Network World News - 1 Settembre 2005

A guardia del Web, come la Volante in città (1 Settembre 2005 - Extra Edition)

In Italia a vigilare sulla "sicurezza" della Rete è la Polizia Postale e delle Comunicazioni: delle sue competenze e metodologie abbiamo parlato con il direttore Domenico Vulpiani

di Giancarlo Magnaghi ed Ettore Iannelli

Domenico Vulpiani, Direttore del Servizio di Polizia Postale e delle Comunicazioni, è uno dei maggiori esperti europei di "computer crime". Oltre all'attività operativa, Vulpiani contribuisce a diffondere le conoscenze relative al computer crime e alle misure di prevenzione e repressione, parlando delle reti e delle strategie di contrasto al cybercrime e al terrorismo in occasione di conferenze, seminari e congressi sulla sicurezza

Lo abbiamo intervistato per chiarire alcuni degli argomenti più delicati relativi al complesso mondo del crimine informatico.

Quali sono gli ambiti di responsabilità della Polizia Postale?

Ve ne sono di generali, connessi alle funzioni di polizia di sicurezza e polizia giudiziaria dipendente dall'appartenenza alla Polizia di Stato, e di particolari, collegati alle funzioni di cui all'articolo 1 della legge 247/97 ("… organi del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazioni …") per quanto attiene alla sicurezza dei servizi della società dell'informazione e alla legge 269/98 in materia di contrasto alla pedofilia on line.

Ma la responsabilità maggiore scaturisce dalla fiducia riposta dai cittadini nella Polizia Postale e delle Comunicazioni quale custode del Web al pari della Volante, sentinella nella città.

L'ultimo quinquennio è stato un crescendo per la Polizia Postale e delle Comunicazioni. Dalla pedofilia on line all'hacking, passando per lo spionaggio industriale fino alla protezione delle infrastrutture critiche. Inoltre il Servizio Polizia Postale e delle Comunicazioni, che è dotato di una sede centrale a Roma e di altri uffici periferici dislocati in 19 compartimenti regionali e 76 sezioni provinciali, è il punto di contatto con le altre forze di polizia, 24 ore al giorno per sette giorni la settimana, per quanto riguarda i crimini informatici.

HACKING

La penetrazione nei sistemi informativi altrui: se è fatta con il preciso intento di nuocere è detta più propriamente "cracking"

Quali sono i rapporti e il coordinamento con le altre forze dell'ordine che si occupano di computer crime?

Non vi sono normative ad hoc ma vi è un costante rapporto sinergico, in particolare nel campo della "computer forensic", ove la competenza della Polizia Postale e delle Comunicazioni è all'avanguardia. In molti casi per il tramite dell'autorità giudiziaria, la Polizia Postale ha compiuto complesse e delicate analisi specialistiche di hard disk al fine di rinvenire dati importanti per le indagini condotte autonomamente o in ausilio ad altri uffici investigativi della Polizia di Stato, ma anche delle altre forze di polizia.

Che tipo di collaborazione avete con le forze dell'ordine internazionali? Quali sono i vostri interlocutori ufficiali nelle altre nazioni?

La collaborazione internazionale gioca un ruolo fondamentale nella repressione del computer crime in quanto la proliferazione di servizi Internet dislocati in tutto il globo crea inevitabili problemi di giurisdizione, con conseguenti difficoltà per gli organi inquirenti a prescindere dallo Stato di appartenenza. Categorie giuridiche consolidate del diritto penale quali il "locus commissi delicti" o la teoria dell'ubiquità divengono sterili nel ciberspazio, dove il diritto processuale si confronta con un universo di riferimento in cui i mezzi di ricerca della prova sono bloccati da normative disomogenee.

Il codice di procedura penale italiano prevede la possibilità di intercettare dati in presenza sia di determinati reati (terrorismo, traffico di droga, pedofilia, traffico d'armi, criminalità organizzata e computer crime), sia di prestabilite condizioni (indispensabilità per le indagini e gravi indizi di reato).

Ma tale contesto è valido soltanto per il nostro Paese. Pertanto, qualora non vi fosse corrispondenza anche in un determinato Stato in cui fosse allocato il server contenente dati importanti per le indagini, gli organi inquirenti nazionali non potrebbero procedere con l'indagine perché la legislazione vigente non offrirebbe l'opportunità di acquisire le informazioni che risultano utili alle indagini.

Come si stabilisce quale nazione è competente nel caso di computer crime?

E' lo Stato in cui è installato il server, dove si trova l'indagato o la parte lesa, dove è stato commesso il reato...

Per il Diritto penale italiano vige la teoria dell'ubiquità ex art. 6 del codice penale: "Il reato si considera commesso nel territorio dello Stato, quando l'azione o la omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione."

Attesa l'obbligatorietà dell'azione penale ex art. 112 della Costituzione ("Il pubblico ministero ha l'obbligo di esercitare l'azione penale") viene da sé che per il legislatore italiano non è rilevante, ai fini della competenza, se in Italia sia stata compiuta la condotta oppure si sia verificato l'evento.

Nel caso di un computer crime commesso da utenti italiani, per esempio lo scambio di materiale pedo-pornografico mediante un servizio di chat gestito da un server estero, il procedimento italiano avrebbe un iter a sé stante che si arresterebbe solo nel caso in cui gli autori della condotta fossero già stati giudicati per i medesimi fatti anche in un altro Stato. A questo punto scatterebbe il principio del "ne bis idem": nessuno può essere giudicato due volte per lo stesso fatto.

Anche nel caso in cui cittadini italiani fossero vittime, e non autori, di reati informatici durante un soggiorno all'estero, la legge italiana sarebbe applicabile per il disposto dell'art. 10 del codice penale ("Lo straniero che (...) commette in territorio estero, a danno dello Stato o di un cittadino, un delitto per il quale la legge italiana stabilisce la pena dell'ergastolo, o la reclusione non inferiore nel minimo a un anno, è punito secondo la legge medesima, sempre che si trovi nel territorio dello Stato").

Altresì è perseguibile ex art. 9 del codice penale: "Il cittadino che (...) commette in territorio estero un delitto per il quale la legge italiana stabilisce la pena dell'ergastolo o la reclusione non inferiore nel minimo a tre anni è punito secondo la legge medesima".

Pertanto il cittadino italiano che si renda responsabile di un computer crime commesso in territorio estero è perseguibile in Italia, in quanto è prevista un pena edittale di tre anni cosi come per la maggior parte dei reati informatici sanzionati dal codice penale vigente.

Le chiamate di disturbo

L'art. 127 della legge 196/2003 indica che "L'abbonato che riceve chiamate di disturbo può richiedere che il fornitore della rete pubblica di comunicazioni o del servizio di comunicazione elettronica accessibile al pubblico renda temporaneamente inefficace la soppressione della presentazione dell'identificazione della linea chiamante e conservi i dati relativi alla provenienza della chiamata ricevuta. L'inefficacia della soppressione può essere disposta per i soli orari durante i quali si verificano le chiamate di disturbo e per un periodo non superiore a quindici giorni". In tale situazione - spiega Vulpiani - non vi è alcun intervento delle forze di polizia o della magistratura per quanto attiene alla ricerca delle fonti di prova. Il cittadino vittima formula una richiesta specifica alla compagnia telefonica che deve ottemperarvi. In seguito l'utente molestato potrà consegnare tali dati agli organi inquirenti per il seguito di competenza, formulando espressa denuncia in quanto si configura il reato di cui all'art. 660 del codice penale.

Come si conciliano il bisogno di sicurezza e di indagini con il diritto alla privacy? Quali sono le autorizzazioni necessarie per esaminare traffico telefonico, e-mail, SMS e altri tipi di comunicazioni?

Il decreto legislativo 196/2003 prescrive che il rilascio di dati personali avvenga secondo due modalità: l'una per fini amministrativi, l'altra per esigenze di giustizia.

Nel primo caso si richiamano gli articoli 123 (al comma 2: "Il trattamento dei dati relativi al traffico (...) è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi") e 124 (al comma 4: "Ad esclusivi fini di specifica contestazione dell'esattezza di addebiti determinati o riferiti a periodi limitati, l'abbonato può richiedere la comunicazione dei numeri completi delle comunicazioni in questione") del medesimo decreto.

In questo caso, l'utente che ritenga di aver subito un indebito in bolletta può, mediante richiesta alla compagnia telefonica, richiedere il traffico in chiaro sulla propria utenza. Tale richiesta è esente da qualunque spesa. Nella seconda ipotesi si richiamano due situazioni, di cui una riferita alle "chiamate di disturbo" (si veda il box a pagina 36 - ndr).

Nel caso di reati connessi al terrorismo, traffico d'armi o di droga e reati informatici la procedura prevede invece che sia il pubblico ministero a procedere ad apposita richiesta, da vagliare da parte del giudice per le indagini preliminari, al fine di acquisire il traffico telefonico che deve essere detenuto dai fornitori di servizi per un periodo complessivo di 48 mesi secondo l'art. 132 del Codice.

La problematica sorta nell'ambito del dettato di cui all'art. 132, si riferisce alla mancata previsione da parte del Legislatore della obbligatorietà di detenere il traffico telematico, inteso quale log di registrazione e accesso nella rete Internet da parte degli utenti. Pertanto tutto ciò che inerisce i servizi telefonici è protetto da normative espresse, in caso contrario l'unico obbligo temporale si riferisce ai sei mesi per contestazioni in fattura.

Esistono in Italia e in Europa normative riguardo le tecniche di "computer forensic"? E' necessario utilizzare metodologie e prodotti hardware e software certificati per assicurare la validità delle prove raccolte?

La computer forensic, ovvero la ricerca di fonti di prova nei supporti di memorizzazione fissi e removibili, rappresenta un universo intrecciato in cui si confrontano know-how specialistici e problematiche relative al diritto processuale penale inerente la raccolta delle fonti di prova. Le tecniche utilizzate si riferiscono all'utilizzo di tool universalmente riconosciuti affidabili dalle forze di polizia impegnate nell'attività di forensic.

Non vi sono normative espresse che richiedono certificazioni di sorta ma è preferibile, al fine di evitare eccezioni da parte della difesa nella fase dibattimentale, utilizzare prodotti software certificati dal nostro Ministero delle comunicazioni, o di sperimentata affidabilità.

Il curriculum

Domenico Vulpiani, laureato in giurisprudenza, ha accumulato la propria esperienza sul campo nel corso della sua carriera. Nella Polizia ha ricoperto importanti incarichi nell'ambito dei servizi di sicurezza a tutela delle alte cariche dello Stato e nel settore dell'antiterrorismo. Dal 1996 è stato il Capo della DIGOS di Roma, occupandosi di indagini di particolare rilievo.

Dal febbraio 2001 è a capo della Polizia Postale e delle Comunicazioni, che conta su duemila operatori specializzati nella tutela delle comunicazioni e nel contrasto ai crimini informatici, con particolare riguardo a hacking, pedofilia e truffe online. Presso il Servizio è in corso di realizzazione il CNAIPIC (Centro Nazionale Anticrimine Informatico Protezione Infrastrutture Critiche), per la prevenzione e la repressione dei crimini informatici a danno dei sistemi informatici strategici per la vita del Paese.

Come affrontare i problemi di sicurezza "non tecnici" ma legati in un certo senso alla natuta stessa delle persone, come il social engineering e il phishing?

Le tecniche di social engineering (la capacità di ricavare da qualcuno informazioni, apparentemente innocue ma utili a entrare in un sistema informativo o a commettere qualche altro reato, sfruttando la sua ingenuità o la sua volontà di rendersi utile - ndr) si affrontano con le medesime tecniche con cui si realizzano: l'arguzia. E' consigliabile non dare a uno sconosciuto operatore telefonico il proprio codice cliente della banca telefonica soltanto perché si accredita come dipendente della banca depositaria del proprio conto corrente.

Sul versante del phishing (una forma di frode telematica in cui una e-mail apparentemente lecita spinge il destinatario a comunicare informazioni riservate, come codici utente e password per l'home banking, che saranno utilizzate invece da terzi a danno del destinatario stesso - ndr) si deve agire in maniera duplice.

Da un parte mediante una campagna di informazione agli utenti affinché non forniscano dati sensibili a sconosciute e-mail provenienti da pseudo istituti bancari. Sul versante dei fornitori di servizi, è necessario sensibilizzare gli stessi perché controllino in maniera accurata la propria rete al fine di individuare le fonti sospette di queste richieste indebite di informazioni riservate. In tal caso, devono segnalare agli organi di polizia l'indirizzo IP da cui provengono. Nw

La legge 269/98

Articolo 14, comma 2 della legge 3 agosto 1998, n. 269: "Nell'ambito dei compiti di polizia delle telecomunicazioni... L'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione svolge, su richiesta dell'autorità giudiziaria... Le attività occorrenti per il contrasto dei delitti di cui agli articoli 600-bis, primo comma, 600-ter, commi primo, secondo e terzo, e 600-quinquies del codice penale commessi mediante l'impiego di sistemi informatici o mezzi di comunicazione telematica ovvero utilizzando reti di telecomunicazione disponibili al pubblico".