta su due aspetti principali: il primo è quello di facilitare le procedure di pagamento attraverso una moneta virtuale della quale immagina che l'utente malcapitato sia poco avvezzo. In secondo luogo non viene chiesta di solito una cifra spropositata in quanto si cerca di incentivare al pagamento piuttosto che indurre la vittima ad altre soluzioni.

Alcuni aspetti penali della vicenda

Da un punto di vista strettamente giuridico, l'azione criminale perpetrata da coloro che realizzano e diffondono il virus in questione ha una rilevanza penale molto ampia in quanto può realizzare la violazione di diverse fattispecie di reato previste dal nostro ordinamento.

In primo luogo, la mera condotta intrusiva del criminale attraverso l'azione del virus e nei confronti del sistema informatico o telematico, quando questo è protetto da misure di sicurezza, può integrare il delitto di accesso abusivo a un sistema informatico o telematico, punito dall'art. 615-ter del codice penale.

Inoltre, la realizzazione e la diffusione delle email di phishing utilizzate per indurre il malcapitato ad aprire l'allegato contenente il codice malevolo, può costituire una condotta punibile ai sensi dell'art. 615-quater del codice penale, che sanziona la detenzione e la

diffusione abusiva di codici di accesso a sistemi informatici o telematici. Il reato si commette, nel caso in esame, quando si realizza la diffusione della email contenente il virus, che rappresenta un mezzo idoneo all'accesso al sistema informatico, al fine di realizzare un profitto (il pagamento della somma di denaro) o di arrecare un danno (la criptazione dei dati).

L'azione del virus WannaCry, così come di altri ransomware di tipo analogo, realizza di fatto un'alterazione o soppressione dei dati o dei programmi informatici presenti nelle macchine infettate, dal momento che, sebbene i dati siano solo criptati e non cancellati o distrutti, fa venir meno la possibilità di recupero da parte del legittimo titolare. Tale condotta è, quindi, punibile anche dall'art. 635-bis del codice penale che prevede il reato di danneggiamento di sistemi informatici e telematici.

Infine, l'azione commessa attraverso il virus può costituire anche il reato di frode informatica, punito e previsto dall'art. 640-ter del codice penale. Con questo reato, il legislatore penale ha inteso punire la condotta di colui che alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico, o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico, procura a sé o ad altri un ingiusto profitto con altrui danno. Quest'ultimo elemento richiesto dalla fattispecie penale si realizza nel momento in cui la vittima versa la somma di denaro richiesta dai criminali per poter ottenere la chiave di decifratura dei dati; in caso di mancato versamento della somma di denaro, comunque potrebbe configurarsi il medesimo reato nella forma del tentativo.

Un'ultima considerazione merita l'aspetto della richiesta di denaro in cambio della possibilità di ottenere nuovamente l'accesso ai dati presenti nel sistema informatico. Tale elemento, infatti, potrebbe ritenersi sufficiente perché si configuri un ulteriore reato, non rientrante nel novero dei cosiddetti reati informatici in senso stretto: il reato di estorsione. Secondo l'art. 629 del codice penale è punita la condotta di colui che mediante violenza o minaccia costringe taluno a fare o ad omettere qualche cosa procurando a sé o ad altri un ingiusto profitto con l'altrui danno. La violenza, che può essere anche psicologica, o la minaccia, richieste dalla fattispecie incriminatrice, nel caso di specie è rappresentata dalla possibilità di perdere l'accesso ai propri dati contenuti nel sistema informatico.

L'intervento di AgID/CERT-PA

Tenuto conto di quanto è stato finora illustrato, delle modalità di diffusione dei virus ransomware e delle conseguenze in termini economici che derivano dalla loro azione, è importante conoscere e adottare una serie di cautele e di misure di sicurezza per ridurre al minimo il rischio di incidenti informatici di questo tipo.

A tal proposito, all'indomani dell'avvenuto attacco da parte del virus WannaCry, le massime istituzioni italiane in ambito di sicurezza informatica, AgID e CERT-PA, hanno pubblicato una serie di linee guida volte ad eliminare la vulnerabilità dei sistemi, ad abbassare il rischio di infezione dal virus e mitigare eventuali attacchi già perpetrati.

In particolare, l'Agenzia per l'Italia Digitale, in virtù delle funzioni ad essa attribuite dall'art. 14-bis, lett. a) del D. Lgs. 82/2005 (Codice dell'Amministrazione Digitale), ha il compito di emanare regole, standard e guide tecniche in materia di sicurezza informatica ed ha specifiche competenze nell'ambito delle misure atte a garantire l'attuazione del "Quadro strategico nazionale per la sicurezza dello spazio cibernetico" e del "Piano nazionale per la protezione cibernetica e la sicurezza informatica". Il CERT-PA, invece, è una struttura interna all'AgID ed è preposta al trattamento degli incidenti di sicurezza informatica del dominio costituito dalle pubbliche amministrazioni.

Di seguito si riportano brevemente alcune specifiche azioni segnalate all'interno delle linee guida pubblicate dall'AgID in collaborazione con il CERT-PA. Per una lettura più completa, si rimanda al testo pubblicato al seguente indirizzo (https://www.cert-pa.it/web/guest/news?id=8394).

In primo luogo, per evitare la compromissione delle macchine è opportuno eliminare la vulnerabilità sfruttata dal malware, attraverso l'adozione dei seguenti accorgimenti:

- Installazione della patch sviluppata e pubblicata da Microsoft con il Microsoft Security Bulletin MS17-010-Critical;
- Installazione di un antivirus aggiornato successivamente al 12 maggio 2017, in grado di proteggere i sistemi dall'attacco dal malware.
- In secondo luogo, le linee guida segnalano anche alcune misure in grado di ridurre la probabilità di infezione da parte del virus:
  - blocco del protocollo SMB e disattivazione del protocollo SMB ove non specificamente richiesto;
  - blocco del traffico diretto verso indirizzi ed URL indicati nelle raccolte disponibili sui siti specializzati, quali, ad esempio AlienVault, US-CERT e CERT-PA;
  - abilitazione del traffico http verso il dominio: iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com in modo da attivare il "kill switch" presente in alcune versioni del malware e bloccare così la sua attività.

in alternativa, è possibile ridirigere tutto il traffico http diretto verso il web server in esso specificato verso un server fittizio che genera una risposta HTTP code 200 per qualsiasi richiesta in arrivo.

- Infine, anche le macchine spente, al momento dell'accensione, potrebbero essere compromesse se non vengono adottate specifiche misure di contenimento dell'attacco. In particolare, il CERT-PA raccomanda, sotto la guida di un esperto di sicurezza informatica, l'adozione delle seguenti cautele:
  - scollegamento della macchina dalla rete locale prima dell'accensione;
  - massima attenzione ad eventuali eventi anomali in fase di avvio (bootstrap)
  - se l'avvio è avvenuto correttamente, all'accensione effettuare immediatamente una ricerca per file la cui estensione sia ".wncry"
  - prima di collegare il sistema alla rete è opportuno chiudere tutte le applicazioni in avvio automatico, in particolare quelle dedicate alla gestione della posta elettronica;

- collegare la macchina alla rete e aggiornare immediatamente l'antivirus prima di consentire alla macchina di collegarsi alla posta elettronica
- installare la patch di sicurezza di cui al bollettino MS17-010, prima di collegarlo alla rete.

In conclusione, appare opportuno segnalare anche la recente pubblicazione in Gazzetta Ufficiale delle "Misure minime di sicurezza informatica per la PA" ad opera dell'Agenzia per l'Italia Digitale con Circolare 17 marzo 2017, n. 1/2017 (GU Serie Generale n.79 del 4 aprile 2017). Il documento, le cui indicazioni devono essere obbligatoriamente recepite dalle pubbliche amministrazioni entro il 31 dicembre 2017, rappresenta un riferimento pratico anche per i soggetti privati al fine di valutare e migliorare il proprio livello di sicurezza informatica e di contrastare le minacce più comuni e frequenti, che va ad integrarsi alle già previste misure di sicurezza obbligatorie previste dal D. Lgs. 196/2003 e dal Regolamento UE 679/2016 in materia di protezione dei dati personali.

Gianluca Satta
Avvocato del Foro di Cagliari, Consulente e Cultore di Diritto dell'Informatica e delle Nuove Tecnologie presso l'Università degli Studi di Cagliari

Alessandro Bonu
IT Infrastructure System and Security Engineer - Digital Forensics Expert

DirICTo
Diritto & Information and Communication Technology

Il programma nazionale sulla *cyber*sicurezza: il DPCM del 17 febbraio 2017 "indirizzi per la protezione cibernetica e la sicurezza informatica nazionali"

A cura di Pietro Lucania

Nel mese di agosto 2016, con l'entrata in vigore della Direttiva UE denominata NIS[1], è stato incardinato uno dei primi tasselli, componenti un più completo mosaico di norme europee destinate a ristrutturare la sicurezza informatica, attraverso il miglioramento delle capacità di *cyber security*, l'incremento della cooperazione e la gestione dei rischi, la classificazione degli incidenti da parte degli operatori di servizi ed una sempre maggiore disponibilità allo scambio informativo tra strutture operanti nel settore[2].

Nel recepire tali indicazioni, il 17 febbraio 2017, il Presidente del Consiglio in carica ha presieduto un'importante riunione del Comitato Interministeriale per la Sicurezza della Repubblica[3], nel corso della quale è stato approvato il programma nazionale per la *cyber security*, attraverso l'adozione di un nuovo Decreto[4] (pubblicato sulla Gazzetta Ufficiale il 13 aprile 2017) che sostituisce il DPCM 24 gennaio 2013 recante le norme che regolamentavano l'architettura nazionale per la sicurezza cibernetica.

Nell'occasione è stato confermato il ruolo centrale del CISR, quale organo collegiale in diretta collaborazione col Presidente del Consiglio per la gestione delle situazioni di crisi sotto un profilo prettamente politico-decisionale e, nel contempo, è stata mutata la connotazione dell'Nsc[5] ossia il Nucleo di

[1] Network and Information Security Directive (NIS).

[2] È proprio la Direttiva NIS, che ha stabilito la nascita dei CSIRT e lo sviluppo del network. L'articolo 9 prevede che ogni paese UE designi una o più di queste strutture come responsabile per la gestione dei rischi e degli incidenti in ambito cyber, a livello nazionale. L'articolo 12, inoltre, si stabilisce che venga creato un gruppo di CSIRT, il cui obiettivo sarà di incrementare la fiducia tra le nazioni europee. L'obiettivo è promuovere una cooperazione operativa veloce ed efficace nell'ambito del blocco contro le minacce informatiche. Infine, si deliberava che il Network dovesse diventare operativo entro sei mesi dalla data di entrata in vigore della Direttiva, quindi proprio a febbraio del 2017.

[3] CISR (Comitato Interministeriale per la Sicurezza della Repubblica), presieduto dal Presidente del Consiglio, di cui fanno parte il Ministro degli Affari Esteri, il Ministro dell'Interno, il Ministro della Difesa, il Ministro della Giustizia, il Ministro dell'Economia e delle Finanze ed il Ministro dello Sviluppo Economico, ed oggi integrato con la partecipazione del Ministro per la Semplificazione e la Pubblica Amministrazione.

[4] Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017 Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali - (pubblicato sulla Gazzetta Ufficiale n. 87 del 13 aprile 2017)

[5] L'NSC è un organismo composto da funzionari in rappresentanza dei ministeri degli Affari esteri, dell'Interno, della Difesa, della Giustizia, dell'Economia

Sicurezza Cibernetica (già alle dipendenze dell'Ufficio del consigliere militare della Presidenza del Consiglio), che passa alle dipendenze del DIS[6] (Dipartimento delle Informazioni per la Sicurezza) al quale spetta la definizione delle linee d'azione funzionali ad apportare i necessari livelli di sicurezza dei sistemi e delle reti di interesse strategico, nonché la verifica e l'eliminazione delle vulnerabilità riscontrate (il tutto, previo coinvolgimento dei settori accademici e della ricerca e della collaborazione di imprese private).

Tale scelta, dai connotati certamente strategici, mira a ridurre le principali problematiche evidenziatesi con il precedente DPCM, puntando verso un assetto più funzionale ed in linea con analoghe *cyber strategies* adottate in Europa.

La costituzione del Nucleo di Sicurezza Cibernetica rappresenta la concreta possibilità di disporre di una struttura fondamentale di *cyber*sicurezza, che è in grado di muoversi con rapidità ed efficienza nella condivisione delle informazioni in ambito nazionale e nello scambio tra analoghe strutture a livello internazionale. Il tutto si completa con la previsione di *budgets* adeguati, seppur non ancora equiparabili ai più consistenti fondi che altri Paesi dell'UE stanno mettendo a disposizione per programmi analoghi.

Nella sua azione, il Nucleo di Sicurezza Cibernetica dovrà rapportarsi con il Ministeri della Difesa, dell'Interno, dell'Economia e Finanze, dello Sviluppo Economico[7], nonché

e delle Finanze, dello Sviluppo economico, del sottosegretario di Stato alla Presidenza del Consiglio - Autorità delegata per la Sicurezza della Repubblica, del direttore generale dell'Agenzia per l'Italia digitale, del Consigliere militare del presidente del Consiglio dei ministri, del direttore generale del Dipartimento delle informazioni per la sicurezza, dei direttori di Aisi e Aise e del ministro per la Semplificazione e la Pubblica amministrazione, oltre ad un nucleo di persone, che si occupa di gestire tecnicamente il flusso di informazioni.

Svolge funzioni di raccordo tra le diverse componenti istituzionali che intervengono nel settore della sicurezza cibernetica; promuove la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica e l'elaborazione delle procedure di coordinamento, in raccordo con le pianificazioni di difesa civile e di protezione civile; mantiene attivo, 24 ore su 24, 7 giorni su 7, l'unità per l'allertamento e la risposta a situazioni di crisi cibernetica; valuta e promuove, procedure di condivisione delle informazioni, anche con gli operatori privati interessati, ai fini della diffusione di allarmi relativi ad eventi cibernetici elle crisi; acquisisce, sia dall'estero sia per il tramite del ministero dello Sviluppo economico (Mise), degli organismi di informazione per la sicurezza, delle Forze di polizia e delle strutture del ministero della Difesa, le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significative ai fini del corretto funzionamento delle reti e dei servizi.

È indicato come il punto di riferimento nazionale per i rapporti con l'Onu, la Nato e l'Unione europea in questo frangente. Inoltre promuove e coordina, in raccordo con il Mise e con l'Agenzia per l'Italia digitale per i profili di rispettiva competenza, lo svolgimento di esercitazioni interministeriali, ovvero la partecipazione nazionale in esercitazioni internazionali che riguardano la simulazione di eventi di natura cibernetica

[6] Il Dipartimento delle informazioni per la sicurezza (DIS) è l'organo di cui si avvalgono il Presidente del Consiglio dei ministri e l'Autorità delegata per l'esercizio delle loro funzioni e per assicurare unitarietà nella programmazione della ricerca informativa, nell'analisi e nelle attività operative di AISE e AISI.

[7] All'interno del quale è ora prevista l'Istituzione di un centro di valutazione e certificazione nazionale per la verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità dei prodotti, apparati e sistemi destinati a essere utilizzati per il funzionamento di reti, servizi e infrastrutture critiche, nonché di ogni altro operatore per cui sussista un interesse nazionale.

con l'Agenzia per l'Italia Digitale del Dipartimento della Funzione Pubblica.

Il Decreto Gentiloni, qui brevemente illustrato, può sinteticamente definirsi un ulteriore e fondamentale contributo per la definizione del complesso quadro istituzionale dedicato alla sicurezza cibernetica e per la realizzazione di un progetto strutturale che sulla sicurezza e sulla protezione da minacce che spesso vengono recepite con fatale ritardo.

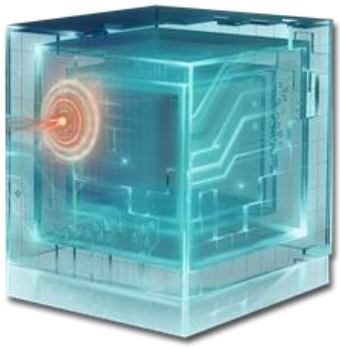
Il successivo passo, a questo punto, può consistere soltanto in azioni conseguenti e concrete da parte di tutti gli attori (istituzionali e non) coinvolti.

Pietro Lucania
Dottore in Scienze Politiche e Scienze Economiche. Master in psicologia giuridica e criminologia. Aree di studio: geopolitica; geoeconomia; new capabilities in warfare; cyberstrategy

DirICTo
Diritto & Information and Communication Technology

Linguaggio comune e standardizzazione delle attività del settore cyber: il National *Cybersecurity Workforce Framework*

A cura di Pietro Lucania



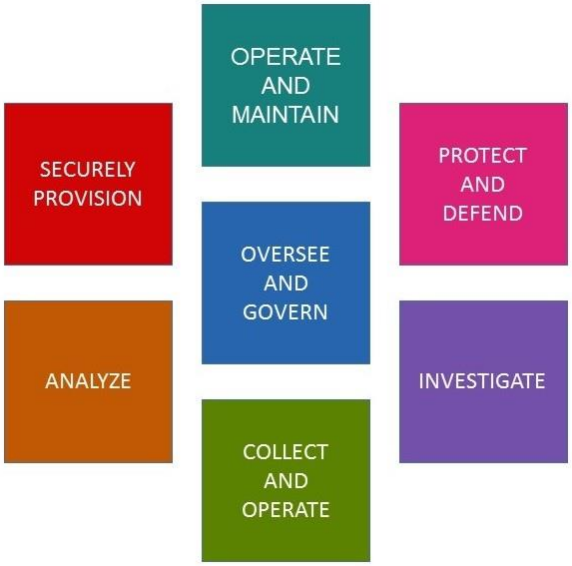
Nel mese di novembre 2016, il National Institute of Standards and Technology statunitense ha pubblicato un aggiornamento del documento denominato NCWF Cybersecurity Workforce Framework, considerato alla stregua di un manuale che mira a fornire ad aziende ed Enti, elementi idonei a meglio definire le attività che vengono svolte in ambito cyber: tra gli obiettivi principali vi è quello di "aiutare le aziende ad identificare, mantenere, reclutare e sviluppare il talento della sicurezza informatica", contribuendo in tal modo alla "formazione di personale destinato alla protezione dei dati e dei sistemi".

Viene così creata una piattaforma dalla quale attingere un lessico comune, grazie al quale verrà facilitata la descrizione e la codificazione delle varie attività che si svolgono nel settore; il framework potrà essere utilizzato anche dalle agenzie governative per classificare il personale che opera nell'ambito della cyber security secondo comuni standard di riferimento.

L'elaborazione del documento è il frutto del progetto NICE acronimo di *National Initiative for Cybersecurity Education*[8] ed è stato ideato per un uso flessibile da parte delle organizzazioni (aziende/enti) a cui si rivolge per soddisfare molte delle esigenze tecniche nel settore della cyber security con particolare riferimento alla standardizzazione delle posizioni di impiego (sia per quanto concerne quelle già adottate e sia per quelle che saranno oggetto di future candidature per le quali dovranno essere approntati bandi e annunci di lavoro), nonché per lo sviluppo di percorsi di carriera che, nel delineare i compiti, consentano di avere chiaro quali sbocchi professionali e quali progressioni sia possibile

[8] The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST), is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our Nation secure. http://csrc.nist.gov/nice.

percorrere.



Per aderire a queste priorità il framework NCWF è stato suddiviso in:

Categories*:* si tratta di 7 macroaree che raggruppano le principali funzioni nell'ambito della sicurezza informatica;

Specialty areas: vi sono distinte 31 aree di specializzazione di lavoro

Work roles: elenca i raggruppamenti più settoriali nell'ambito dell'IT e della sicurezza informatica, comprendenti particolari abilità e competenze necessarie per l'esecuzione di compiti specifici.

Tasks*:* comprende tutte le tipologie riconducibili agli incarichi professionali che possono essere assegnati a professionisti operanti nella cyber security

Knowledge, Skills, and Abilities (KSAs): elenca e descrive quali sono le conoscenze, le competenze e le qualità necessarie per eseguire attività specifiche, rilevabili a seguito di esperienza maturata o di formazione acquisita.

Con riferimento ai primi due ambiti, le 7 macro aree e le 31 aree di specializzazione è stata operata una complicata opera di raggruppamento di ambiti lavorativi, apparentemente diversi e/o distanti tra loro ma che coesistono nel panorama della cyber security, come è evidente dal riepilogo sotto riportato.

ANALIZE

area di specializzazione dedicata ai responsabili delle analisi delle informazioni e conseguente valutazione in possibile funzione di intelligence; si suddivide in:

All Source Intelligence

Analizza le informazioni riguardanti le minacce provenienti da diverse fonti, le normative vigenti e le indicazioni specifiche emanate da tutta la Comunità di Intelligence; opera delle sintesi contestualizzando vari scenari previsionali.

Exploitation Analysis

Analizza le informazioni raccolte per identificare le vulnerabilità e il potenziale di sfruttamento.

Targets

Applica metodologie, tecnologie e criteri facenti parte del patrimonio conoscitivo di vari Enti e Paesi.

Threat Analysis

Identifica e valuta le capacità e le attività poste in essere dai criminali informatici/organizzazioni/intelligence avversari; elabora proposte finalizzate alla

predisposizione di nuovi strumenti normativi o ne consente una migliore applicazione, fornendo ausilio alle attività investigative, di intelligence e di counter intelligence.

COLLECT AND OPERATE

Area dedicata ai responsabili per le operazioni di attacco informatico, preposti alla raccolta di informazioni per la sicurezza informatica e il loro utilizzo per in funzione di intelligence; si suddivide in:

Collection Operations

Attraverso la gestione del processo di raccolta delle informazioni, opera classificazioni in ragione di appropriate strategie.

Cyber Operations

Esegue attività di raccolta prove, relativamente ad attività criminali o poste in essere da intelligence avversarie, al fine di mitigare minacce attuali o future, protezione da attività di spionaggio, sabotaggio, attività terroristiche o a supporto di altre attività di intelligence.

Cyber Operations Planning

Esegue individuazione di obiettivi specifici e processi di pianificazione nel settore cyber; Raccoglie informazioni e sviluppa dettagliati piani ed ordini di operazione per tutte le tipologie di operazioni sia per le operazioni di informazione e sia per le operazioni in ambito cyber.

INVESTIGATE

Area dedicata ad investigare sulle cause di eventi/crimini informatici ed il rilevamento delle prove; ripartita in:

Digital forensics

Ha compiti di raccolta, elaborazione, conservazione ed analisi delle prove informatiche a supporto delle attività di mitigazione dalle vulnerabilità da reati informatici.

Investigation

Fornisce tattiche, tecniche e procedure standard da applicare a processi investigativi, svolge attività di sorveglianza e verifica dell'applicabilità degli strumenti normativi nel settore.

OPERATE AND MAINTAIN

area destinata a fornire il supporto e la manutenzione necessaria a garantire l'efficienza e la sicurezza dei sistemi IT; è ripartita in:

Customer Service and Technical Support

Preposto alla risoluzione di problematiche tecniche ripristino dei sistemi a seguito di guasti in risposta a specifiche richieste (assistenza clienti a vari livelli).

Data Administration

Sviluppa ed amministra Banche Dati e sistemi di gestioni che consentono la raccolta, l'interrogazione e lo sviluppo dei dati.

Knowledge Management

Responsabile della gestione ed amministrazione dei processi e degli strumenti che consentono l'identificazione, la documentazione e l'accesso al capitale intellettuale ed ai contenuti informativi.

Network Services

Responsabile della gestione e manutenzione delle reti, controllo e predisposizione di hardware e software che consentano la condivisione ad ampio raggio di tutte le attività di trasmissione a sostegno dell'informazione e dei sistemi informativi.

System Administration

Installazione gestione e manutenzione dei server al fine di garantirne la riservatezza, l'integrità e la disponibilità; responsabile della gestione delle password e dei controlli di accesso, della creazione di account e dell'amministrazione dei sistemi.

Systems Security Analysis

Area preposta alla conduzione di test e di operazioni tecniche finalizzate alla manutenzione dei sistemi di sicurezza.

OVERSIGHT AND DEVELOPMENT

Area preposta a fornire il management aziendale indispensabile al coordinamento delle varie figure professionali che possono così svolgere in modo più efficace i compiti nella cyber security, fanno parte di essa, le aree di specializzazione:

Education and training

Responsabile della conduzione della formazione interna: sviluppa, pianifica e coordina i corsi di formazione i metodi e le tecniche usate.

Information Systems Security Operations (Information Systems Security Officer)

Sovrintende I processi di *insurance information* nell'ambito di sistemi informativi; comprende la figura dell'*Information Systems Security Officer*.

Legal Advice and Advocacy

Fornisce consulenza legale su una serie di argomenti: inquadramenti giuridici ed aggiornamenti giurisprudenziali

Security Program Management (Chief Information Security Officer)

Gestisce la sicurezza delle informazioni, verifica eventuali implicazioni in seno alle organizzazioni, fornisce programmi specifici in ragione di diverse aree di responsabilità; coordina il personale nelle pianificazioni di emergenza e nella formazione sugli ambiti di sicurezza.

Strategic Planning and Policy Development

Pianificazione strategica, definizione di obiettivi e priorità.

PROTECT AND DEFEND

area responsabile per l'identificazione, l'analisi e la mitigazione delle minacce in ambito cyber; comprende le seguenti aree di specializzazione:

Computer Network Defense Analysis

In grado di predisporre misure difensive al fine di proteggere le informazioni, i sistemi di raccolta e le reti da minacce informatiche; raccoglie numerose informazioni provenienti da diverse fonti, allo scopo di identificare ed analizzare i principali eventi critici che si verificano nella rete.

Computer Network Defense Infrastructure Support

Amministra le infrastrutture necessarie per garantire in modo efficace la sicurezza della rete informatica; esegue test, fornisce aggiornamenti e servizi di potenziamento delle reti, monitorandone le attività.

Incident Response

Responsabile dell'immediata risposta a fronte di minacce rilevate; predispone tutti gli interventi idonei a mitigare le minacce, conservare i dati e garantire lo svolgimento essenziale dei servizi.

Vulnerability Assessment and Management

Effettua una valutazione delle minacce e delle vulnerabilità, valuta i livelli di rischio; sviluppa e segnala le contromisure ritenute più idonee alla mitigazione dei rischi in vari contesti.

SECURELY PROVISION

si occupa della sicurezza delle forniture; della progettazione e costruzione di sistemi informatici sicuri; si suddivide in:

Information Assurance Compliance

Preposto alla supervisione ed alla valutazione della documentazione, nonché alla validazione ed all'accredito dei processi necessari affinché i nuovi sistemi siano in grado di soddisfare i massimi requisiti di garanzia e sicurezza.

Software Assurance e Security Engineering

Sviluppa, crea e modifica codici ed applicazioni informatiche, seguendo le migliori *best practices*

Systems Development

Analizza e verifica lo sviluppo del ciclo di vita dei sistemi informatici.

Systems Requirements Planning

Opera continue consultazioni con i clienti per raccogliere e valutare i requisiti funzionali, traducendo le singole esigenze in soluzioni tecniche.

Systems Security Architecture

Opera sulle capacità dei sistemi di sviluppo; traduce la tecnologia e le condizioni ambientali in sistemi, processi e design di sicurezza.

Technology Research and Development

Conduce la valutazione delle tecnologie e dei processi di integrazione; fornisce e supporta le capacità dei prototipi e ne valuta la loro utilità.

Test and Evaluation

Sviluppa e conduce prove di sistemi per valutarne la conformità mediante l'applicazione di principi e metodi per la pianificazione economica, la validazione dei dati, la verifica e le caratteristiche tecnico-funzionali, l'interoperabilità dei sistemi.

Il framework NCWF potrà quindi essere utilizzato per una chiara identificazione dei soggetti e delle professionalità attinenti alla cyber security come peraltro è già stato previsto dal *Federal Cybersecurity Workforce Assessment Act* del 2015[9].

L'obiettivo è quello di dotare le organizzazioni facenti parte del settore pubblico, privato ed accademico di un ausilio di fondamentale importanza che consenta alle loro strutture preposte alla sicurezza informatica, di operare garantendo efficienza, professionalità e qualità ai massimi livelli.

Le stesse organizzazioni potranno così beneficiare di ulteriori strumenti per l'analisi delle dinamiche endogene ed esogene che consentiranno loro di valutare impatti e situazioni attuali, anticipare esigenze future e predisporre le scelte strategiche ritenute più utili.

Un nuovo approccio verso la sicurezza informatica è senza alcun dubbio una risposta vincente per tutti i settori aziendali consapevoli di poter formare una nuova forza lavoro capace di contrastare i mutevoli e pericolosi rischi attuali; e a beneficiare di tutto questo, non saranno soltanto le singole organizzazioni partecipanti ai progetti, ma l'intero sistema Paese che sta conducendo una politica di sicurezza nel settore, con notevoli sforzi anche in termini di risorse economiche.

Non a caso, nello stesso periodo di novembre 2016, il *Department of Homeland Security*, ha rilasciato le linee guida riguardanti la propria politica di sicurezza informatica, per quanto riguarda i dispositivi "intelligenti".

Il documento si sviluppa in sei principi strategici, attraverso i quali si vuole costruire una difesa nei confronti di hacker e di quei soggetti che operano intrusioni e manomissioni in tali dispositivi.

La "percezione di sicurezza" degli utenti, è un concetto che si sviluppa, in primo luogo, attraverso idonee misure di tutela da parte di chi è proposto alla governance del Paes

Pietro Lucania
Dottore in Scienze Politiche e Scienze Economiche. Master in psicologia giuridica e criminologia. Aree di studio: geopolitica; geoeconomia; new capabilities in warfare; cyberstrategy

[9] The Federal Cybersecurity Workforce Assessment Act of 2015 is one of several cybersecurity measures bundled in the new budget, which requires each agency to identify all positions that carry out some kind of cyber function. Agency leaders will assign each position an employment code under the creation of a new National Initiative for Cybersecurity Education. The bill also includes a timeline to implement this project. http://federalnewsradio.com/cybersecurity/2015/12/new-cyber-workforce-guidelines-included-2016-budget.