

sicurezza sono ormai comuni; meno comuni sono i dibattiti sul perché sono così inefficaci. In breve: molti degli investimenti per la sicurezza antiterrorismo negli Stati Uniti non sono pensati per proteggerci dai terroristi, ma per proteggere i nostri pubblici ufficiali dalle critiche in caso di un altro attacco terroristico.

Boston, 31 gennaio. Come parte di una campagna di marketing innovativa e anticonformista, una serie di insegne lampeggianti dall'aspetto amatoriale, tutte rappresentanti personaggi dell'Aqua Teen Hunger Force, uno spettacolo in onda su Cartoon Network, sono state disposte sui ponti, vicino a un centro medico, nei pressi di uno svincolo autostradale e in altri luoghi pubblici molto affollati.

La polizia ha scambiato queste insegne innocenti per ordigni esplosivi e ha chiuso alcuni settori della città, spendendo più di un milione di dollari per tutta l'operazione. Le autorità hanno maledetto la trovata pubblicitaria considerandola uno scherzo terroristico, mentre altri hanno schernito le forze dell'ordine di Boston per la loro esagerata reazione. Quasi nessuno ha guardato oltre le accuse e le canzonature e si è messo a discutere le ragioni per cui le autorità di Boston hanno reagito in quel modo. La loro reazione è stata eccessiva perché quelle insegne erano strane.

Se qualcuno lasciasse uno zaino imbottito di esplosivo in un cinema affollato, o facesse saltare un camion-bomba nel bel mezzo di una galleria, nessuno pretenderebbe di sapere perché la polizia non ha notato nulla prima. Ma se si scoprisse che uno strano dispositivo con fili e luci intermittenti è in realtà una bomba (proprio come quelle dei film), vi sarebbero lunghe indagini e richieste di dimissioni. La polizia ci ha messo due settimane ad accorgersi di quelle insegne, ma una volta notate si è scatenato il putiferio perché i loro posti di lavoro erano a rischio.

Questa è la sicurezza "CYA", ossia per pararsi le spalle (CYA sta per Cover Your Ass, letteralmente "pararsi il fondoschiena"). Purtroppo è molto diffusa.

La sicurezza aerea sembra destinata a guardarsi indietro continuamente. Prima dell'11 settembre erano bombe, pistole e coltelli. Poi è passata a lamette e taglierini. Richard Reid ha cercato di far saltare un aereo e improvvisamente tutti dobbiamo toglierci le scarpe. Dopo quel che è accaduto con i liquidi la scorsa estate, adesso dobbiamo sorbirci una serie di stupidi divieti per sostanze liquide e gel.

Ma se vi fermate a considerare tutto questo in termini di CYA, allora comincia ad avere un senso. La TSA vuole essere certa che in caso di un altro attacco terroristico ai danni di un aereo, non venga considerata responsabile per non averlo potuto prevenire. Un anno fa nessuno avrebbe potuto accusare la TSA per non aver rilevato esplosivi liquidi. Ma dato che tutto sembra ovvio col senno di poi, difendersi contro ciò che i terroristi hanno provato a mettere in atto l'ultima volta non è altro che pura e semplice salvaguardia del posto di lavoro.

Abbiamo visto questo tipo di sicurezza CYA quando Boston e New York hanno iniziato a effettuare perquisizioni casuali in metropolitana a seguito degli attentati di Londra, o quando sono cominciate a spuntare barriere di cemento armato intorno agli edifici a seguito dell'attentato dinamitardo di Oklahoma City. La vediamo anche negli inutili tentativi di rilevamento di ordigni nucleari; le autorità impiegano la sicurezza CYA contro la minaccia gonfiata dai media, in modo da poter dire "ci abbiamo provato".

Allo stesso tempo stiamo ignorando potenziali pericoli e minacce che però non fanno notizia. Attacchi contro centrali chimiche, per esempio. Ma se mai ci fosse davvero un attacco, la musica cambierebbe rapidamente.

Il pararsi le spalle spiega inoltre l'incapacità della TSA di eliminare nominativi dalla no-fly list, non importa quanto siano innocenti i malcapitati. Nessuno vuole rischiare la propria carriera togliendo qualcuno dalla no-fly list che potrebbe in futuro (malgrado sia una possibilità remotissima) rivelarsi come la prossima mente organizzativa del terrorismo.

Un'altra forma di sicurezza CYA è rappresentata dalle contromisure ultraspecifiche messe in atto durante grandi eventi come le Olimpiadi e gli Oscar, o nella protezione di piccole città. In tutti questi casi, gli incaricati della sicurezza non osano restituire i fondi stanziati con un messaggio come "usate questi soldi per misure di sicurezza generali più efficaci". Se avessero torto e accadesse qualcosa, perderebbero il posto di lavoro.

E infine possiamo vedere in opera la sicurezza CYA a livello nazionale, grazie ai nostri uomini politici. Gli USA potrebbero essere un paese migliore se finanziassero il lavoro di intelligence e traduttori arabi, ma per una strategia di rielezione più efficace è meglio investire denaro in qualcosa di più visibile ma inutile, come un documento di identità nazionale o un muro fra Stati Uniti e Messico.

Proteggere un paese da minacce bizzarre, da minacce che sono già state tentate precedentemente o che hanno catturato la fervida immaginazione dei media, e da minacce troppo specifiche, sono tutti esempi di sicurezza che ha il solo scopo di parare le spalle di qualcuno; sicurezza CYA, appunto. Questo accade non perché le autorità coinvolte (la polizia di Boston, la TSA, ecc.) siano incompetenti o non stiano facendo il proprio lavoro, ma perché non esiste un livello sufficiente di supervisione, pianificazione e coordinamento nazionali.

Le persone e le organizzazioni rispondono a degli incentivi. Non possiamo pretendere che la polizia di Boston, la TSA, il tizio che coordina la sicurezza degli Oscar, le autorità locali, mettano sulla bilancia le proprie esigenze di sicurezza contro la sicurezza dell'intero paese. Tutti risponderanno ai particolari incentivi che arrivano dall'alto. Ciò di cui abbiamo bisogno è una politica antiterrorismo coerente a livello nazionale, basata su valutazioni di vere minacce, invece di strategie che fomentano la paura, mirate alla rielezione, o di stanziamenti di fondi pubblici ottenuti con intrighi politici.

Purtroppo però potrebbe non esserci una soluzione. Tutto il denaro viene convogliato proprio in strategie che fomentano la paura, mirate alla rielezione, e in stanziamenti di fondi pubblici ottenuti con intrighi politici. E, come molte altre cose, la sicurezza segue il denaro.

<http://www.schneier.com/blog/archives/2007/02/nonterrorist_em.html>

Sicurezza aerea:

<http://www.schneier.com/blog/archives/2006/08/terrorism_secur.html>

Perquisizioni in metropolitana:

Dopo che questa vicenda fece notizia, vi fu un'epidemia di attacchi che copiavano la medesima strategia. Su 31 dirottamenti, l'anno seguente, in metà dei casi i dirottatori fecero richiesta di paracadute. Le cose peggiorarono a tal punto che la FAA ordinò a Boeing di installare una speciale chiusura (chiamata Cooper Vane) sulle scalette posteriori dei 727, così da renderne impossibile l'abbassamento in volo.

Internet è piena di copioni. Lo spam fu inventato da degli avvocati che volevano reclamizzare i loro servizi per aspiranti titolari di "green card"; ora lo spam è generalizzato. Altre persone hanno inventato il phishing, il pharming, lo spear phishing. Il virus, il worm, il Trojan: è difficile credere che queste tattiche di attacco via Internet, oggi onnipresenti, erano fino a non molto tempo fa tecniche a cui nessuno aveva mai pensato.

La maggior parte degli aggressori sono copioni, sono degli emuli. Non sono sufficientemente intelligenti da inventare un nuovo sistema per derubare un convenience store, per sottrarre denaro attraverso il Web o per dirottare un aereo. Invece provano e riprovano gli stessi attacchi, oppure leggono di un nuovo attacco sui giornali e decidono di replicarlo.

Nel combattere le minacce, ha senso concentrarsi sui copioni quando già esiste un certo numero di persone intenzionate a commettere il reato, e che passeranno a una nuova tattica una volta dimostrata la sua efficacia. Nei casi in cui non vi sono molti attacchi o aggressori, e quei pochi sono più intelligenti della media (lo stile terroristico di al-Qaeda, per esempio), concentrarsi sui copioni è meno fruttuoso, poiché gli aggressori risponderanno cambiando di volta in volta i loro metodi di attacco.

Si confronti tutto questo coi i bombaroli suicidi in Israele, che sono per la maggior parte attacchi in serie. Le autorità sanno sostanzialmente distinguere un attacco con bombaroli suicidi, e svolgono un ottimo lavoro nella difesa contro le particolari tattiche che tendono a ripetersi di volta in volta. È sempre un braccio di ferro, ma si ottiene comunque molta sicurezza difendendosi dai copioni.

In ogni caso è importante comprendere quale aspetto del reato verrà adottato dagli emuli. I reati "splash-and-grab" non hanno nulla a che vedere con i convenience store: i copioni possono prendere di mira qualsiasi esercizio pubblico in cui sia facile procurarsi del caffè e che abbia un solo impiegato di turno. E per questa tattica non è nemmeno essenziale usare caffè: in un caso è stata utilizzata della candeggina. La nuova idea è quella di tirare qualcosa di nocivo sul volto del commesso, prendere il denaro e scappare.

Analogamente, quando un bombarolo suicida fa saltare un ristorante in Israele, le autorità non assumono automaticamente che i prossimi attacchi a opera di copioni prenderanno di mira altri ristoranti. Si concentrano invece sui dettagli dell'ordigno, sul meccanismo di innesco e sul modo in cui il dinamitardo ha raggiunto il bersaglio. Questi sono gli elementi che gli emuli replicheranno. Il prossimo bersaglio potrebbe essere un cinema o un albergo o un qualsiasi luogo affollato.

Una lezione per la lotta antiterrorismo in America: siate flessibili. Non siamo minacciati da un gruppo di copioni, quindi è meglio concentrare i nostri sforzi in direzione di misure di sicurezza che possano funzionare a prescindere dalle tattiche e dai bersagli:

Noi non crediamo che operazioni di polizia come queste debbano essere considerate 'antiterrorismo', a meno che il soggetto o il bersaglio non siano ragionevolmente collegati ad attività terroristiche".

("EOUSA" è l'acronimo di Executive Office for United States Attorneys, che è una parte del Dipartimento di Giustizia degli Stati Uniti).

Il rapporto offre una straordinaria quantità di particolari, se avete voglia di esaminare le 80 e più pagine del rapporto più altre 80 pagine di appendici.

<<http://www.usdoj.gov/oig/reports/plus/a0720/final.pdf>>

** *** ***** ***** ***** ***** ***** ***** *****

Minaccia da trama cinematografica a Vancouver

L'idiozia di questa faccenda è impressionante: "Un investigatore di reati informatici della polizia di Vancouver ha avvertito la città che i piani per un sistema di connessione Internet wireless esteso a tutta la città mettono l'intera comunità a rischio di un attacco terroristico durante i Giochi Olimpici Invernali del 2010".

Il problema? Beh, il problema pare essere che i terroristi potrebbero venire a vedere i Giochi Olimpici e usare Internet mentre sono in città.

"Se è presente un sistema wireless aperto esteso a tutta la città, in qualità di malintenzionato potrei sedermi in un autobus con un portatile e perpetrare crimini a livello globale", ha spiegato Fenton. "Sarebbe praticamente impossibile trovarmi".

Vi sono poi terribili riferimenti ai sistemi SCADA, e al fatto che la città renda disponibili alcuni dei suoi servizi via Internet. È chiaro che questo tizio ha investito molte energie pensando ai rischi, ma senza un minimo di buonsenso. Sta sopravvalutando il cyberterrorismo. Sta sopravvalutando l'importanza di questo particolare metodo di accesso Internet wireless. Sta sopravvalutando l'importanza dei Giochi Olimpici Invernali del 2010.

Ma il quotidiano era più che felice di stare al gioco e diffondere il terrore. La didascalia della foto che accompagna l'articolo dice: "La polizia avverte: chiunque dotato di un portatile e di accesso wireless potrebbe commettere un atto terroristico".

<<http://www.canada.com/topics/news/national/story.html?id=207f6d54-68fc-40da-8ae3-dc9f057c2f54&k=25065>>

oppure <<http://tinyurl.com/2nmy5j>>

Cyberterrorismo:

<<http://www.schneier.com/crypto-gram-0306.html#1>>

** *** ***** ***** ***** ***** ***** ***** *****

News

Secondo un nuovo rapporto, l'FBI ha smarrito 160 portatili, fra cui almeno dieci contenenti informazioni riservate, negli ultimi quattro anni. Ma non sono notizie del tutto cattive. Una simile indagine condotta nel 2002 diede come risultato 317 portatili smarriti o rubati all'FBI nei due anni precedenti. L'FBI: ora perdiamo meno portatili!

<<http://www.usdoj.gov/oig/reports/FBI/index.htm>>
<<http://www.washingtonpost.com/wp-dyn/content/article/2007/02/12/AR2007021200629.html>>
oppure <<http://tinyurl.com/38hsvh>>
<<http://www.eweek.com/article2/0,1895,2094290,00.asp>>
<<http://arstechnica.com/news.ars/post/20070212-8821.html>>

Esiste una vulnerabilità UAC di sicurezza in Windows Vista. La cosa interessante è che Microsoft l'ha inquadrata come compromesso fra sicurezza e facilità d'uso. Corretto, naturalmente, ma pare che qualcuno abbia preso una pessima decisione a riguardo.

<<http://blogs.zdnet.com/security/?p=29&tag=nl.e589>>
<<http://theinvisiblethings.blogspot.com/2007/02/running-vista-every-day.html>>
oppure <<http://tinyurl.com/yo42z7>>

Lentamente ma inesorabilmente AACS, la protezione di Blu-Ray e HD DVD è stata craccata. Ora è stata compromessa ancor più in profondità. Come ho già detto, quel che sarà interessante osservare è quanto bene HD DVD e Blu-Ray si riprenderanno. Entrambi sono stati realizzati aspettandosi questo genere di crack, ed entrambi sono dotati di meccanismi per ripristinare la sicurezza per i prossimi film. Non resta che vedere quanto bene funzioneranno questi sistemi di ripristino.

<http://www.boingboing.net/2007/02/13/bluray_and_hddvd_bro.html>
I crack precedenti:
<http://www.schneier.com/blog/archives/2006/12/aacs_cracked_1.html>
<http://www.schneier.com/blog/archives/2007/01/bluray_cracked.html>

Il sito Web della TSA è stato preso di mira da degli hacker, o era semplicemente scritto male e con un pessimo design delle pagine web?

<http://blog.wired.com/27bstroke6/2007/02/homeland_securi.html>
<<http://paranoia.dubfire.net/2007/02/tsa-has-outsourced-tsa-traveler.html>>
oppure <<http://tinyurl.com/ywm7qx>>

Back door nel mondo reale: un test di ingegneria sociale in cui gli aggressori entrano in un edificio attraverso una porta sul retro lasciata aperta per i fumatori.

<http://www.theregister.com/2007/02/15/smoke_ban_hack_risk/>

OpenSSL ora è certificato FIPS 140-2. Il procedimento è durato cinque anni. Si tratta di un problema che presenta cicli di certificazione molto lunghi; i cicli di sviluppo del software sono più veloci.

<<http://www.linux.com/article.pl?sid=07/02/08/1935232>>

Qualsiasi cosa è una bomba, oggi giorno? Nel New Mexico una squadra di artificieri ha fatto saltare due lettori di CD attaccati con nastro adesivo ai banchi di una chiesa, che

stavano riproducendo messaggi pornografici durante la Messa. Non è altro che una bravata da liceali e mi auguro che i ragazzini che l'hanno messa in pratica vengano adeguatamente puniti. Ma non sono terroristi. E fatico a credere che la polizia abbia davvero pensato che i lettori CD fossero ordigni esplosivi.

<<http://www.cnn.com/2007/US/02/22/church.foul.language.ap/index.html>>

Nel frattempo, la polizia britannica ha fatto brillare un distributore di nastro adesivo lasciato al di fuori di una stazione di polizia nell'Irlanda del Nord.

<http://news.bbc.co.uk/1/hi/northern_ireland/6387857.stm>

Per non essere da meno, la polizia olandese ha scambiato uno dei propri trasmettitori per una bomba. Almeno non hanno fatto saltare per aria nulla.

<http://www.playfuls.com/news_10_14162-Dutch-Police-Seal-Off-Street-On-Taking-Own-Transmitter-For-Bomb.html>

oppure <<http://tinyurl.com/2b6qn4>>

Bene, gente, abbiamo davvero bisogno di idee, qui. Se ci mettiamo a pensare che qualsiasi oggetto strano sia una bomba, allora la quantità di falsi allarmi finirà con l'estinguere qualsiasi speranza di sicurezza.

<http://www.schneier.com/blog/archives/2007/02/nonterrorist_em.html>

Se avete problemi a identificare una bomba, questo quiz dovrebbe aiutarvi.

<<http://www.bombornot.com>>

E questa è una vignetta sul tema:

<<http://www.geekculture.com/joyoftech/joyarchives/919.html>>

La polizia di Boston ha fatto brillare un contatore di traffico. Sto cominciando a pensare che ci sia qualcosa di profondamente sballato nella catena di comando della polizia a Boston. Dipartimento di Polizia di Boston: c'è sempre "errore" in "terrore".

<http://www.boingboing.net/2007/02/28/boston_police_blow_u.html>

<http://wbztv.com/local/local_story_059122735.html>

<<http://www3.whdh.com:80/news/articles/local/BO44642/>>

<http://www.schneier.com/blog/archives/2007/03/boston_police_b.html>

Elenco di password di default dei router:

<<http://www.phenoelit.de/dpl/dpl.html>>

<<http://www.phenoelit.de/dpl/>>

<<http://www.governmentsecurity.org/articles/DefaultLoginsandPasswordsforNetworkedDevices.php>>

<<http://www.virus.org/default-password/>>

"Windows per le navi da guerra". Non credo sia una buona idea.

<http://www.theregister.co.uk/2007/02/26/windows_boxes_at_sea/>

Un articolo sullo stesso tema del 1998, che riguarda Windows NT e la USS Yorktown.

<<http://www.wired.com/news/technology/0,1282,13987,00.html>>

Si dice che vi sia un bug software nel caccia stealth Raptor F-22. Pare che i sistemi informatici abbiano avuto problemi nel volare a ovest lungo la linea del cambiamento di data. Non si sa quale sistema operativo girava sui computer di bordo.

<<http://it.slashdot.org/article.pl?sid=07/02/25/2038217>>

<<http://www.f-16.net/index.php?name=PNphpBB2&file=viewtopic&p=91277>>

<<http://www.flightglobal.com/articles/2007/02/14/212102/pictures-navigational-software-glitch-forces-lockheed-martin-f-22-raptors-back-to-hawaii.html>>
oppure <<http://tinyurl.com/26p5s6>>
<<http://www.dailytech.com/article.aspx?newsid=6225>>

Con tutta l'attenzione rivolta al riciclaggio di denaro estero, stiamo ignorando il problema all'interno degli Stati Uniti.

<<http://members.forbes.com/forbes/2007/0212/096.html>>

Come ingannare l'accesso alla memoria hardware:

<http://www.darkreading.com/document.asp?doc_id=118291>

Buone nuove per quanto concerne la legislazione canadese antiterrorismo. In primo luogo, i certificati di sicurezza sono stati dichiarati anticostituzionali.

<<http://www.cbc.ca/canada/story/2007/02/23/security-certificate.html>>

E secondariamente, la Camera dei Comuni ha votato contro l'estensione di due provvedimenti di una legge antiterrorismo del 2001. Erano scaduti alla fine di febbraio.

<<http://www.cbc.ca/canada/story/2007/02/27/terror-vote.html>>

<<http://www.thestar.com/News/article/186476>>

Poster sulla paranoia:

<<http://digitalfury.popmartian.com/images/20070202/paranoia.jpg>>

I tag RFID più piccoli al mondo: come granelli di polvere.

<<http://news.bbc.co.uk/1/hi/technology/6389581.stm>>

<http://www.theregister.co.uk/2007/02/19/rfid_powder/>

Attacco di tipo privilege escalation ai danni della Xbox 360:

<<http://www.securityfocus.com/archive/1/461489/30/0/threaded>>

Un articolo molto interessante sul sistema DRM di Apple, che Apple chiama FairPlay.

<<http://www.roughlydrafted.com/RD/RDM.Tech.Q1.07/2A351C60-A4E5-4764-A083-FF8610E66A46.html>>

oppure <<http://tinyurl.com/229pcm>>

In Australia si sta discutendo l'efficienza economica degli sky marshal. Non ho mai visto una simile analisi costi-efficacia da parte degli Stati Uniti.

<<http://www.theage.com.au/news/national/skyhigh-cost-of-flying-cops/2007/02/24/1171734074064.html>>

oppure <<http://tinyurl.com/ywpt4t>>

Articolo affascinante sul cambiamento generazionale del concetto di privacy:

<<http://nymag.com/news/features/27341/>>

L'FBI ha emesso National Security Letters (lettere di sicurezza nazionale) illegali sotto il PATRIOT Act statunitense.

<http://www.schneier.com/blog/archives/2007/03/fbi_issued_ille_1.html>

"Digital Security and Privacy for Human Rights Defenders" [Sicurezza digitale e privacy per i difensori dei diritti umani]:

di autobus e monumenti nazionali. A volte operano come comuni cittadini e possono effettuare soltanto arresti civili, ma in un numero crescente di stati vengono loro affidati poteri ufficiali di polizia.

Questa tendenza dovrebbe essere fonte di grande preoccupazione da parte dei cittadini. Il far rispettare la legge dovrebbe essere una funzione del governo, e la sua privatizzazione mette tutti a rischio.

Il problema più evidente è legato alle priorità. Le forze di polizia pubbliche hanno il compito di proteggere i cittadini delle città e dei paesi sui quali hanno giurisdizione. Naturalmente vi sono casi in cui dei poliziotti hanno oltrepassato i limiti, ma queste sono eccezioni, e gli ufficiali e i dipartimenti di polizia sono in definitiva responsabili nei confronti del pubblico.

Gli agenti di polizia privata sono diversi. Non lavorano per noi, lavorano per delle aziende. E sono interessati alle priorità dei loro datori di lavoro o delle aziende che li assumono. I diritti fondamentali del cittadino, l'incolumità pubblica e i diritti civili non sono le loro preoccupazioni principali.

Inoltre, molte delle leggi che ci proteggono dagli abusi della polizia non si applicano al settore privato. Le garanzie costituzionali che regolano la condotta delle forze di polizia, gli interrogatori e la raccolta di prove non si applicano ai privati. Quelle informazioni che sarebbe illegale raccogliere su di voi da parte del governo, possono essere raccolte da data broker commerciali e quindi vendute alla polizia.

Abbiamo visto tutti quei serial polizieschi in televisione in cui gli agenti "leggono i diritti alle persone". Se siete fermati da una guardia di sicurezza privata non avrete tutti quei diritti.

Per esempio, una legge federale nota come Section 1983 vi permette di denunciare la violazione dei diritti civili da parte delle forze di polizia ma non da parte di privati cittadini. Il Freedom of Information Act ci consente di sapere che cosa stanno facendo le forze dell'ordine pagate dal governo, ma la legge non si applica a privati e aziende. Insomma, la maggior parte delle protezioni dei vostri diritti civili ha effetto soltanto sulla "vera" polizia.

L'addestramento e la regolamentazione sono un altro problema. Le guardie di sicurezza privata spesso ricevono un addestramento minimo, o non sono per niente addestrate. Non si diplomano nelle accademie di polizia. E mentre alcuni stati regolamentano queste compagnie di vigilanza, altri non hanno nessun tipo di normativa: chiunque può indossare un'uniforme e giocare al poliziotto. Abusi di potere, violenza, e comportamento illegale sono fenomeni molto più diffusi nella vigilanza privata che non nella vera polizia.

Un terribile esempio di tutto ciò accadde nel South Carolina nel 1995. Ricky Coleman, una guardia di sicurezza della catena Best Buy, senza licenza né addestramento, e con precedenti penali di violenza, ha ucciso per soffocamento un sospettato di frode mentre un'altra guardia di sicurezza lo teneva fermo al suolo.

Questa tendenza è più grande della polizia stessa. Un numero sempre maggiore dei penitenziari negli Stati Uniti viene gestito da aziende con fini di lucro. L'IRS ha iniziato ad appaltare parte della raccolta di imposte arretrate ad alcune aziende di recupero crediti che percepiranno una percentuale del denaro recuperato come compenso per i loro servizi. E vi sono circa 20.000 uomini, fra polizia e milizia privata, stanziati in Iraq che lavorano per il Dipartimento della Difesa.

Attraverso gran parte della storia, chi deteneva il potere incaricava specifici individui per mantenere la pace, raccogliere le imposte e dichiarare guerre. La corruzione e l'incompetenza erano la norma, e la giustizia un fenomeno assai raro. È proprio per questo che, sin dal 1600, i governi europei si sono costituiti intorno a un servizio civile professionale in grado di far rispettare le leggi e proteggere i diritti.

Le guardie di sicurezza privata capovolgono completamente questo principio fondamentale del governo moderno. Che si tratti di poliziotti della FedEx nel Tennessee che possono richiedere mandati di perquisizione ed effettuare arresti, un elicottero di sorveglianza finanziato da privati a Jackson, Mississippi, che può aggirare le restrizioni costituzionali sullo spionaggio aereo, o "agenti" della Capitol Special Police nel North Carolina che stanno facendo pressioni per estendere la loro giurisdizione oltre i confini delle proprietà private che già proteggono, queste forze di polizia finanziate da privati non ci stanno proteggendo né lavorano per i nostri migliori interessi.

<<http://www.washingtonpost.com/wp-dyn/content/article/2007/01/01/AR2007010100665.html>>

oppure <<http://tinyurl.com/y26xgr>>

<<http://www.nlg-npap.org/html/research/LWprivatepolice.pdf>>

Questo editoriale di opinione è originariamente apparso sul "Minneapolis Star-Tribune":

<<http://www.startribune.com/562/story/1027072.html>>

Quando ho postato questo intervento sul mio blog, ho ricevuto parecchi commenti negativi da parte di simpatizzanti del Libertarian Party che ritengono che in un certo qual modo il mercato renda i poliziotti privati più responsabili nei confronti del pubblico rispetto alle forze di polizia stipendiate dal governo. Mi spiace, ma è una sciocchezza. Best Buy risponderà ai propri clienti; un complesso residenziale risponderà ai propri inquilini. I piccoli criminali che attaccano quelle entità commerciali sono un'esternalità economica e non conteranno negli argomenti economici. Dopo tutto la gente potrebbe essere più propensa a fare shopping da Best Buy se le sue guardie di sicurezza fanno risparmiare denaro arginando la criminalità. A chi importa se nel frattempo rompono la testa di qualcun altro.

Ciò detto, con il mio intervento non è mia intenzione sottintendere che le pubbliche forze di polizia siano magicamente onorevoli e moralmente ineccepibili, dico solo che le forze economiche in atto sono differenti. Così che il pubblico possa considerare attentamente quale sia il minore fra i due mali, ecco lo studio di Radley Balko, "Overkill: The Rise of Paramilitary Police Raids in

America" [Gli eccessi: la crescita dei raid di polizia paramilitare in America]:

<http://www.cato.org/pub_display.php?pub_id=6476>

E una mappa interattiva dei raid della polizia pubblica andati storti:

<<http://www.cato.org/raidmap/>>

** *** ***** ***** ***** ***** ***** ***** ***** *****

Le news di BT Counterpane

Schneier ha ricevuto il 2007 EFF Pioneer Award, insieme a Yochai Benkler e Cory Doctorow.

<http://www.eff.org/news/archives/2007_03.php#005149>

PC World ha nominato Schneier la trentunesima persona più influente del Web:

<<http://www.pcworld.com/printable/article/id,129301/printable.html>>

Un articolo su Schneier dell'Hindustan Times:

<<http://www.schneier.com/news-031.html>>

Come parte della serie Big Thinkers di BT, Esther Dyson ha intervistato Schneier e altre due persone (Risto Siilasmaa, Presidente di F-Secure Corporation; e Michael Barrett, CISO di PayPal) sui problemi di sicurezza di rete.

<http://www.networked.bt.com/bigthinkers_security.php>

Le altre interviste per la stessa serie si trovano qui.

<<http://www.networked.bt.com/bigthinkers.php>>

Schneier terrà un discorso pubblico a Londra il 21 marzo:

<<http://www.lse.ac.uk/collections/informationSystems/newsAndEvents/2007events/SSIT7.htm>>

oppure <<http://tinyurl.com/25c2ap>>

Schneier intervorrà al Temple Sharey Tefilo-Israel a South Orange, New Jersey il 25 marzo.

Schneier intervorrà al NIST a Gaithersburg, Maryland, il 10 aprile:

Schneier intervorrà al Security and Liberty Forum di UNC Chapel Hill il 14 aprile:

<<http://www.seclibforum.org/>>

** *** ***** ***** ***** ***** ***** ***** ***** *****

Il Canile: Sniffex

Niente più che una truffa di sicurezza nazionale: una bacchetta raddomantica per esplosivi. Questo è una truffa azionaria pump and dump. Il sito di Sniffex è giù, ma Google ne ha una cache, e pare che siano tornati alla carica come Homeland Safety International. Hanno pure un brevetto.

<<http://www.sniffex.com/>>

<<http://72.14.253.104/search?q=cache:T397Ap3BNTIJ:www.sniffex.com/+SNIFFEX&hl=en&ct=clnk&cd=1&gl=us&client=opera>>
oppure <<http://tinyurl.com/ysl3le>>
<<http://www.homelandsafetyintl.com/>>
<<http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnu m.htm&r=1&f=G&l=50&s1=6,344,818.PN.&OS=PN/6,344,818&RS=PN/6,344,818>>
<http://blog.wired.com/defense/2007/02/sniffing_bomb_d.html> oppure
<<http://tinyurl.com/28mg44>>

** *** ***** ***** ***** ***** ***** ***** *****

Drive-By pharming

Sid Stamm, Zulfikar Ramzan e Markus Jakobsson hanno sviluppato un attacco brillante e potenzialmente devastante contro i router domestici, una cosa che chiamano "drive-by pharming".

Anzitutto l'aggressore crea una pagina web contenente un semplice pezzo di codice JavaScript malevolo. Quando la pagina viene vista, il codice effettua un tentativo di login nel router ADSL dell'utente, quindi cerca di cambiarne le impostazioni dei server DNS in modo da puntare verso un server DNS controllato dall'aggressore. Una volta che il computer dell'utente riceve dal router le informazioni aggiornate sulle impostazioni DNS (dopo che la macchina è stata riavviata), le future richieste DNS vengono rivolte al server DNS dell'aggressore, che le risolve.

E quindi sostanzialmente l'aggressore entra in possesso della connessione Internet della vittima.

La condizione principale affinché l'attacco abbia successo è che l'aggressore riesca a indovinare la password del router. Ciò è sorprendentemente facile, dato che i router domestici arrivano tutti con una password di default comune che in moltissimi casi non viene mai cambiata.

Hanno scritto codice proof of concept che può eseguire con successo tutti i passaggi dell'attacco su router domestici Linksys, D-Link e NETGEAR. Se gli utenti modificano le password del loro router ADSL, inserendo password più difficili da indovinare, saranno al sicuro da questo attacco.

Cisco sostiene che 77 dei suoi router sono vulnerabili.

Si noti che l'attacco non richiede da parte dell'utente lo scaricamento di alcun software malevolo: è sufficiente guardare la pagina web che contiene il codice JavaScript malevolo.

<http://www.symantec.com/enterprise/security_response/weblog/2007/02/driveby_pharming_how_clicking_1.html>
oppure <<http://tinyurl.com/2uqwug>>

<http://www.symantec.com/avcenter/reference/Driveby_Pharming.pdf>
<<http://it.slashdot.org/article.pl?sid=07/02/16/1421238>>
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9011588&intsrc=hm_list>
oppure <<http://tinyurl.com/2vy7xv>>

Un commento dal mio blog: "L'attacco viene chiamato CSRF, cioè Cross-Site Request-Forgeries. È documentato da alcuni anni. Ricordo di esservi incappato due o tre anni fa, e di essere rimasto molto sorpreso dal fatto che non avesse ottenuto maggiore pubblicità, ma fortunatamente le cose sono cambiate lo scorso anno. Non solo i router, ogni genere di applicazioni web intranet è vulnerabile a questa linea d'attacco (specialmente quando si tratta di software standard, o nel caso qualcuno abbia informazioni dall'interno; e quando gli utenti rimangono autenticati la maggior parte del tempo)".

** *** *****

Clonare i chip RFID prodotti da HID

Vi ricordate del fiasco di Cisco all'edizione 2005 di BlackHat? Il prossimo nella coda degli idioti è HID, azienda costruttrice di schede RFID, che ha impedito a Chris Paget di presentare una ricerca su come clonare quelle schede. L'ACLU si è presentata al suo posto.

Quando queste aziende impareranno la lezione? HID non potrà impedire che il pubblico venga a sapere di tale vulnerabilità, e finirà col fare la figura del gorilla dalla mano pesante. E non è nemmeno un segreto; Paget ha dimostrato l'attacco al sottoscritto e ad altri durante la RSA Conference il mese scorso.

Vi è una differenza tra una falla di sicurezza e l'informazione riguardate la falla di sicurezza; HID deve porre rimedio alla prima e non deve preoccuparsi della seconda. L'esposizione totale è un vantaggio per tutti.

<http://www.darkreading.com/document.asp?doc_id=1182851>
<<http://www.networkworld.com/news/2007/022707-battle-brewing-over-rfid-chip-hacking.html>>
oppure <<http://tinyurl.com/2dvqww>>
<http://www.aclunc.org/issues/technology/bytes_and_pieces/blackhat_presenters_threatened_with_patent_suit_for_exposing_rfid_vulnerabilities.shtml>
oppure <<http://tinyurl.com/2q8tkj>>

La dimostrazione dell'attacco:

<<http://weblog.infoworld.com/techwatch/archives/010227.html>>

La storia di Cisco:

<http://www.schneier.com/blog/archives/2005/07/cisco_harasses.html>
<http://www.schneier.com/blog/archives/2005/08/more_lynnisco.html>

L'esposizione totale:

<<http://www.schneier.com/crypto-gram-0111.html#1>>

** *** *****

Commenti dei lettori

Su questi argomenti vi sono centinaia di commenti nel mio blog, molti davvero interessanti. Cercate l'argomento sul quale intendete dare la vostra opinione, e unitevi al dibattito.

<<http://www.schneier.com/blog>>

** *** *****

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia. I numeri arretrati sono disponibili all'indirizzo <<http://www.schneier.com/crypto-gram.html>>. Per iscriversi, cancellare l'iscrizione o cambiare il proprio indirizzo a cui recapitare la newsletter, visitate sempre <<http://www.schneier.com/crypto-gram.html>>

La versione italiana è curata da Communication Valley SpA

<<http://www.communicationvalley.it/>>

Per iscriversi o cancellarsi andare all'indirizzo <<http://www.cryptogram.it/>>

I numeri arretrati sono disponibili all'indirizzo <<http://www.cryptogram.it/>>

Per informazioni <crypto-gram@communicationvalley.it>

I commenti a CRYPTO-GRAM devono essere inviati a schneier@counterpane.com. Si sottintende il permesso di riprodurre tali commenti, salvo indicazione contraria. I commenti possono venire adattati per ragioni di spazio e di chiarezza.

Inoltrate liberamente CRYPTO-GRAM a colleghi ed amici che possano trovare questa pubblicazione di un certo interesse. Viene concessa l'autorizzazione a ristampare CRYPTO-GRAM, a condizione che sia stampata integralmente.

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è l'autore dei best seller "Beyond Fear", "Secrets and Lies" [tradotto in Italia col titolo "Sicurezza Digitale"] e "Applied Cryptography", e inventore degli algoritmi Blowfish, Twofish e Yarrow. È il fondatore e CTO di Counterpane Internet Security, Inc., e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla crittografia. Il suo sito Web è all'indirizzo <<http://www.schneier.com>>.

BT Counterpane è leader mondiale nella protezione delle informazioni su network - l'inventore del Managed Security Monitoring gestito in outsourcing e la principale autorità nella riduzione efficace delle nuove minacce in ambito IT. BT Counterpane protegge reti per conto di governi e di aziende inserite nella Fortune 1000 a livello mondiale.

<<http://www.counterpane.com>>

Crypto-Gram è una newsletter personale. Le opinioni qui espresse non sono necessariamente quelle di BT o di BT Counterpane.

Copyright (c) 2007 - Bruce Schneier.