Polizia di Stato

Operazione "Data Room"

Le *data room* sono utilizzate in diversi contesti commerciali, nel caso in cui più soggetti ovvero imprese debbono condividere una grande quantità di dati riservati, confidenziali (comunque non destinati al pubblico), inerenti l'offerta di servizi o beni in vendita, evitando quindi il rischioso passaggio di informazioni. In breve si tratta di vere e proprie casseforti contenenti informazioni messe in comune, cui accedere in maniera sicura, abbattendo il rischio di divulgazione, anche accidentale, connesso al trasferimento o alla distribuzione del dato stesso. La *data room* tradizionale infatti era una stanza costantemente sorvegliata, situata, di solito, presso la sede del venditore o in quella dei suoi legali che gli interessati ed i loro consulenti potevano visitare allo scopo di consultare documenti, registri ed altri dati resi disponibili. Con l'avvento della tecnologia le data room sono state riprodotte in ambiente virtuale (cd. virtual data room). Una virtual data room consiste in un sito, una piattaforma o comunque uno spazio virtuale riservato, il cui accesso è consentito ad un numero definito di soggetti ai quali viene fornito un chiave sicura, che consente la consultazione del contenuto. I soggetti abilitati possono così accedere ai dati, eseguirne il download senza dover rispettare turni di consultazione. Nel settore della fornitura di servizi essenziali ed in particolare dei servizi di telecomunicazioni, le data room (quali Opera, sistema DTU, Tim Retail, portale Wholesale) raccolgono dati riservati, messi in comune dagli operatori di settore, per la gestione della cd. portabilità e della manutenzione della rete. Tali preziosi *caveau* di informazioni sono gestiti da Tim, manutentore della infrastruttura di rete e soprattutto del cosiddetto *ultimo miglio*, l'ultimo tratto della infrastruttura che atterra presso il singolo utente consumatore. I dati relativi alla gestione tecnica dell'utenza, da sempre hanno sul mercato un grande valore economico (si pensi alle informazioni relative alle segnalazioni di guasto) e possono consentire l'attuazione di pratiche commerciali aggressive, volte al procacciamento di clientela, magari predisposta alla portabilità proprio in ragione di problematiche varie, segnalate e presenti all'interno delle DATA ROOM. E' stata avviata la fase conclusiva dell'operazione "***DATA ROOM***", un'articolata attività di indagine coordinata dalla **Procura della Repubblica di Roma**, e condotta dagli investigatori specializzati del **Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – CNAIPIC del Servizio Polizia Postale e delle Comunicazioni**, con la collaborazione dei **Compartimenti di Napoli, Perugia, Ancona e Roma.** Oltre 100 specialisti della Polizia Postale sono impegnati a dare esecuzione a **20 provvedimenti cautelari**, in particolare 13 ordinanze che dispongono gli arresti domiciliari ed ulteriori 7 ordinanze che dispongono l'obbligo di dimora nel comune di residenza ed il divieto di esercitare imprese o ricoprire incarichi direttivi in imprese e persone giuridiche. I destinatari di dette misure sono oggetto, unitamente ad ulteriori 6 indagati, di perquisizioni locali ed informatiche. Gli indagati sono responsabili, a vario titolo ed in concorso tra loro, della violazione aggravata dei reati previsti all'art. 615 ter c.p. (accesso abusivo a sistema informatico), all'art.615 quater c.p. (detenzione abusiva e diffusione di codici di accesso), riguardando le condotte sistemi di pubblico interesse, e della violazione della legge sulla privacy art. 167-bis D. Lgs. 193/2003 (comunicazioni e diffusione illecita di dati personali oggetto di trattamento su larga scala). Il provvedimenti restrittivi, emessi dal **GIP presso il Tribunale di Roma,** sono stati eseguiti nei confronti degli indagati residenti sul territorio capitolino ed in diverse province campane. Tra i destinatari dei provvedimenti figurano dipendenti infedeli di compagnie telefoniche, (i procacciatori materiali dei "preziosi" dati), gli intermediari che si occupavano di gestire il commercio illecito delle informazioni estratte dalle banche dati ed i titolari di call center telefonici, che sfruttavano tali importanti informazioni per contattare i potenziali clienti e lucrare le previste commissioni per ogni portabilità, **che arrivano fino a 400 euro** per ogni nuovo contratto stipulato**.** A carico degli indagati, nel corso delle complesse attività investigative, sono stati acquisiti concreti e inequivocabili elementi probatori circa l'esecuzione di ripetuti accessi abusivi alle *data room* in uso ai gestori telefonici operanti sul territorio nazionale e gestite direttamente da TIM, contenenti gli ordini di lavoro di delivery ed i reclami di *assurance* provenienti dalle segnalazioni dell'utenza relativamente ai disservizi della rete di telecomunicazioni. Le articolate indagini sono state avviate nel mese di febbraio scorso dal CNAIPIC, su delega della Procura della Repubblica di Roma, a seguito di una denuncia depositata da parte di Telecom Italia, nella quale si segnalavano vari accessi abusivi ai sistemi informatici gestiti da TIM, riscontrate quantomeno a partire dal gennaio 2019. Gli accessi abusivi avvenivano tramite *account* o *virtual desktop* in uso ai dipendenti di gestori di servizi di telefonia e di società partner per l'accesso ai database, chiavi spesso carpite in modo fraudolento, direttamente gestiti dalla stessa società denunciante, in ragione della concessione delle attività di manutenzione della infrastruttura telefonica nazionale. Le banche dati vengono ordinariamente alimentate da tutti i gestori telefonici in relazione alle segnalazioni ricevute dai clienti sui disservizi rilevati, rappresentando oltretutto una vera e propria istantanea, delle condizioni della infrastruttura nazionale di telecomunicazioni. La "filiera criminale", all'interno della quale ogni componente ha uno specifico compito, funzionale al

raggiungimento dell'obiettivo finale, aveva predisposto addirittura degli "automi", grazie alla collaborazione di un esperto programmatore romano, anch'esso colpito da misura cautelare, ossia dei software programmati per effettuare continue, giornaliere interrogazioni ed estrazione di dati. Le estrazioni, per come verificato nel corso delle intercettazioni, venivano sistematicamente portate avanti con un volume medio di centinaia di migliaia di record al mese. Gli indagati gestivano tali volumi modulandoli a seconda della illecita "domanda" di mercato, come emerge ad esempio da una conversazione nella quale uno degli indagati chiede ad un dipendente infedele una integrazione di 15.000 record per arrivare ai 70.000 pattuiti per il mese in corso, preannunciando un ulteriore ordine per 60.000 utenze mobili. Le informazioni estratte dal database, divenivano quindi oggetto di un illecito mercimonio, in quanto particolarmente appetibili per le società di vendita di contratti da remoto che cercano per l'appunto di intercettare la clientela più "vulnerabile", a causa di problemi o disservizi, per proporre quindi il cambio del proprio operatore telefonico. Il complesso "sistema" vedeva da un lato una serie di tecnici infedeli in grado di procacciare i dati, dall'altro una vera e propria rete commerciale che ruotava attorno alla figura di un imprenditore Campano, acquirente della preziosa "merce" ed a sua volta in grado di estrarre "in proprio", anche con l'utilizzo di software di automazione, grosse quantità di informazioni, in virtù di credenziali illecitamente carpite a dipendenti ignari. La "merce" veniva poi piazzata sul mercato dei call center, **13 sono quelli già individuati,** tutti in area campana, ed oggetto di altrettante attività di perquisizione. I dati stessi, adeguatamente "puliti" per essere utilizzati dai diversi call center, passavano di mano in mano, rivenduti a prezzi ridotti in base alla "freschezza" del dato stesso, motore di un movimento che alimenta il fenomeno delle continue proposte commerciali che tutti ben conoscono. Di assoluto livello criminale la mole dei proventi, come emerge da più di una una conversazione nella quale alcuni indagati discutono dei corrispettivi, frutto dell'attività illecita, pattuendo la ripartizione dei proventi illeciti del mese, per decine di migliaia di euro da spartirsi tra gli operatori infedeli ed i collettori/rivenditori dei dati. Le indagini tecniche hanno inoltre permesso altresì di far emergere come l'attività di commercializzazione di liste di utenti e relativi recapiti, riguardasse anche i sistemi informatici in uso a gestori operanti nel settore dell'energia, in corso di ulteriore approfondimento. Le complesse investigazioni hanno visto gli specialisti del Servizio Polizia Postale e delle Comunicazioni impegnati in attività di intercettazioni telefoniche e pedinamenti degli indagati, nonché in complesse attività di riscontro ed analisi sui sistemi informatici afferenti le piattaforme contenenti i dati, rese possibili anche grazie **alla preziosa collaborazione della struttura di sicurezza aziendale di Telecom Italia**. Si tratta della prima operazione su larga scala volta alla tutela dei dati personali trafugati, un fenomeno noto a tutti che vede coinvolti dipendenti infedeli, call center compiacenti ed intermediari e che ha quale oggetto ciò che sul mercato ha assunto un significativo valore commerciale: i dati riservati relativi all'utenza. Per l'esecuzione dei provvedimenti restrittivi e di perquisizione, oltre che per l'espletamento dell'attività informativa, il **CNAIPIC** ha coordinato un team di specialisti al quale hanno preso parte i **Compartimenti della Polizia Postale di Roma, Napoli, Perugia ed Ancona.**

Il CNAIPIC

Nel quadro delle strategie di protezione delle infrastrutture critiche informatizzate, l'istituzione, all'interno del Servizio Polizia Postale e delle Comunicazioni, del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) si propone come modello operativo di assoluto carattere innovativo, anche in relazione al contesto internazionale. Ai sensi dell'art. 7 bis della legge 31 luglio 2005 n. 155 (che ha convertito con modificazioni il decreto legge 27 luglio 2005 n. 144, recante "Misure urgenti per il contrasto del terrorismo internazionale") il CNAIPIC è incaricato, in via esclusiva, dello svolgimento di attività di prevenzione e contrasto dei crimini informatici, di matrice criminale comune, organizzata o terroristica, che hanno per obiettivo i sistemi informatici o le reti telematiche a supporto delle funzioni delle istituzioni e delle aziende che erogano o gestiscono servizi o processi vitali per il Sistema Paese, convenzionalmente definite infrastrutture critiche informatizzate e che, sempre ai sensi della citata norma di legge, sono state individuate come tali con il decreto del Ministro dell'Interno del 09 gennaio 2008. Il CNAIPIC interviene, quindi, in favore della sicurezza di una gamma di infrastrutture connotate da una criticità intersettoriale (in virtù dei sempre più stretti vincoli di interconnessione ed interdipendenza tra i differenti settori infrastrutturali) e su una tipologia di minaccia che può avere tanto un'origine extraterritoriale quanto una proiezione ad "effetto domino" e transnazionale delle sue conseguenze. Il modello operativo si fonda, inoltre, sul principio delle partnership "pubblico-privato": il CNAIPIC, infatti, assume (mediante un Sala operativa disponibile h24 e 7 giorni su 7) una collocazione centrale all'interno di un network di realtà infrastrutturali critiche (istituzionali ed aziendali), ed opera in stretto collegamento con organismi di varia natura (nazionali ed esteri), impegnati tanto nello specifico settore quanto sul tema della sicurezza informatica, con i quali intrattiene costanti rapporti di interscambio informativo e provvede (attraverso Unità di intelligence e di analisi) alla raccolta ed all'elaborazione dei dati utili ai fini di prevenzione e contrasto della minaccia. Il suddetto rapporto di partenariato trova il proprio momento di formalizzazione nella stipula di specifiche convenzioni; dal 2008 ad oggi sono state stipulati 78 accordi. All'interno del CNAIPIC è inoltre operativo l'ufficio del punto di contatto italiano per le emergenze tecnico-operative connesse al verificarsi di episodi di criminalità informatica transnazionale, secondo quanto stabilito dalla Convenzione sul Cybercrime sottoscritta a Budapest il

23 novembre 2001. Il punto di contatto opera 24 ore su 24 e 7 giorni su 7, all’interno della rete High Tech Crime costituita in ambito G7, e successivamente estesa al Consiglio d’Europa. La rete, attualmente composta da 86 Paesi, ha quale scopo primario la pronta risposta alle richieste di c.d. *freezing* dei dati all’omologa struttura, in attesa della formalizzazione tramite rogatoria o MLAT.

26/06/2020