Agenda digitale 8 marzo 2019

Quali rischi per gli operatori della Cybersecurity

https://www.agendadigitale.eu/sicurezza/la-difesa-anti-malware-e-sempre-legittima-troppe-incognite-sulla-cyber-security/

Un attacco informatico "è come il ghiaccio sporco sulle strade, quando te ne accorgi è sempre troppo tardi" scriveva Dan Verton.

Si fa un gran parlare di Cybersecurity a tutti i livelli. I tempi i cui fu pubblicato un bel libro di Dan Verton (2002) sulla Cybersecurity e sul Cyberterrorismo sono molto lontani ma è sempre attuale il suo monito, presente nella testa di ogni operatore: un attacco Cyber è come il ghiaccio sporco sulle strade, quando te ne accorgi è sempre troppo tardi. Negli anni successivi i fatti hanno dimostrato le sue preoccupazioni e non soltanto le aziende ma interi Paesi sovrani sono letteralmente terrorizzati dagli effetti degli attacchi cibernetici. Sia sotto un profilo tecnico infrastrutturale (e quindi anche economico) sia sotto il profilo politico, sia sotto quello della segretezza delle informazioni che potrebbero essere esfiltrate. Numerosi sono gli episodi accaduti che hanno aumentato la compliance delle aziende nel comparto sicurezza e sicurezza informatica ma soprattutto molti sono i prodotti e gli investimenti in termini anche di risorse specializzate che aziende, forze di polizia, pubbliche amministrazioni e servizi di sicurezza stanno impegnando su questo settore. *Security Operation Center* (SOC), veri e propri centri interni o esterni di sicurezza informatica, consulenti, ingegneri e ditte altamente specializzate nel settore formano scudi e protezione, per quanto possibile, alla massiccia offensiva cibernetica a cui oggi sono soggette le infrastrutture critiche del paese, le multinazionali e anche le piccole /medie aziende di informatica che spesso in qualità di sub -

responsabili del trattamento gestiscono milioni di dati per conto di grandi top player.

Nell'azione di contrasto ai tentativi di attacco informatico, nell'analisi dei malware, dei virus e dei sistemi dai quali questi malware provengono gli operatori tecnici informatici e consulenti possono effettuare qualsiasi operazione ? E' tutto legittimo oppure vi sono dei rischi concreti di commettere dei reati ? Fare penetration test o sfruttare le vulnerabilità o le password in chiaro lasciate nei codici sorgenti dei malware possono essere utilizzate per disinnescare la minaccia? fino a dove può spingersi il consulente senza incorrere in un reato ? Sono tutte domande non trascurabili soprattutto perché i limiti informatici del cyberspazio sono spesso molto più labili e indeterminati dei limiti fisici.

Se nel corso delle sue operazioni commette condotte di intrusione abusiva nel domicilio informatico altrui, o di danneggiamento di dati, informazioni, programmi e sistemi informatici altrui o di alterazione dei sistemi informatici e telematici, anche se finalizzato a tutelare la propria azienda da un tentativo di attacco o da una minaccia vi è il rischio che successivamente al deposito della relazione consulenziale o dopo la pubblicazione degli studi sul malware qualcuno faccia o faccia fare accertamenti giudiziari sui fatti relativi all'attacco informatico e il consulente poi si possa trovare indagato per accesso abusivo a sistema informatico o danneggiamento informatico. Anche se la condotta di intrusione è motivata da una necessità di comprendere più a fondo le cause, la provenienza dell'attacco e magari il luogo o lo spazio in cloud dove sono custoditi i dati illecitamente esfiltrati, qualcuno potrebbe ritenere configurabile un illecito penalmente rilevante.

A prescindere dai casi di completa assenza dell'elemento psicologico richiesto per tali delitti (quindi del dolo) e quindi prescindendo dai semplici e banali casi di mera colpa anche se colpa cosciente o di una responsabilità colposa omissiva, non si può trascurare l'ipotesi in cui,

il consulente abbia e si sia prefigurato una volontà ben precisa di sfruttare quelle credenziali rinvenute o quella vulnerabilità trovata per accedere lo stesso all'interno di uno spazio informatico o effettuare certe operazioni al fine di tutelare l'azienda per la quale lavora o con la quale ha un contratto di consulenza. In molti i casi questi malware esfiltrano dati dai server della vittima e li mettono in modo automatico (e a prescindere dall'owner del programma) in spazi in cloud dedicati e prestabiliti. E' abbastanza chiaro che un consulente, una società di cybersecurity tenti tutto il possibile sempre ovviamente nei limiti della legittimità, per rientrare in possesso dei dati, per toglierli dalla disponibilità di terzi soggetti criminali o comunque segua le tracce informatiche lasciate dagli hacker (quelli cattivi) e dai loro sistemi software. La domanda da porsi è : il consulente deve fermarsi sulla porta non oltrepassando la soglia del domicilio informatico ? Deve astenersi dal porre in essere condotte di difesa attiva (differenze dalla difesa passiva) con sistemi Honeypot ("barattolo del miele" che funge da trappola o esca) e deve sempre e comunque fermarsi e non andare più avanti salvo avvisare le forze di polizia ?

In quest'ultima ipotesi vale la pena di rilevare che in tali casi i tempi di reazione devono essere cosi rapidi che avvisare le forze di polizia specializzate (già oberate di lavoro e in ristrettezze spesso di uomini e mezzi), preparare la denuncia (anche solo per i casi di tentativi ?) e depositarla impiegano tempi cosi lunghi sufficienti a far sparire le tracce necessarie per assicurare i criminali alla giustizia.

E' possibile che in tali specifici casi non siano ravvisabili delle condizioni scriminanti per tali operatori ? E' ben possibile che non sia invocabile una legittima difesa proporzionata all'offesa ?

Si potrebbe riflettere sulla scriminante dell'esercizio del diritto e dell'adempimento del dovere nelle quali entrambe le scriminanti poggiano sul principio di non contraddizione tra le norme dell'ordinamento, con l'unica differenza che nel primo caso, si lascia

al soggetto il potere di scelta tra più possibilità di comportamento (essendo libero di esercitare o meno un suo diritto), mentre, nel secondo, tale facoltà manca, perché vi è l'obbligo di porre in essere la condotta lesiva. Si tratta pur sempre di un conflitto tra norme che proibiscono ed autorizzano uno stesso comportamento e in cui la norma sul diritto prevale sulla norma incriminatrice.

In questa sede non si vuole giustificare sempre e comunque l'indagine di soggetti privati fino ad arrivare a rendere libera ogni attività invasiva di indagine contro tutti e tutto. Assolutamente non è questo il senso dei concetti qui riportati. Le perplessità sorgono soltanto in quelle ipotesi ove vi è una reazione di difesa attiva a chiari e inequivocabili tentativi o condotte riuscite di attacco informatico. Quindi nessun caso di indagini informatiche invasive "fai da te" ma una giusta fase di difesa attiva e proattiva e una presa di coscienza che oltre ad un certo livello è bene informare l'Autorità giudiziaria anche attraverso le forze di polizia specializzate.

In conclusione, ad avviso di chi scrive occorre cominciare a ragionare su questi temi e verificare anche attraverso un dibattito che auspico costruttivo e informato se non vi siano già tutti gli strumenti per legittimare tali condotte e consentire una giusta reazione alle minacce del cybercrime.