

CRYPTO-GRAM
15 gennaio 2010

Scritta da Bruce Schneier
Chief Security Technology Officer di BT
e-mail: schneier@schneier.com
Web: <<http://www.schneier.com>>

Edizione italiana curata da Communication Valley, Business Unit di Security Reply.
<<http://www.communicationvalley.it/>>

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia.

Per consultare i numeri arretrati, o per iscriversi, andare all'indirizzo:
<<http://www.schneier.com/crypto-gram.html>>.

Oppure si può leggere il presente numero direttamente sul Web, all'indirizzo:
<<http://www.schneier.com/crypto-gram-0910.html>>.

Gli stessi articoli della newsletter sono disponibili sul blog di Bruce Schneier "Schneier on Security": <<http://www.schneier.com/blog>>.

Crypto-Gram è anche consultabile in formato RSS.

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

In questo numero:

- La sicurezza aeroportuale dopo l'Underwear Bomber
- I miei interventi sull'Underwear Bomber
- Ancora sull'Underwear Bomber
- News
- Concorso: un nuovo logo per la TSA
- Un altro concorso: migliorare la sicurezza aeroportuale
- Le news su Schneier
- Migliorare l'intelligence
- Intercettare il feed video dei Predator
- Penetrare nell'area sicura degli aeroporti
- Commenti dei lettori

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

La sicurezza aeroportuale dopo l'Underwear Bomber

Dopo il fallito attentato di Natale a opera dell'Underwear Bomber (lett. 'dinamitardo delle mutande'), ci si è precipitati a 'sistemare' la sicurezza, trascurando il dibattito su

che cosa ha funzionato e cosa no, e su che cosa ci renderà più sicuri in futuro e cosa no.

I checkpoint di sicurezza hanno funzionato. Visto che controlliamo la presenza di ordigni esplosivi evidenti, Umar Farouk Abdulmutallab (o, più precisamente, chiunque abbia costruito la bomba) ha dovuto assemblare un ordigno molto meno affidabile del previsto. Invece di utilizzare un timer o un pistone o un altro tipo di meccanismo di detonazione sicuro -- come farebbe qualunque utilizzatore commerciale di PETN (pentaeritritile tetranitrato) -- ha dovuto ripiegare su un sistema ad hoc, artigianale, e molto meno efficiente: un meccanismo che prevedeva una siringa, una sosta di 20 minuti nella toilette e non sappiamo bene che altro. E non ha funzionato.

Certo, gli screener dell'aeroporto di Amsterdam hanno permesso ad Abdulmutallab di imbarcarsi con del PETN cucito all'interno delle mutande, ma nemmeno questo è un errore. Non esiste alcun checkpoint di sicurezza gestito da alcun governo, in nessuna parte del mondo, progettato per rilevare questo genere di cose. Non si tratta di una nuova minaccia, è vecchia di almeno una decina d'anni. Né si tratta di qualcosa di inaspettato: chiunque sostenga il contrario non sta prestando la dovuta attenzione. Ma è difficile far esplodere il PETN, e lo abbiamo visto il giorno di Natale.

In più, i passeggeri sull'aereo sono stati in gamba. Per anni ho sostenuto che le uniche due cose che ci hanno reso più sicuri dall'attentato dell'11 settembre sono state il rinforzo della porta della cabina di pilotaggio, e convincere i passeggeri a ribellarsi agli aggressori. Ed è stata proprio questa reazione dei passeggeri che, il giorno di Natale, ha prontamente neutralizzato Abdulmutallab dopo che questi si era dato fuoco ai pantaloni.

Se vogliamo vedere dove ha fallito la sicurezza, questa ha fallito ancor prima che Abdulmutallab arrivasse in aeroporto. Perché gli è stato concesso un visto americano? Perché nessuno ha indagato ulteriormente dopo il suggerimento di suo padre? Se da una parte sono sicuro che vi sono molte cose da migliorare e da sistemare, ricordiamoci che tutto è ovvio col senno di poi. Una volta accaduto il fatto, è facile puntare il dito ai vari indizi e sostenere che qualcuno avrebbe dovuto 'unire i vari punti'. Ma prima del fatto, quando vi sono milioni di punti da collegare (alcuni importanti sommersi in una moltitudine di elementi irrilevanti), portare alla luce un complotto è molto più arduo.

Malgrado ciò, i rimedi proposti si concentrano tutti sui dettagli del complotto invece che sulla minaccia più generale. Installeremo degli scanner del corpo intero, anche se esistono tantissimi modi per nascondere il PETN (lo si può introdurre in un orifizio, spalmare sottilmente su un tessuto, ecc.) e fare in modo che le macchine non lo rilevino. Effettueremo il profiling dei passeggeri provenienti da 14 determinati paesi, anche se per un terrorista è molto semplice arrivare da un altro paese al di fuori dell'elenco. L'obbligo a star seduti durante l'ultima ora di volo è stata l'idea in assoluto più ridicola.

Il problema di tutte queste contromisure è che si rivelano efficaci se e solo se indoviniamo il complotto nel dettaglio. Difendersi contro una tattica particolare o proteggere un particolare bersaglio ha senso se tattiche e bersagli sono un numero ridotto. Ma esistono centinaia di tattiche e milioni di bersagli, e pertanto l'unico effetto che avranno queste misure è indurre i terroristi a fare solo alcuni leggeri ritocchi ai loro piani.

È il pensiero magico: se ci difendiamo contro quel che i terroristi hanno compiuto la scorsa volta, saremo magicamente al sicuro anche da quel che commetteranno la prossima volta. Ovviamente così non può funzionare. Confischiamo pistole e bombe, e i terroristi si servono di taglierini. Proibiamo taglierini e cavatappi, e i terroristi nascondono l'esplosivo nelle loro scarpe. Controlliamo le scarpe, e loro passano agli esplosivi liquidi. Limitiamo le quantità di liquidi, e loro si riempiono le mutande di PETN. Implementiamo gli scanner del corpo intero, e i terroristi risponderanno in qualche altra maniera. È un giochino stupido, e sarebbe ora che smettessimo di giocare.

Ma non possiamo farne a meno. Come specie, è nella nostra natura essere impauriti da determinati scenari -- terroristi con esplosivo nelle mutande, terroristi sulla metropolitana, terroristi muniti di polverizzatori -- e vogliamo sentirci protetti contro queste storie. E quindi implementiamo un teatrino di sicurezza contro le storie, ignorando le minacce più generali ed estese.

Ciò di cui abbiamo bisogno è una sicurezza che sia efficace anche quando non riusciamo a indovinare il prossimo complotto terroristico: intelligence, investigazione e risposta alle emergenze. Ne è una chiara dimostrazione l'aver neutralizzato l'attentato dei dinamitardi liquidi. Sono stati arrestati a Londra, prima ancora che arrivassero in aeroporto. Che avessero scelto di utilizzare esplosivi liquidi -- scelti precisamente perché non erano contemplati nei controlli di sicurezza -- piuttosto che solidi o in polvere, non ha avuto importanza. Così come non è stato rilevante il tipo di bersaglio, che avrebbe potuto essere un aereo, un centro commerciale o un cinema affollato. Sono stati arrestati e il complotto sventato. Questa è sicurezza efficace.

Infine dobbiamo essere indomiti. La vera falla di sicurezza nel giorno di Natale è stata la nostra reazione. Stiamo reagendo spinti dalla paura, sprecando denaro sulla storia, sullo scenario, invece che per proteggerci dalla minaccia. Abdulmutallab ha avuto successo nel provocare il terrore anche se il suo attacco è fallito.

Se rifiutiamo di farci terrorizzare, se rifiutiamo di implementare teatrini di sicurezza e teniamo sempre presente che non potremo mai completamente eliminare il rischio del terrorismo, allora i terroristi falliranno anche quando i loro attacchi andranno a buon fine.

Questo articolo è apparso precedentemente su Sphere, il sito di notizie di AOL.com.
<<http://www.sphere.com/2010/01/07/opinion-our-reaction-is-the-real-airport-security-failure/19307060/>>
oppure <<http://tinyurl.com/ylpszdg>>

Un'opinione analoga:
<http://www.sltrib.com/opinion/ci_14120146>

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

I miei interventi sull'Underwear Bomber

Questa è stata la mia prima reazione:
<http://www.schneier.com/blog/archives/2009/12/separating_expl.html>

Rachael Maddow mi ha intervistato:

<<http://www.msnbc.msn.com/id/26315908/vp/34615697#34615697>>

Ho tenuto molte interviste: alla televisione, alla radio, a mezzo stampa.

Jeffrey Goldberg ha pubblicato un Q&A con me per il sito the Atlantic:

<http://jeffreycgoldberg.theatlantic.com/archives/2009/12/bruce_schneier_on_the.php

>

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

CNN.com ha pubblicato due revisioni di miei vecchi articoli:

<<http://www.cnn.com/2009/OPINION/12/29/schneier.air.travel.security.theater/index.html>

>

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

<<http://www.cnn.com/2010/OPINION/01/07/schneier.security/index.html>>

Ho partecipato a una discussione sul profiling per la sicurezza negli aeroporti per la rubrica "Room for Debate"; nulla che non abbia già detto in precedenza.

<<http://roomfordebate.blogs.nytimes.com/2010/01/04/will-profiling-make-a-difference/>>

oppure <<http://tinyurl.com/yap6ktv>>

Questo è stato il mio secondo post sull'argomento:

<http://www.schneier.com/blog/archives/2010/01/christmas_bombe.html>

Nel 2002 avevo parlato delle carenze dell'intelligence.

<<http://www.schneier.com/crypto-gram-0206.html#1>>

Mi fa molto piacere che la mia espressione 'teatrino della sicurezza' sia finalmente diventata di uso corrente. La mia variante preferita è 'teatro della sicurezza dell'assurdo'.

<<http://douthat.blogs.nytimes.com/2009/12/28/the-follies-of-security-theater/>>

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

<<http://www.msnbc.msn.com/id/34686891/ns/travel-tips>>

<<http://www.jpost.com/servlet/Satellite?cid=1262339404286&pagename=JPost%2FJP%2FArticle%2FShowFull>

>

oppure <<http://tinyurl.com/ycpplv7>>

<http://scienceblogs.com/tfk/2010/01/security_theater_2.php>

<<http://news.firedoglake.com/2010/01/01/welcome-backlash-against-security-theater-and-overhyping-of-fear/>>

oppure <<http://tinyurl.com/yg48z8f>>

<<http://www.intellectualconservative.com/2010/01/05/a-better-solution-to-airline-safety/>

>

oppure <<http://tinyurl.com/ye3h6op>>

<<http://pajamasmedia.com/rogerkimball/2010/01/04/obamas-sweetly-scented-cashmere-afghan/>

>

oppure <<http://tinyurl.com/yghwr2r>>

<<http://www.theglobeandmail.com/news/opinions/security-theatre-of-the-absurd/article1418698/>

>

oppure <<http://tinyurl.com/yb4j3u2>>

Credo che dovremmo iniziare a chiamarle 'mutande di distruzione di massa'.

<http://www.nydailynews.com/news/national/2009/12/29/2009-12-29_untitled_2qaeda29m.html>
oppure <<http://tinyurl.com/ydl3kks>>

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

Ancora sull'Underwear Bomber

Analisi eccellente da parte di The Register:
<http://www.theregister.co.uk/2010/01/08/mutallab_comment/>

Ottimi i commenti di Ray McGovern, ex analista per la CIA:
<<http://consortiumnews.com/2010/010510c.html>>

David Brooks sulla resistenza di fronte alle imperfezioni della sicurezza:
<http://www.schneier.com/blog/archives/2010/01/david_brooks_on.html>

Nate Silver sui rischi del terrorismo aereo:
<http://www.schneier.com/blog/archives/2010/01/nate_silver_on.html>

Il rischio comparativo del terrorismo, con un mio commento sull'argomento:
<http://www.schneier.com/blog/archives/2010/01/the_comparative.html>

Matt Blaze sulle nuove misure di screening 'imprevedibili' varate dalla TSA:
<http://www.schneier.com/blog/archives/2010/01/matt_blaze_on_t.html>

Problemi nell'adottare il modello di sicurezza dell'aeroporto di Israele:
<http://www.schneier.com/blog/archives/2010/01/adopting_the_is.html>

Non è chiaro se uno scanner del corpo intero avrebbe individuato l'Underwear Bomber di Natale:
<http://news.bbc.co.uk/2/hi/uk_news/8439285.stm>

Un'azienda pubblicizza scanner degli orifizi:
<<http://www.wired.com/dangerroom/2010/01/crack-new-scanner-finds-explosives-inside-body-cavities/>>
oppure <<http://tinyurl.com/ybrbcbt>>

Una serie di vignette molto azzeccate:
<<http://geekandpoke.typepad.com/geekandpoke/2009/12/security-theatre.html>>
oppure <<http://tinyurl.com/yz7h9pt>>
<http://www.rall.com/uploaded_images/1-7-10-720155.jpg>
<<http://www.cartoonistgroup.com/store/add.php?iid=42588>>

Jon Stewart è stato proprio divertente lo scorso 4 gennaio.
<<http://www.thedailyshow.com/watch/mon-january-4-2010/terror-2-0-by-yemen>>
oppure <<http://tinyurl.com/y8vw747>>

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

News

Considerare il movimento per i diritti civili USA come un'insurrezione:

<http://www.schneier.com/blog/archives/2009/12/the_us_civil_ri.html>

Una serie eccellente in quattro parti: "Risk and Security in the Telecommunications Industry" [Rischio e sicurezza nell'industria delle telecomunicazioni].

<http://pacific-tier.com/blog/2009/10/risk_and_security_in_the_telec.html>

oppure <<http://tinyurl.com/yl6pg92>>

<http://pacific-tier.com/blog/2009/10/telecom_risk_and_security_part.html>

oppure <<http://tinyurl.com/ykus3fh>>

<http://pacific-tier.com/blog/2009/10/telecom_risk_and_security_part_1.html>

oppure <<http://tinyurl.com/ye7qzhv>>

<http://pacific-tier.com/blog/2009/10/telecom_risk_and_security_part_2.html>

oppure <<http://tinyurl.com/ykmxam7>>

Serratura con riconoscimento facciale:

<http://www.chinavasion.com/product_info.php/pName/facial-recognition-time-attendance-system-and-access-door-lock/>

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

Un post molto ponderato sulla politica del potere nel cyberspazio:

<http://politics.theatlantic.com/2009/12/whenever_i_write_about_the.php>

Il mio articolo su chi dovrebbe essere a capo della sicurezza cibernetica:

<<http://www.schneier.com/essay-265.html>>

L'Australia riporta un po' di buonsenso nello screening aeroportuale; mi chiedo se durerà.

<http://www.schneier.com/blog/archives/2009/12/australia_resto.html>

Tecnologia MagnePrint per carte di credito/debito: sembra una soluzione in cerca di un problema.

<http://www.schneier.com/blog/archives/2009/12/magneprint_tech.html>

Sconfiggere BitLocker, persino con il TPM.

<http://testlab.sit.fraunhofer.de/downloads/Publications/Attacking_the_BitLocker_Boot_Process_Trust2009.pdf>

oppure <<http://tinyurl.com/yel869n>>

<<http://news.zdnet.co.uk/security/0,1000000189,39926434,00.htm>>

<http://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html>

Una notizia davvero grave: il database dei buoni e dei cattivi appartenente a Babbo Natale è stato hackerato.

<<http://precision-blogging.blogspot.com/2009/12/another-leak-worst-so-far.html>>

oppure <<http://tinyurl.com/ybvrm6g>>

Lettere di Babbo Natale, per informare i bambini dell'intrusione:

<http://www.schneier.com/blog/archives/2009/12/santas_naughtyn.html#c403744>

oppure <<http://tinyurl.com/y9de7ce>>

<http://www.schneier.com/blog/archives/2009/12/santas_naughtyn.html#c403754>

oppure <<http://tinyurl.com/ydgg68a>>

Jack Bauer (della serie televisiva "24") interroga Babbo Natale:
<<http://www.youtube.com/watch?v=X6yUCbqAGrq>>

Howard Schmidt nominato capo della sicurezza cibernetica degli Stati Uniti:
<http://www.schneier.com/blog/archives/2009/12/howard_schmidt_1.html>

Luggage Locator -- localizzatore di bagaglio. Pessima idea davvero:
<http://www.schneier.com/blog/archives/2009/12/luggage_locator.html>

Misure di sicurezza delle piante:
<http://www.schneier.com/blog/archives/2009/12/plant_security.html>

Ottimo articolo di analisi di Alessandro Acquisti in IEEE Security & Privacy: "The Behavioral Economics of Personal Information" [L'economia comportamentale delle informazioni personali]

<http://www.computer.org/cms/Computer.org/ComputingNow/homepage/2009/1209/W_SP_NudgingPrivacy.pdf>

oppure <<http://tinyurl.com/yz43ty>>

Serie di filmati interessanti che illustrano il fenomeno noto come 'cecità al cambiamento' (change blindness), ossia la tendenza del cervello umano a ignorare importanti variazioni visive. Le conseguenze per la sicurezza sono piuttosto gravi.

<<http://www.youtube.com/watch?v=38XO7ac9eSs>>

<<http://www.youtube.com/watch?v=ubNF9QNEQLA>>

<http://www.youtube.com/watch?v=vBPG_OBgTWg>

Daniel C. Dennett sull'argomento:

<http://www.ted.com/index.php/talks/dan_dennett_on_our_consciousness.html>

oppure <<http://tinyurl.com/6mb4uj>>

Crack impressionante di un criptosistema quantico:
<http://www.schneier.com/blog/archives/2009/12/quantum_cryptog_1.html>

Il Vaticano ammette che la sicurezza perfetta è sia impossibile da ottenere che indesiderabile:

<http://www.schneier.com/blog/archives/2010/01/vatican_admits.html>

Il furto nei negozi di vendita al dettaglio a opera dei dipendenti è sempre stato un problema, ma le tessere regalo lo rendono ancor più facile:

<http://www.nytimes.com/2009/12/30/business/30theft.html?_r=3&hp>

Craccata una memory stick USB certificata FIPS 140-2 Level 2:
<http://www.schneier.com/blog/archives/2010/01/fips_140-2_level.html>

Fattorizzato un numero a 768 bit:
<http://www.schneier.com/blog/archives/2010/01/768-bit_number.html>

Ricerca interessante sulla power law associata agli attacchi terroristici:
<http://www.schneier.com/blog/archives/2010/01/the_power_law_o.html>

Editoriale d'opinione sul National Clandestine Service della CIA:
<<http://www.nytimes.com/2010/01/10/opinion/10grenier.html>>

In Giappone sono stati rubati gioielli per 3,2 milioni di dollari semplicemente facendo un buco nel muro:

<http://www.schneier.com/blog/archives/2010/01/32_million_jewe.html>

Loretta Napoleoni sull'economia del terrorismo:

<http://www.ted.com/talks/loretta_napoleoni_the_intricate_economics_of_terrorism.html>

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

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

Concorso: un nuovo logo per la TSA

Patrick Smith, della rubrica "Ask The Pilot", ha avuto un'ottima idea: "A tutti gli artisti: credo che la TSA abbia proprio bisogno di un nuovo logo e di un motto sagace. Magari c'è qualche grafico che può realizzare una nuova interpretazione del classico emblema circolare dell'agenzia, con l'aquila e la bandiera americana. Mi immagino un'aquila diversa, che stringe fra le zampe un taglierino e un tubetto di dentifricio. E in alto la scritta 'Transportation Security Administration'. In basso, invece, le tre semplici parole che definiscono la mission della TSA: 'Tedium, Weakness, Farce' [Tedio, Debolezza, Farsa]".

Dai, facciamolo. Annuncio ufficialmente il Concorso 'Nuovo Logo per la TSA'. Le regole sono semplici: creare un logo per la TSA. Utilizzate pure la sezione commenti sul mio blog per offrire spunti e suggerimenti, ma solo dei logotipi veri e propri saranno considerati validi per la partecipazione al concorso. Il termine è il 6 febbraio. Il vincitore riceverà una copia dei miei libri, una copia del libro di Patrick Smith, una bottiglietta vuota da 33 cl con l'etichetta 'Soluzione salina' che si può riempire e riutilizzare più volte per passare i checkpoint di sicurezza della TSA, e un permesso di imbarco fasullo da usarsi con qualsiasi volo in qualsiasi giorno dell'anno.

Inviare la vostra idea -- e ammirate le proposte altrui -- sul mio blog:

<http://www.schneier.com/blog/archives/2010/01/tsa_logo_contes.html>

Pubblicherò l'elenco dei finalisti intorno al 6 febbraio, e poi tutti potranno votare il vincitore.

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

Un altro concorso: migliorare la sicurezza aeroportuale

Slate ha tenuto un concorso sulla sicurezza aeroportuale in cui i partecipanti erano invitati a presentare suggerimenti e idee "per rendere la sicurezza negli aeroporti più efficace, più efficiente o più piacevole". La scadenza era fissata per la scorsa settimana.

Avevo già presentato un suggerimento ancor prima che mi fosse chiesto di far parte della giuria. Dato che ora il mio contributo non è più valido, lo riporto qui:

“Ridurre il budget della TSA, e investire il denaro in:

1. Intelligence. Le misure di sicurezza incentrate su tattiche o bersagli specifici sono uno spreco di denaro a meno che non si riesca a indovinare esattamente quale sarà il prossimo attacco. Misure di sicurezza che si limitano a spingere i terroristi a fare pochi lievi cambiamenti alle loro tattiche o bersagli rappresentano denaro male investito.
2. Investigazione. Dato che i terroristi scelgono deliberatamente complotti e strategie che non stiamo considerando, la sicurezza migliore è quella di sventare tali complotti prima che raggiungano gli aeroporti. Ricordare l’arresto dei dinamitardi liquidi a Londra.
3. Risposta alle emergenze. I danni provocati dal terrorismo dipendono più dalle nostre reazioni agli attacchi che non dagli attacchi stessi. Siamo resistenti per natura, ma come reagiamo in quelle prime ore e nei primi giorni è cruciale.

E come beneficio aggiunto, tutte queste contromisure ci proteggono anche dal terrorismo non aereo. Tutto quel che dobbiamo fare è smetterla di concentrarci su specifiche trame da film, e iniziare a considerare la minaccia generale”.

Probabilmente non è ciò che si aspettavano, e si tratta certamente di consigli che il governo non considererà neanche alla lontana, ma è la soluzione più intelligente.

<<http://www.slate.com/id/2240570/>>

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

Le news su Schneier

Ecco i sei link del faccia a faccia con Marcus Ranum tenuto durante la conferenza Information Security Decisions a Chicago.

<http://searchsecurity.techtarget.com/video/0,297151,sid14_gci1376072,00.html>
oppure <<http://tinyurl.com/yfusvts>>
<http://searchsecurity.techtarget.com/video/0,297151,sid14_gci1376098,00.html>
oppure <<http://tinyurl.com/ydzge6e>>
<http://searchsecurity.techtarget.com/video/0,297151,sid14_gci1376215,00.html>
oppure <<http://tinyurl.com/yzjnuj4>>
<http://searchsecurity.techtarget.com/video/0,297151,sid14_gci1376222,00.html>
oppure <<http://tinyurl.com/ydt3zoq>>
<http://searchsecurity.techtarget.com/video/0,297151,sid14_gci1376274,00.html>
oppure <<http://tinyurl.com/ybfrsgx>>
<http://searchsecurity.techtarget.com/video/0,297151,sid14_gci1376328,00.html>
oppure <<http://tinyurl.com/ylqra4p>>

Un'altra intervista al sottoscritto, stavolta per ZDNet.uk:

<<http://news.zdnet.co.uk/security/0,1000000189,39927707,00.htm>>

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

Migliorare l'intelligence

Il presidente Obama, nel suo discorso la settimana passata, ha giustamente posto l'accento su come migliorare le carenze dell'intelligence che hanno fatto sì che Umar Farouk Abdulmutallab passasse inosservato, invece che sulle tecnologie mirate ai dettagli del suo piano d'attacco. Ma se l'istinto di Obama è nella giusta direzione, riformare l'intelligence e adattarla a questo nuovo secolo, con le sue nuove minacce, è un compito assai più arduo di quanto possa piacere al presidente. Non servono nuove tecnologie, nuove leggi, nuovi sovrani della burocrazia; e nemmeno nuove agenzie, per l'amor del cielo. Ciò che impedisce la condivisione di informazioni fra le organizzazioni di intelligence è la cultura della generazione che ha edificato quelle stesse organizzazioni.

Il sistema di intelligence statunitense è un apparato in continua, irregolare estensione, e che racchiude l'FBI e il Dipartimento di Stato, la CIA e la National Security Agency, e il Dipartimento per la Sicurezza Nazionale (esso stesso è il risultato della fusione di due dozzine di organizzazioni diverse) designato e ottimizzato per combattere la Guerra Fredda. A quel tempo l'unico, gigantesco avversario era l'Unione Sovietica: più burocratica che mai, con un budget enorme, e capace di operazioni di spionaggio veramente sofisticate. L'America doveva difendersi contro avanzate operazioni di intercettazione elettronica, con gli agenti sovietici che cercavano di corrompere o sedurre gli agenti americani, e una capacità di raccolta di intelligence a livello mondiale che si attaccava a ogni nostra parola.

In quell'ambiente la segretezza era fondamentale. Le informazioni dovevano essere protette da guardie armate e da doppie recinzioni, condivise soltanto fra coloro che avevano le giuste autorizzazioni di sicurezza e che dovevano essere specificatamente messi al corrente; ed era preferibile non trasmettere alcuna informazione piuttosto che trasmetterla in modo non sicuro.

Gli avversari di oggi sono diversi. Esistono ancora governi a caccia dei segreti americani, come la Cina. Ma si tratta di segreti molto più spesso aziendali che non militari, e la maggioranza delle altre organizzazioni di interesse sono come al Qaeda: decentralizzate, mal finanziate e incapaci delle intricate operazioni spia-contro-spia che poteva architettare l'Unione Sovietica.

Contro avversari del genere la condivisione delle informazioni è più importante della segretezza. Le nostre organizzazioni di intelligence devono scambiare strategie ed esperienza con l'industria, e devono condividere informazioni fra le parti che le costituiscono. I complotti terroristici odierni sono affari ad hoc e male organizzati, e quei punti che è così importante connettere prima di un attacco potrebbero trovarsi su scrivanie differenti, in edifici diversi, in mano a organizzazioni diverse.

I critici di questa posizione hanno fatto notare che esistono leggi che proibivano la condivisione fra agenzie ma, come ha scoperto la 9/11 Commission, la legge permette molta più condivisione di quanto si stia facendo attualmente. Questa condivisione non avviene in gran parte a causa di rivalità fra agenzie, della dipendenza da sistemi di informazione obsoleti, e di una cultura di segretezza. Ciò di cui abbiamo bisogno è una comunità di intelligence che si scambia idee, spunti e fatti sulla propria versione di Facebook, di Twitter e delle wiki. Occorre l'organizzazione in senso ascendente che ha fatto diventare Internet la più grande collezione di scibile umano e di idee mai realizzata.

Il problema è molto più sociale che tecnologico. Insegnare a vostra madre a mandare SMS e a vostro padre a usare Twitter non li rende parte della generazione di Internet, e dare a tutti quei combattenti della Guerra Fredda lezioni di blogging non cambierà la loro mentalità né la loro cultura. Il motivo per cui questo continua a rappresentare un problema, il motivo per cui il presidente George W. Bush non ha potuto cambiare le cose persino dopo che la 9/11 Commission arrivò alle stesse conclusioni alle quali è arrivato oggi il presidente Obama, è generazionale. Internet è il più grande divario generazionale dopo il rock and roll, e questo è vero sia all'interno del governo che fuori. Potrebbe essere necessario attendere che i veterani delle varie agenzie vadano in pensione e che siano sostituiti da persone cresciute insieme a Internet.

Questo editoriale di opinione è precedentemente apparso sul San Francisco Chronicle.
<<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/01/14/ED0L1BIFK6.DTL>>
oppure <<http://tinyurl.com/y8cjosq>>

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

Intercettare il feed video dei Predator

A volte una crittografia mediocre è meglio di una crittografia forte, e a volte è ancora meglio non criptare del tutto.

Il Wall Street Journal ha riportato questa settimana che i militanti iracheni, e probabilmente anche gli afgani, stanno utilizzando software commerciale per intercettare i Predator americani, altri veicoli aerei senza equipaggio (UAV), e persino aerei con equipaggio. I sistemi non sono stati 'hackerati' -- gli insorgenti non li possono controllare -- ma dato che il downlink non è criptato, possono guardare lo stesso streaming video che vedono le truppe di coalizione a terra.

La reazione più ingenua è quella di ridicolizzare l'esercito. La criptatura è un affare così semplice, persino le TV ad alta definizione la producono -- una routine software e il gioco è fatto -- e il Pentagono è a conoscenza di questo problema sin dai tempi del conflitto in Bosnia negli anni Novanta. Ma criptare i dati è la parte più facile; il difficile è gestire le chiavi. Ogni UAV deve condividere una chiave con la stazione di terra. Queste chiavi devono essere prodotte, protette, trasportate, utilizzate e quindi distrutte. E l'attrezzatura, sia i Predator che i terminali a terra, deve essere segretata e controllata, e ogni utente deve possedere un'autorizzazione di sicurezza.

Il canale di comando e controllo è, ed è sempre stato, criptato -- perché è al tempo stesso più importante e più semplice da gestire. Gli UAV vengono pilotati da aviatori comodamente seduti dietro una scrivania nelle basi militari statunitensi, dove la gestione delle chiavi è più semplice. Ma il feed video è un'altra questione. Deve essere disponibile per moltissime persone, di nazionalità diverse e con differenti permessi di sicurezza, davanti ai terminali sul campo più disparati, in svariate aree geografiche e in ogni genere di condizioni -- in una situazione di costante cambiamento. La gestione delle chiavi in un simile contesto sarebbe un incubo.

E poi, che valore ha veramente il video downlink per il nemico? Il timore principale sembra essere che i militanti guardino il video, notino che la loro zona è sorvegliata, e

scappino prima di essere colpiti dai missili. Oppure che notino un gruppo di marines muoversi in una zona riconoscibile e li attacchino. Potrebbe essere un'ottima scena per un film, ma non è un quadro molto realistico. Senza un contesto, e dando semplicemente un'occhiata a svariati streaming video, il rischio causato dall'intercettazione è minimo.

Ora mettiamo a confronto questa situazione con i rischi aggiunti in caso di criptatura: un soldato sul campo non ha accesso al video in tempo reale per un errore nella gestione delle chiavi; un UAV non può essere spedito rapidamente in una nuova zona perché non sono ancora pronte le chiavi; non possiamo condividere i dati video con i nostri alleati perché non possiamo dare loro le chiavi; molti soldati non possono servirsi di questa tecnologia perché non hanno i permessi di sicurezza appropriati. Con una simile analisi dei rischi, non criptare il feed video è quasi certamente la decisione giusta.

Ma esiste un'altra possibilità. Durante la Guerra Fredda, l'avversario principale della NSA era l'intelligence sovietica, e la NSA sviluppò delle soluzioni crittografiche adeguate. Sebbene quel livello di sicurezza non ha alcun senso in Bosnia, e men che meno in Iraq e Afghanistan, è quel che la NSA poteva offrire. Se dovete criptare, dicevano, dovete farlo nel modo 'giusto'.

Il problema è che il mondo è cambiato. Gli avversari insorgenti di oggi non hanno il livello di raccolta di intelligence né le capacità criptanalitiche che aveva il KGB. Allo stesso tempo, la raccolta di dati informatici e di rete è diventata più semplice e assai poco costosa, pertanto possiedono abilità tecniche che i sovietici si sognavano. Difendersi da questo genere di avversari non richiede una crittografia a livello militare solo nei punti più importanti; richiede una crittografia a livello commerciale che copra ogni punto possibile.

Per una tale soluzione, la NSA dovrebbe sviluppare un livello completamente nuovo di sistemi di sicurezza leggeri e di grado commerciale per applicazioni militari -- non semplicemente classificazioni come 'Delicato ma non Riservato' o 'Per uso esclusivamente ufficiale' per i dati da ufficio. La NSA dovrebbe permettere il passaggio di chiavi a personale non autorizzato che osserva il downlink, chiavi magari lette attraverso linee telefoniche non sicure e conservate nella tasca posteriore dei pantaloni. Tutto questo richiederebbe il tipo di sistemi di gestione delle chiavi che si trovano nei protocolli internet o nei sistemi DRM. Non sarebbe un sistema perfetto, ma decisamente più proporzionato alle minacce vere e proprie.

E aiuterebbe a difendersi da una minaccia completamente diversa che deve affrontare il Pentagono: quella delle pubbliche relazioni. Non importa se le persone responsabili hanno compiuto la giusta decisione di sicurezza quando hanno affrettato la produzione dei Predator; non importa se si sono convinti che gli avversari locali non sarebbero stati in grado di sfruttarli; non importa se si sono dimenticati di aggiornare la loro analisi della minaccia, ferma all'epoca della Bosnia, per tenere in conto dei progressi tecnologici; adesso la storia è nelle mani della stampa. E il Pentagono viene criticato aspramente perché non ci sta proteggendo dalla minaccia -- perché è facile scrivere una frasetta dal grande impatto mediatico in cui si dipinge la minaccia come qualcosa di veramente spaventoso. E quindi ora il Pentagono deve difendersi contro la minaccia percepita ai danni delle truppe, non importa se la difesa protegge davvero i soldati o meno. Mi ricorda tanto la TSA, in effetti.

Per cui adesso l'esercito ha preso l'impegno di criptare il video... prima o poi. I Predator di prossima generazione, chiamati Reaper (ma chi dà i nomi a questi aggeggi, i ragazzini delle medie?), avranno la stessa vulnerabilità. Forse avremo il video criptato nel 2010, o nel 2014, ma non credo che questo sia neanche lontanamente possibile a meno che la NSA allenti gli stretti requisiti in materia di gestione e classificazione delle chiavi e implementi una soluzione crittografica più leggera e meno sicura per questo genere di scenari. Il vero fallimento qui è l'incapacità del modello di sicurezza della Guerra Fredda di affrontare le minacce odierne.

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/politics/security/commentary/securitymatters/2009/12/securitymatters_1223>

oppure <<http://tinyurl.com/yb7jx8s>>

Militanti iracheni, e forse anche afgani:

<<http://online.wsj.com/article/SB126102247889095011.html>>

<<http://www.wired.com/dangerroom/2009/12/not-just-drones-militants-can-snoop-on-most-us-warplanes/>>

oppure <<http://tinyurl.com/y9zp5ny>>

<http://wikileaks.org/wiki/Reading_mission_control_data_from_Predator_Drone_video_feeds,_20_Dec_2009>

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

<<http://arstechnica.com/tech-policy/news/2009/12/predator-drones-use-less-encryption-than-your-tv.ars>>

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

<http://www.networkworld.com/news/2009/12/1809-drone-video-traffic-intentionally-unencrypted.html?source=NWWNLE_nlt_daily_am_2009-12-21>

oppure <<http://tinyurl.com/yeonm2k>>

<<http://www.wired.com/dangerroom/2009/12/fixing-drone-data-a-not-so-modest-proposal/>>

oppure <<http://tinyurl.com/yc959v7>>

<http://www.armytimes.com/news/2009/12/army_uav_hack_122009w/>

<<http://formerspook.blogspot.com/2009/12/predator-channel.html>>

<http://www.newyorker.com/reporting/2009/10/26/091026fa_fact_mayer>

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

Penetrare nell'area sicura degli aeroporti

Un uomo non identificato ha oltrepassato la sicurezza aeroportuale al Newark Airport l'altra domenica, entrando nell'area sicura attraverso l'uscita, e provocando l'evacuazione immediata di un intero terminale e ritardi nei voli che si sono estesi fino al giorno successivo. Non è un evento comune, ma capita regolarmente. Il risultato è sempre quello, e non è affatto detto che sistemare il problema sia la soluzione giusta.

Questo tipo di falla di sicurezza è inevitabile, semplicemente perché le guardie sono esseri umani e non sono perfette. A volte si tratta di qualcuno che entra da un'uscita, e non viene notato da una guardia annoiata o distratta. A volte è qualcuno che passa correndo attraverso il checkpoint e si perde nella folla. Altre volte è colpa di una porta

aperta che dovrebbe essere chiusa a chiave. Malgrado sembri incredibile a chi viaggia spesso, in moltissimi casi il malcapitato nemmeno sa di aver fatto qualcosa di sbagliato.

Sostanzialmente, ogni qual volta si trova (o potrebbe esserci) una persona non controllata sperduta nell'area sicura di un aeroporto, la TSA può fare due cose. Può dire "non è nulla di serio" e ignorare l'accaduto. Oppure può far evacuare l'intera area sicura, far ispezionare ogni angolo e recesso (nei grandi contenitori dei tovaglioli di carta dei fast food, sopra i controsoffitti delle toilette, ovunque), alla ricerca di chiunque si sia nascosto o di un oggetto nascosto da qualcuno, e poi ricontrollare tutti i passeggeri, provocando ritardi di sei, otto, dodici o più ore. Tutto qua: queste sono le uniche opzioni. E nessun responsabile sceglierà di ignorare il rischio; anche se le probabilità che si tratti di un'operazione terroristica sono infime, se chi ha il potere decisionale in tale situazione si sbaglia, si gioca la carriera.

Molti aeroporti europei organizzano i controlli di sicurezza in modo differente. All'aeroporto Schipol di Amsterdam, per esempio, i passeggeri vengono controllati alle porte d'imbarco. È una soluzione più costosa e che richiede una diversa progettazione dell'aeroporto, ma nel caso di una violazione della sicurezza soltanto la porta d'imbarco viene fatta evacuare e ispezionare, e solo i passeggeri che si trovano in quell'area vengono ricontrollati.

Gli aeroporti americani potrebbero fare di più per proteggersi da questo rischio, ma sono ragionevolmente sicuro che non ne valga la pena. Potremmo raddoppiare il numero delle guardie per ridurre il rischio di distrazioni, e riprogettare gli aeroporti per attenuare l'incidenza di questo genere di episodi, ma si tratta di soluzioni costose a un problema già raro di per sé. E per quanto non mi piaccia ammetterlo, credo che la cosa più intelligente da fare è convivere con questa grave ma occasionale seccatura.

Questo articolo è originariamente apparso su ThreatPost.com

<http://threatpost.com/en_us/blogs/fixing-security-problem-isnt-always-right-answer-010510>

oppure <<http://tinyurl.com/yfe7bxa>>

<<http://www.nytimes.com/2010/01/04/nyregion/04newark.htm>>

<<http://www.ofcourseimright.com/?p=872>>

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

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>>

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

Dal 1998 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, Business Unit di Security Reply. <<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 BT Counterpane e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Frequentemente scrive e partecipa a conferenze sulla sicurezza informatica e sulla 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) 2010 - Bruce Schneier.