Paolo Dr. DAL CHECCO, PhD
Consulente Informatico Forense

Via Giovanni Schiaparelli, 12, 10148 Torino
Tel. +39 011 19117921, Fax. 011 19112371
Email: paolo@dalchecco.it, P.IVA 10470950014
PEC: paolo.dalchecco@pec.it, Web: www.dalchecco.it

Commissioni Riunite I (Affari Costituzionali, della Presidenza del Consiglio e Interni) e IX (Trasporti, Poste e Telecomunicazioni)

Memoria Scritta su Atto del Governo n. 164

Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione – cd. NIS2

19 luglio 2024

*Dr. **Paolo Dal Checco**, Consulente Informatico Forense*

Premetto che come **Docente** a Contratto di Sicurezza Informatica presso la Scuola Universitaria Interdipartimentale di Scienze Strategiche e **Consulente Informatico Forense** il contributo che ritengo di poter dare alla Commissione che è in procinto di valutare l'Atto del Governo n. 164 è prevalentemente di natura **informatica forense**, cioè orientata più che agli aspetti della **sicurezza informatica** verso ciò che riguarda una corretta **gestione degli incidenti informatici**, con la dovuta attenzione alla cristallizzazione delle **evidenze digitali**.

Per quanto questo approccio metta in risalto la fase di *post-incident*, è comunque parte integrante di una corretta implementazione delle misure di sicurezza, come dimostra il fatto che nella gestione della sicurezza digitale è ormai comunemente inserita anche la pratica della **forensic readiness**, cioè la capacità di far fronte a un potenziale evento dannoso grazie alla predisposizione ragionata e mirata a una corretta gestione di un'attività eseguita secondo i principi della **digital forensics**.

L'implementazione della sicurezza informatica in conformità alla direttiva europea c.d. NIS2 è infatti focalizzata principalmente sulla prevenzione degli incidenti informatici e sulle misure di sicurezza, lasciando indefiniti gli aspetti critici che seguono un incidente informatico o ne delineano la gestione, quali l'*informatica forense*, la *forensic readiness* e l'*incident response*. Questo rappresenta probabilmente una lacuna significativa che merita di essere colmata per una protezione completa delle infrastrutture informatiche, senza stravolgere troppo l'Atto ma integrando alcuni punti specifici con semplici nozioni derivate dalla pratica della *digital forensics* ben nota a chi realizza **perizie informatiche** in ambito di processi civili e penali e spesso s'imbatte in casi d'incidenti informatici.

I passaggi nei quali pare più adeguato prendere in considerazione la questione della corretta gestione delle prove informatiche sono quelli nei quali viene coinvolto il CSIRT, che nell'Atto viene più volte

designato quale gruppo di intervento nazionale per la sicurezza informatica in caso di incidente in ambito nazionale. Poiché il CSIRT spesso non può intervenire direttamente durante o a seguito d'incidenti informatici, è opportuno che vengano date delle indicazioni anche direttamente alle strutture coinvolte, affinché predispongano la prima fase di reazione all'incidente e cautelamento delle evidenze.

Giova evidenziare che anche l'ENISA – più volte citata nell'Atto – si occupa oltre che di Sicurezza Informatica anche di tutto ciò che riguarda i princìpi di raccolta informatica forense delle prove, con documentazione pubblica focalizzata sulle attività di perizia informatica su PC, Server, Smartphone, Network, IoT, Web. Questa particolare attenzione dell'ENISA all'argomento potrebbe essere il *trait d'union* tra la Sicurezza Informatica e l'Informatica Forense nell'Atto.

Relativamente all'Art. 25, circa gli "*Obblighi in materia di notifica di incidente*", ritengo che sarebbe opportuno non trascurare l'aspetto della **cristallizzazione delle prove digitali** sulle quali si basano le valutazioni ai punti a-e del Comma 5. La lettera d) del Comma 5 pare la più adeguata per integrare un ulteriore punto che contempli la richiesta di fornire – all'interno della relazione finale – una descrizione delle misure adottate per acquisire la **prova informatica** sulla quale si basano le risultanze delle **analisi forensi**. Come puro suggerimento, sarebbe strategico inserire come primo punto della lettera d) del comma 5 dell'Art. 25, la frase: "*una descrizione delle modalità con le quali sono state cautelate, raccolte ed eventualmente cristallizzate le evidenze digitali*".

In sostanza, la lettera d) del comma 5 dell'Art. 25 che descrive cosa devono comunicare i soggetti interessati al CSIRT Italia ai fini della notifica di cui al comma 1, potrebbe diventare:

> *d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda:*
> *1) una descrizione delle modalità con le quali sono state cautelate, raccolte ed eventualmente cristallizzate le evidenze digitali;*
> *2) una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto;*
> *3) il tipo di minaccia o la causa originale (root cause) che ha probabilmente innescato l'incidente;*
> *4) le misure di attenuazione adottate e in corso;*
> *5) ove noto, l'impatto transfrontaliero dell'incidente;*

Il motivo di questa integrazione è che a seguito della segnalazione potrebbero nascere contenziosi o cause penali o civili, derivare responsabilità, sanzioni o imputazioni che potrebbero generare la necessità della redazione di una o più **perizie informatiche forensi** il cui valore probatorio dipenderà proprio dalla modalità con la quale saranno state raccolte le **prove digitali**.

Tanto più che questo approccio sarebbe pienamente in linea con quanto già enunciato al punto d) del Comma 3 dell'Art. 15 "*Gruppo nazionale di risposta agli incidenti di sicurezza informatica – CSIRT Italia*" dove vengono enunciati i compiti dello CSIRT Italia, tra i quali appunto quello di "*raccogliere e analizzare **dati forensi***", attività che senza una corretta cristallizzazione delle **prove informatiche** diventa complessa se non impossibile o quantomeno il rischio è quello di ridurre la validità e utilizzabilità delle evidenze se non correttamente raccolte.

Un ulteriore periodo ove sarebbe auspicabile integrare con un breve cenno all'informatica forense è il Comma 2 dell'Art. 28 "*Specifiche Tecniche*", ove si specifica che "*l'Autorità nazionale competente NIS tiene conto delle linee guida e degli orientamenti non vincolanti elaborati da ENISA ai sensi dell'articolo 25, paragrafo 2, della direttiva (UE) 2022/2555 e può redigere e aggiornare*

Paolo Dal Checco, PhD – Consulente Informatico Forense, Perizie Informatiche e Indagini Digitali
Iscritto all'Albo dei Periti e dei CTU della Procura di Torino e al Ruolo dei Periti e degli Esperti della CCIAA di Torino
Via Giovanni Schiaparelli, 12, 10148 Torino, Tel. 011 1911 7921, Fax. 011 1911 2371, P. IVA 10470950014
Email: paolo@dalchecco.it, PEC: paolo.dalchecco@pec.it, Web: www.dalchecco.it

periodicamente un elenco delle categorie di tecnologie più idonee ad assicurare l'effettiva attivazione delle misure di gestione dei rischi per la sicurezza informatica", aggiungendo il cappello di chiusura "*e la raccolta delle evidenze digitali.*" in maniera tale da rafforzare anche l'aspetto dirimente delle prove informatiche oltre che quello della sicurezza.

Ancora, al Comma 6 dell'Art. 34 "*Principi generali per lo svolgimento delle attività di vigilanza ed esecuzione*" alla lettera a) ove si parla del rispetto dei diritti della difesa e di come viene tenuto conto di particolari circostanze nella valutazione della gravità della violazione, potrebbe essere opportuno indicare anche – come elemento di particolare gravità – "*la mancata conservazione delle prove informatiche atte a dimostrare e documentare l'evento occorso*". In alternativa – o in aggiunta – potrebbe risultare meno discriminante inserire come lettera i) al Comma 6 sempre dell'Art. 35 la voce "*le modalità con le quali sono state cautelate e presentate o rimosse ed omesse le prove informatiche che documentano la violazione subita*" sempre a indicare l'importanza della corretta presentazione delle evidenze digitali ma soprattutto il danno che può derivare dall'omissione, cancellazione, errata gestione delle stesse.

Sempre in merito all'Art. 35 "*Principi generali per lo svolgimento delle attività di vigilanza ed esecuzione*", ove vengono menzionati gli Audit e il fatto che "*L'Autorità nazionale competente NIS può richiedere, anche solo in parte, di acquisire gli esiti di tali audit sulla sicurezza e di tali scansioni di sicurezza.*", sarebbe opportuno integrare con la possibilità, da parte dell'Autorità Nazionale competente NIS, di richiedere oltre che gli Audit anche il **registro degli incidenti di sicurezza** e delle **violazioni dei dati personali** (Par. 5 Art. 33 GDPR – Notifica del Data Breach) o comunque i report, perizie informatiche, analisi forensi relativi a incidenti precedentemente occorsi, così come anche eventuali notifiche di **data breach** segnalate al Garante in passato. Il punto, in questo contesto, è che la gestione di passati incidenti può essere indice di come verranno gestiti quelli eventualmente prossimi. Vero che nell'Art. 14 "*Cooperazione tra Autorità nazionali*" è già stabilito come il Garante e l'Autorità Nazionale competente NIS devono scambiarsi vicendevolmente le informazioni relative alle violazioni o meglio alle sanzioni, ma è comunque opportuno che l'Autorità Nazionale competente NIS possa richiedere direttamente ai soggetti i registri le segnalazioni.

Sempre sulla linea dell'importanza della "*forensic readiness*", che permette di ridurre i costi delle attività di perizia informatica in caso d'incidente informatico consolidandone invece i risultati, si potrebbe prendere in considerazione una integrazione dell'Art. 37 "*Misure di esecuzione*", nello specifico al Comma 3 relativo alle intimazioni dell'Autorità Nazionale competente NIS ai soggetti, con l'aggiunta di una voce che annoveri la richiesta di "*implementare un corretto piano di forensic readiness atto a rendere più efficiente la gestione di eventuali incidenti informatici*".

Come ultimo punto, non inerente attività d'informatica forense ma più prossimo alle questioni di "***ethical hacking***", ritengo che possa esser ulteriormente approfondito l'Art. 16 "*Divulgazione coordinata delle vulnerabilità*" garantendo tutele solide e concrete a chi segnala vulnerabilità tramite pratiche di "***responsible disclosure***" che spesso rischiano di essere controproducenti per il segnalatore che, quindi, non è incentivato a collaborare creando così indirettamente un danno per la mancata azione riparatoria che sarebbe potuta seguire alla segnalazione.

Ringrazio per l'opportunità concessami, rimango a disposizione ai riferimenti in calce per eventuali approfondimenti e porgo Cordiali Saluti.

Paolo Dal Checco

Paolo Dal Checco, PhD – Consulente Informatico Forense, Perizie Informatiche e Indagini Digitali
Iscritto all'Albo dei Periti e dei CTU della Procura di Torino e al Ruolo dei Periti e degli Esperti della CCIAA di Torino
Via Giovanni Schiaparelli, 12, 10148 Torino, Tel. 011 1911 7921, Fax. 011 1911 2371, P. IVA 10470950014
Email: paolo@dalchecco.it, PEC: paolo.dalchecco@pec.it, Web: www.dalchecco.it

Dr. Paolo Dal Checco, Ph.D
(Short Bio)

*Dopo la **Laurea quinquennale in Informatica conseguita con Lode** nel 2003, a Torino, ha ottenuto nel 2006 un **Dottorato di Ricerca in Informatica**, sempre a Torino, presso il Gruppo di Sicurezza. Ha partecipato durante e dopo il dottorato a numerosi progetti nazionali e internazionali di **ricerca e sviluppo**, che hanno portato anche alla produzione di pubblicazioni e registrazione di brevetti, svolgendo docenza in ambiti universitari, ICT e aziendali.*

*Iscritto all'**Albo dei CTU e dei Periti del Tribunale di Torino**, attualmente svolge attività di Consulenze Informatiche Forensi e Perizie Informatiche in ambito forense collaborando con Procure, Tribunali e Forze dell'Ordine oltre che con aziende, privati e Avvocati.*

*Ha all'attivo circa **15 anni di consulenze informatiche forensi** e in ambito di sicurezza informatica per privati, aziende, Avvocati e le maggiori Procure e Tribunali d'Italia (Torino, Milano, Bologna, Venezia, Genova, Firenze, Como, Udine, Ravenna, etc…) in casi anche di rilevanza nazionale.*

*Ha erogato servizi di perizia informatica forense, oltre che docenza, in **oltre 2.000 fascicoli giudiziari**, annoverando così come clienti oltre un migliaio di referenti tra aziende, privati, Studi Legali, Procure, Tribunali e Forze dell'Ordine.*

*Dal 2020 è titolare e socio amministratore della società **Forenser Srl**, che opera nell'ambito delle perizie informatiche forensi e indagini digitali, raccogliendo professionisti in ambito digital forensics per erogare servizi a privati, aziende, studi legali, Autorità Giudiziaria e Forze dell'Ordine.*

*Dal 2015 al 2018 e dal 2022 a oggi è **Professore a Contratto per l'Università degli Studi di Torino** per il Corso di Sicurezza Informatica presso la Scuola Universitaria Interfacoltà in Scienze Strategiche, Struttura Universitaria Interdipartimentale in **Scienze Strategiche (SUISS)**.*

*Cultore della Materia e in commissione d'esame presso l'Università degli Studi di Milano, Dipartimento di Scienze Giuridiche "Cesare Beccaria" e docente a contratto del Corso di Perfezionamento in "Criminalità Informatica e Investigazioni Digitali" dell'**Università di Milano**.*

*Docente a contratto, inoltre, del Master e Corso di "Cybersecurity and critical infrastructure protection" presso l'**Università degli Studi di Genova**, infine dal 2020 docente a contratto nel Master di II livello in "Specialista in Cybersecurity, Digital Forensics e Data Protection" presso l'**Università Telematica UniCusano**".*

*Ha eseguito ed esegue saltuariamente docenze in ambiti investigativi sulle cryptocurrency, su OSINT e su attività di perizia informatica forense presso **CEPOL**/Scuola di Polizia Economica Finanziaria di Ostia Lido, presso la Scuola di Polizia Internazionale di Caserta, il Master Cybersecurity **Sole 24 Ore Formazione**, il Master **24 Ore Business School**, il Master di II livello in **Sicurezza delle cure, governo clinico e gestione del contenzioso**, il Master **Cybersecurity** SAA - Modulo Security Analytics intelligence, il **Master DPO** presso il Politecnico di Milano organizzato da Poliedra*

*Svolge da alcuni anni attività di docenza a contratto su chiamata presso la **Scuola Internazionale di Alta Formazione per la Prevenzione e Contrasto del Crimine Organizzato** di Caserta, è accreditato nell'albo docenti presso la **Provincia Autonoma di Bolzano**, presso la **Scuola Superiore di Magistratura** ed è tra i docenti accreditati per i corsi **Altalex** e **IPSOA** di formazione all'avvocatura.*

*È nel **consiglio direttivo** dell'**Osservatorio Nazionale di Informatica Forense (ONIF)**, di cui è cofondatore insieme ai principali periti informatici forensi italiani, e **LAB4INT**, associazione che si occupa di formazione e divulgazione di materie scientifiche e investigazioni forensi nell'ambito dell'Autorità e della Polizia Giudiziaria.*