Poliziamoderna

I guardiani del Web

All’inizio erano solo adolescenti cresciuti a pane e informatica, che smontavano e rimontavano computer come fossero costruzioni Lego. Incursori solitari nei sistemi informativi di un’azienda, di una banca o semplicemente di una scuola, un po’ per curiosità, spesso per compiere qualche bravata (qualche virus dispettoso sparso qua e là) di cui vantarsi con gli amici. In definitiva c’era poco di cui preoccuparsi. Dietro lo stereotipo dell’hacker buono, ha però iniziato a farsi largo una realtà ben diversa, fatta di truffe, di furti di identità, insomma di veri e propri crimini informatici, con i quali anche la polizia ha finito per dover fare i conti. Ne abbiamo parlato con il prefetto Alessandro Pansa, direttore centrale della polizia criminale. **Lei è stato tra i primi a intuire che Internet avrebbe cambiato la natura dei fenomeni criminali. Quali strategie investigative ha dovuto mettere in campo la polizia per poterli contrastare?**Nella seconda metà degli anni ’80 la polizia criminale si pose il problema di affrontare il tema della criminalità informatica che, prima dello sviluppo di Internet nel nostro Paese, era poco nota ma già abbastanza pericolosa.La scelta che fu fatta si basò su uno studio approfondito di tutte le problematiche connesse a tale fenomeno e fu affidato a me. Trattandosi di materia specialistica, fu deciso di costituire a livello centrale una struttura altamente specializzata. Questo piccolo nucleo sviluppò competenze molto elevate e riuscì a creare all’interno dell’Amministrazione una sensibilità adeguata alla nascita del fenomeno criminale, tant’è che subito dopo vennero attivate delle antenne sul territorio all’interno delle Criminalpol. Alcuni anni dopo e precisamente nel 1996, la consapevolezza chiara della dimensione nazionale del fenomeno comportò il trasferimento delle competenze dal nucleo di specialisti a livello centrale ad una intera specialità distribuita sul territorio. Si passò alla riconversione della polizia postale, garante del sistema di comunicazione per corrispondenza, in una polizia garante di tutti i sistemi di telecomunicazioni.Oggi infatti disponiamo di una specialità di professionalità elevata distribuita sul territorio che persegue strategie di alto profilo ottenendo risultati di prestigio assoluto.**A che punto è la collaborazione e lo scambio di informazioni con le altre polizie europee necessari per rispondere a un fenomeno esteso ormai su scala mondiale?**Un fenomeno per sua natura delocalizzato e tipicamente virtuale non può che essere contrastato da una polizia virtualmente unica.Non siamo ancora a questo livello di integrazione tra le forze di polizia europee, ma la cooperazione è sviluppata in maniera notevole, sia in ambito comunitario sia in ambito internazionale. La rete dei collegamenti di polizia a livello mondiale è fatta di luci e ombre. Alcuni Paesi, tra cui certamente il nostro, collaborano in maniera efficiente, altri, invece, costituiscono dei veri e propri buchi neri nella rete transnazionale di sicurezza contro i crimini informatici che danno molto da pensare agli operatori del settore.**Come è invece la situazione dal punto di vista della normativa internazionale?** Sebbene esistano anche delle convenzioni internazionali come quella del Consiglio d’Europa presentata a Roma nel 2000 e sottoscritta nel 2001 a Budapest, in corso di ratifica, vi sono molti Stati che non hanno una normativa adeguata, alcune volte per mero ritardo nell’aggiornamento del proprio ordinamento giuridico, altri invece per mancanza di una sensibilità correlata al fenomeno.**Uno dei settori più colpiti dal cyber crime è il mondo finanziario internazionale. Quanto è importante una strategia comune con banche e aziende produttrici di software?**Sia il mondo bancario, sia quello industriale hanno modificato nel tempo il loro atteggiamento nei confronti del cyber crime. Da una fase iniziale di indifferenza di fronte al problema, sono passati ad una consapevolezza del pericolo ma hanno maturato l’idea del fai da te, nel senso di voler risolvere il problema in casa evitando la pubblicità, giudicata troppo negativa, ogni qualvolta si verificano intrusioni fraudolente nei loro sistemi informatici.La cautela nel proteggere l’immagine aziendale permane tuttora, ma la forma di collaborazione, soprattutto a livello strategico con le banche e le aziende, è molto cresciuta.Sono lontani i tempi in cui l’azienda vittima di un “hackeraggio” risolveva i suoi problemi assumendo l’hacker. Siamo molto vicini alla realizzazione di un sistema quasi di teleallarme come quelli antirapina e antifurto, di cui tutte le aziende di credito ora dispongono. Esiste già oggi un centro per la tutela dei sistemi sensibili del Paese costituito presso il Servizio polizia delle telecomunicazioni (Centro nazionale anticrimini informatici per la protezione delle infrastrutture critiche).**Parte dell’opinione pubblica ha ancora una visione avventurosa dei giovani hacker che entrano nei sistemi informatici di aziende e istituzioni per il gusto della sfida, ma è ancora davvero così?**Non è più aderente alla realtà l’immagine, peraltro più mediatica che reale, del giovane che sfida i grandi sistemi informatici per il gusto di dimostrare la sua abilità. Oggi, senza catastrofismi esagerati come alcuni esperti sogliono disegnare, gli scenari verso i quali andiamo sono di due profili ben definiti: il primo riguarda l’uso delle reti telematiche a fini criminali, il secondo crimini commessi in danno dei sistemi telematici.Nel primo caso pensiamo all’uso mediatico di Internet per usi sovversivi (le rivendicazioni di atti terroristici), al trasferimento di materiale illegale (la pedopornografia) e altri. Nel secondo caso le ipotesi riguardano il furto di informazioni, il danneggiamento dell’informazione, le truffe telematiche e via di seguito.**Quali sono gli scenari cui dovremo fare fronte nel prossimo futuro?**Credo che gli scenari siano quelli prima descritti o loro

possibili evoluzioni, ma il problema principale che dovremmo affrontare nel nostro futuro è quello dell’esatto bilanciamento tra l’uso dei sistemi informatici e il diritto inviolabile della privacy del cittadino.

01/12/2006