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 I e II Camera dei Deputati

Contributo Scritto al Disegno di Legge n. 1717

"Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici"

8 aprile 2024

*Dr. **Paolo Dal Checco**, Esperto in Informatica Forense e Sicurezza Informatica*

Ringrazio innanzitutto per l'invito a partecipare a questa indagine conoscitiva con un contributo scritto relativo al disegno di legge C. 1717 Governo recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici": spero di poter dare il mio umile contributo tramite la presente memoria che mi è stata richiesta.

Ho ascoltato e letto gli atti di alcuni degli interventi precedenti, tenuti da esimi esperti di Sicurezza Informatica, membri delle Forze dell'Ordine, dirigenti di aziende in ambito cybersecurity, Procuratori della Repubblica, Responsabili di Osservatori, etc… apprezzandone il contenuto.

Mi auguro quindi – come esperto d'Informatica Forense, oltre che di Sicurezza Informatica – di poter dare un contributo che sia utile alle Commissioni, traendo idee e spunti dall'esperienza di oltre 13 anni di perizie informatiche forensi in ambito di processi civili e penali, nei quali cybersecurity e reati informatici trovano un punto d'incontro per sfociare poi in ambito giudiziario.

Occupandomi prevalentemente d'informatica forense – o "*digital forensics*" per utilizzare il termine anglosassone – mi sono concentrato particolarmente sugli aspetti del DDL legati ai reati informatici, trovando nel testo principale e nel supplemento che ho avuto il piacere di leggere ottimi spunti e integrazioni ma anche alcune parti che potrebbero essere maggiormente approfondite.

Ho osservato innanzitutto con piacere che vi è un intervento marcato sul delitto di accesso abusivo ad un sistema informatico, di cui all'articolo 615-ter del codice (comma 1, lettera a) che, oltre al raddoppio dei limiti edittale, amplia "*la circostanza di cui al numero 2) al fine di affiancare all'uso della violenza anche l'impiego della minaccia, mentre in quella di cui al numero 3) è stata contemplata altresì l'ipotesi in cui dal fatto derivi « la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare » dei dati, delle informazioni o dei programmi contenuti nel sistema informativo*".

Tale adeguamento parrebbe essere legato agli attacchi informatici di tipo "ransomware" che contemplino anche una successiva "extorsion", in sostanza estendendo l'accesso abusivo a una successiva duplice estorsione, legata da un lato alla minaccia di non permettere il recupero dei dati se non a fronte di pagamento di un riscatto, dall'altro estende la minaccia a una possibile riproduzione o trasmissione dei dati sottratti, che quindi si va a sommare all'inaccessibilità al titolare dei dati sottratti.

Sarebbe forse opportuno trattare ulteriormente questa seconda tipologia di estorsione, che ha come conseguenza – quando la vittima non si rende disponibile a pagare il riscatto – la pubblicazione del materiale riservato sottratto alla vittima, che sia privata o aziendale. Questo tipo di condotta sta diventando all'ordine del giorno e potrebbe quindi essere contemplata in modo più diretto.

Vero che, in ogni caso, nel DDL viene rafforzata la gestione giuridica degli episodi di ransomware (noti anche talvolta come "*cryptolocker*", "*cyber extorsion*" o, in contesti privati, "sextorsion") introducendo al terzo comma dell'articolo 629 un'autonoma figura di estorsione per i casi in cui essa venga realizzata «mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies, ovvero con la minaccia di compierle»

Noto poi che, come si trova evidenziato nelle memorie già prodotte dagli auditi, vi è un marcato aumento delle pene, con un inasprimento degli aspetti repressivi, ma non vi è altrettanto dispiego di risorse nella fase di prevenzione. Lo scrivente concorda con il fatto che in un complesso meccanismo come quello che sottende ai reati informatici, la prevenzione sia uno degli aspetti strategici. Si pensi ad esempio al D.Lgs 231, ove l'art. 24 bis disciplina i "delitti informatici" permettendo all'ente di evitare le sanzioni nel caso in cui dimostri di aver correttamente previsto la commissione dei reati presupposto tramite la redazione di un adeguato Modello Organizzativo 231, con un opportuno Organismo di Vigilanza a supporto dello stesso.

È certamente d'interesse il fatto che il DDL miri a incentivare la collaborazione, nelle fasi d'indagine, introducendo un'attenuante con riduzione delle pene dalla metà a due terzi a favore di colui che "*si adoper[i] per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi*".

Infine, dal punto di vista informatico forense, sarebbe opportuno ampliare gli aspetti legati alla normativa di riferimento per le acquisizioni forensi, cioè la raccolta degli elementi di prova a uso giudiziario, a oggi regolamentate esclusivamente dalla Legge 48 del 2008. Vi sono articoli come il 244 CPP "Casi e forme delle ispezioni" dove si riporta che "*l'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica (359), anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*": potrebbe essere utile, essendo passati 16 anni dall'entrata in vigore della Legge, aggiornarla tenendo conto della realtà delle situazioni tecnologiche nelle quali ci s'imbatte durante le attività di rilievo.

Parimenti si evince dall'Art. 247 "Casi e forme delle perquisizioni", dove si legge come "*quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*".

Maggiori dettagli emergono nell' Art. 254-bis "Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni", dove viene riportato che "*l'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità.*"

Le modifiche introdotte al CPP dalla Legge 48/2008 potrebbero quindi, dopo ben 16 anni di operato, essere riviste proprio in occasione del DDL 1717, specificando in modo più dettagliato le modalità con le quali devono essere operate le attività di rilievo, ispezione, sequestro informatico e perquisizione, aggiornando se possibile i riferimenti generici agli "*adeguati supporti*" e al fatto che tali supporti debbano assicurare "*la conformità dei dati acquisiti a quelli originali e la loro immodificabilità*".

L'acquisizione della prova – spesso definita "copia forense" – è il passo più importante nel flusso di attività legato all'informatica forense, con la Legge 28/2008 c'è stato un tentativo di normarlo, si ritiene strategico aggiornare e rifinire quanto modificato appunto da tale Legge, considerato come da 16 anni a questa parte la tecnologia ha fatto enormi passi avanti, è cambiato il contesto, sono praticamente scomparsi dei supporti (es. floppy disk, CDROM, etc…) mentre altre modalità di archiviazione dei dati sono diventate di uso comune (cloud drive, etc…) richiedendo quindi un cambio di approccio mentale e giuridico.

Così come con la blockchain, di cui alcuni auditi hanno già parlato, anche con il cloud si assiste a una decentralizzazione del dato, che da un luogo fisico specifico passa a una geolocalizzazione che talvolta è persino difficile circoscrivere all'interno di un continente.

Sempre relativamente alla localizzazione geografica, che con cloud e blockchain assume un significato decisamente più lato, lo scrivente ritiene che il DDL sia un'ottima occasione per chiarire le questioni legate alla competenza territoriale, o *locus commissi delicti*. Sentenze di Cassazione hanno già chiarito come, in particolare in ambito di reati di accesso abusivo, il luogo in cui tale reato si consuma può non essere quello in cui risiede il server ma l'ultimo momento in cui la condotta umana è stata individuabile dal punto di vista fisico e materiale. In sostanza, la tendenza è quella d'identificare il luogo di commissione del delitto ove l'operatore ha agito illegalmente e non ove risiede il sistema acceduto che, appunto, in caso di cloud o blockchain potrebbe anche non avere una geolocalizzazione precisa.

Infine, ulteriore occasione che potrebbe essere colta è quella di una revisione dell'art. 617-bis cp "Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche" e dell'art. 615 quater cp "Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici" poiché tali reati rischiano di essere formalmente consumati da chiunque si occupi di sicurezza informatica. Chiaramente l'elemento soggettivo può essere dirimente, ma lo scrivente ha rilevato che La lettera b) modifica l'articolo 615-quater c.p. ampliando dal «profitto» al più generico «vantaggio» il dolo specifico previsto per la configurabilità della fattispecie. Se consideriamo che "al fine di procurare un profitto (o vantaggio) a sé o altri" può essere lo scopo per il quale gli esperti di sicurezza operano le loro attività di assessment, è evidente che i due articoli sopra riportati andrebbero quantomeno presi in considerazione per un aggiornamento.

Si pensi ai sistemi di penetration testing o vulnerability assessment, ai data leak utilizzati per audit o indagini OSINT, ai software di probe, tutti sistemi o dati che i ricercatori utilizzano per poter svolgere il proprio lavoro ma il cui utilizzo/detenzione potrebbe configurare un reato specifico. Così come sono stati inseriti inasprimenti di pene in altri contesti di reato, andrebbero forse ravvisate delle attenuanti o esclusioni proprio nell'ambito di questi due reati.

Ringrazio per l'opportunità concessami e porgo Cordiali Saluti.

Paolo Dal Checco

Dr. Paolo Dal Checco, Ph.D

Consulente Informatico Forense, Dottore di Ricerca in Informatica, iscritto all'Albo dei CTU e dei Periti del Tribunale di Torino, nel direttivo e tra i soci fondatori dell'Osservatorio Nazionale d'Informatica Forense, ONIF, CEO della società Forenser Srl, esperto di sicurezza informatica e digital forensics / informatica forense, Professore a Contratto per l'anno 2023/2024 del corso di Sicurezza Informatica presso la Scuola Universitaria Interfacoltà in Scienze Strategiche dell'Università degli Studi di Torino.

Paolo Dal Checco opera da oltre 13 anni come esperto in digital forensics e investigazioni digitali come CTP e CTU informatico, collaborando con Tribunali, Studi Legali, Aziende e privati in attività di perizia informatica su dispositivi digitali, OSINT, cryptocurrency e threat intelligence, in particolare operando in ambito di acquisizione e analisi forense delle prove informatiche in processi civili e penali con produzione di elaborato peritale, partecipazione a Udienze e Operazioni Peritali, Descrizioni Giudiziarie, CTU, Sequestri e Incidenti Probatori. CV integrale sul sito www.dalchecco.it o Linkedin.