

L'eccesso di sensazionalismo per quanto riguarda le minacce di sicurezza è dannoso:
<<http://www.wired.com/news/infostructure/0,1377,59556,00.html>>

L'epidemia del giorno su Internet è il worm Blaster. Non ne ho scritto nulla a riguardo perché non è molto interessante; è l'ennesima variazione di cose che abbiamo visto per anni. Ma c'è una nuova idea: una variante del worm scarica un file il cui nome contiene un termine anatomico che viene bloccato da molti filtri antispam. Mi domando quante email che parlano del worm non raggiungono mai il destinatario perché il nome del worm viene esplicitato. MOLTO furbo.
<<http://www.counterpane.com/alert-v20030811-001.html>>

Una delle macchine per il voto elettronico è stata analizzata da esperti della sicurezza informatica, e i risultati non sono affatto promettenti:
<<http://www.msnbc.com/news/943558.asp?0cv=TA00&cp1=1>>
<<http://www.avirubin.com/vote.pdf>>
<<http://www.scoop.co.nz/mason/stories/HL0307/S00198.htm>>
<<http://apnews.excite.com/article/20030726/D7SGT1780.html>>

Ma a nessuno importa della sicurezza delle macchine per il voto:
<<http://newsforge.com/article.pl?sid=03/07/25/1349255&tid=4>>

Un buon articolo su come falsare un'elezione grazie a questo genere di macchine:
<http://www.truthout.org/docs_03/voting.shtml>

Sicurezza e paura:
<<http://www.csoonline.com/read/070103/fear.html>>

Prendersi gioco delle verifiche delle firme sulle carte di credito:
<<http://www.zug.com/pranks/credit/index.html>>

Un buon articolo sul CALEA (Communications Assistance to Law Enforcement Act). Fra le altre cose, l'autore sostiene che i terminali CALEA sono stati regolarmente vittime di intrusioni.
<<http://www.pbs.org/cringely/pulpit/pulpit20030710.html>>

Articolo molto interessante sui vari tipi di frode ai danni dei Bancomat:
<<http://www.iht.com/articles/105087.html>>

Ancora una volta, la corte ha ordinato al Dipartimento degli Interni di scollegare i propri computer da Internet se non sono in grado di proteggere la privacy dei dati degli Indiani d'America.
<http://www.gcn.com/vol1_no1/security/22935-1.html>
<<http://www.dcd.uscourts.gov/96-1285at.pdf>>
<<http://www.dcd.uscourts.gov/96-1285as.pdf>>

Scrissi proprio di questo problema un anno e mezzo fa:
<<http://www.counterpane.com/crypto-gram-0112.html#2>>

Affrontare le regolamentazioni di sicurezza:
<<http://www.csoonline.com/read/070103/chaos.html>>

Api poliziotte. Un affascinante articolo su come le api trattano i problemi di sicurezza:
<http://www.nature.com/nsu/nsu_pf/020422/020422-16.html>

La posta totalmente anonima diventerà un ricordo del passato?
<<http://computerworld.com/newsletter/0,4902,83804,00.html?nlid=SEC2>>

Tre esempi:

1. Il mese scorso, Alastair Campbell, direttore della Comunicazione e della Strategia del primo ministro inglese Tony Blair, si è trovato in una difficile posizione durante le udienze del Parlamento inglese, spiegando il ruolo che quattro dei suoi impiegati hanno avuto nella creazione di un falso dossier sull'Iraq che il governo britannico ha pubblicato nel febbraio 2003. I nomi di questi quattro impiegati sono stati trovati nascosti all'interno di un file del dossier, in formato Microsoft Word, che è stato pubblicato sul sito web di Downing Street per la stampa. Il "dodgy dossier", come è stato soprannominato dalla stampa inglese, ha sollevato seri dubbi sulla qualità dell'intelligence inglese prima della seconda guerra del Golfo.

2. Lo scorso anno, durante la caccia al cecchino di Washington DC, è stata trovata una lettera, che il cecchino aveva lasciato per la polizia, che conteneva determinati nomi e numeri di telefono. Forse per convincere il pubblico impaurito del fatto che le forze di polizia stessero facendo davvero qualcosa, hanno dato l'autorizzazione a pubblicare la lettera -- rivista e adattata -- sul sito Web del Washington Post. Purtroppo le revisioni sono state fatte con l'insensato sistema di piazzare dei rettangoli neri sopra il testo sensibile nel file PDF. Un semplice script è stato in grado di rimuovere quei rettangoli e di recuperare l'intero PDF.

3. Tre anni fa, su Crypto-Gram, ho raccontato la storia di un documento della CIA che il New York Times aveva corretto e pubblicato in formato PDF sul proprio sito web. Il documento riguardava un vecchio complotto iraniano, e conteneva i nomi dei cospiratori. Il New York Times aveva corretto il documento in maniera reversibile, esattamente come ha fatto il Washington Post.

Gli esempi sono sufficienti. Quanto è diffuso questo problema? In un recente studio, S.D. Byers si è messo in Internet per vedere quali tipi di informazioni nascoste riusciva a intercettare. Si è concentrato su Microsoft Word, perché i documenti Word sono tristemente famosi per contenere informazioni riservate che non si vorrebbe condividere. Queste informazioni comprendono i nomi degli autori o di chi ha modificato il documento (come ha scoperto il governo Blair), dati riguardanti i computer, le reti e le stampanti che hanno a che fare con il documento, testo precedentemente cancellato dal documento, e in alcuni casi testo proveniente da documenti completamente diversi.

Byers ha raccolto 100.000 documenti MS Word, presi a caso dal web. Ha realizzato tre script per effettuare ricerche di testo nascosto, e ne ha trovato in tutti i documenti. Per la maggior parte si trattava di dati di scarso interesse -- come il nome dell'autore -- ma a volte si è imbattuto in cose molto interessanti. La sua conclusione: questo è un problema penetrante.

MS Word era al centro dell'attenzione nello studio di Byers, ma anche altri tipi di file possono diffondere informazioni riservate: file di Excel, PowerPoint, in formato PDF, PostScript, ecc. Le aziende che posseggono questi formati non hanno giustificazioni per non aver creato un programma che elimini le informazioni nascoste in quei tipi di file. E di certo esiste un'opportunità commerciale per delle terze parti che vogliono creare un tale prodotto, ma occorre che siano al di fuori degli Stati Uniti, perché altrimenti potrebbe rivelarsi una violazione del DMCA. I formati di file Microsoft, chiusi e proprietari, rendono difficile la creazione di un tale programma "correttore" e, a meno che Microsoft non faccia qualche cambiamento nel proprio software (ad esempio nei valori di utilizzo e di default), questi "correttori" rimarranno una soluzione imperfetta.

Dimenticavo; i giornali si servono continuamente di tecniche come questa per eliminare le correzioni da una miriade di documenti. Credo che non ne faccia parola perché teme di perdere l'accesso a tutte quelle informazioni confidenziali.

La ricerca di Byers:

<http://www.user-agent.org/word_docs.pdf>

aspettare che richieste ostili e ai danni del cliente possano suscitare un altrettanto ostile riscontro da parte dei clienti. Alla lunga, questo diventa un componente significativo del cambiamento delle regole. Finché le compagnie aeree / i farmacisti / gli hotel possono ribattere che nessuno si oppone alle regole, essi non avranno alcun interesse a cambiarle. Nel momento in cui diventa chiaro che reazioni ostili nei confronti delle regole cominciano a costare denaro (perché occorre più tempo e perché diventa difficile assumere dei buoni impiegati), allora prenderanno provvedimenti.

Da: "Taylor, Stephen" <STEPHEN.TAYLOR@saic.com>
Oggetto: Come reagire

Le esperienze negative con persone che non hanno il potere di prendere delle decisioni non sono una novità, ma le cose stanno peggiorando. Penso che stiamo tutti accusando il fatto che ci sono troppe persone su questo pianeta; siamo sempre e solo l'ennesima faccia in una coda allo sportello. Per me è un effetto di quest'America sempre più simile a un centro commerciale e della crescita delle burocrazie aziendali e governative. Le procedure che lei non ha gradito sono state stabilite forse senza nemmeno rifletterci sopra. Una volta instaurate, gli impiegati le seguono, oppure rischiano il posto.

Potrebbe valere la pena reagire in particolari circostanze. L'educazione è la chiave per cambiare una cultura in modo permanente. La gente ha bisogno di comprendere la sicurezza in modo da non essere ingannata dai politici e da chi dirige i media. Una compagnia aerea, per esempio, non dovrebbe poter respingere il suggerimento di installare delle serrature sulle porte della cabina di pilotaggio (prima dell'11 settembre). I media dovrebbero smetterla di abusare della parola "sicurezza", come se la parola medesima significasse le stesse cose per tutti. E per venire a qualcosa a me caro in questo momento, quelle aziende che trattano informazioni finanziarie non dovrebbero poter essere ingannate così facilmente da qualcuno con un numero di Previdenza Sociale rubato. La situazione legata all'uso di tale numero è molto grave, ormai necessita di più che un semplice provvedimento.

Da: Carsten Turner <carsten@netway.com>
Oggetto: Come reagire

Nell'esempio della farmacia, invece di scrivere "Non farò mai più acquisti qui", si potrebbe scrivere "Farò presente l'accaduto ai produttori della merce che lei vende, e dirò loro che, finché continueranno a trattare con lei, non acquisterò i loro prodotti". È un po' una variazione della lettera al giornale ove si dice "Sono stufo del vostro giornalismo scandalistico, per cui scriverò ai vostri inserzionisti per dire loro che cosa ne penso".

Lei è un solo consumatore, e decidere di non rivolgersi più a quella farmacia non sarà un gran danno per il farmacista. Ma se, andando a bussare alle porte dei vari produttori, troverà chi la pensa come lei, allora il danno alla farmacia sarà maggiore.

Da: Radovan Semancik <semancik@bgs.sk>
Oggetto: Come reagire

Se fossi il proprietario di un albergo, vorrei davvero conoscere l'identità dei miei ospiti. Il rischio di conti non pagati o di qualche altro danno potrebbe essere elevato. Se possedessi gli edifici di una grande azienda, vorrei conoscere l'identità delle persone che vi entrano. Potrebbero esserci delle risorse di grande valore da proteggere, e se un qualsiasi individuo entra per fare della manutenzione, vorrei sapere chi è e vorrei controllare il suo permesso d'ingresso. Potrei anche giustificare la compagnia giapponese di telefoni cellulari: sono esposti a molti rischi. Ma quel che non capisco è perché richiedano il numero del passaporto se poi non

lo controllano: è questo, a mio modesto parere, il vero difetto della sicurezza, non il fatto che vogliono identificare i loro clienti.

Non posso dire di capire lo stile di vita "americano" e i vostri ideali di pubblica sicurezza. Se ho ben capito, voi non possedete alcun documento che possa affermare la vostra identità (come una carta d'identità). Se questo è vero, come fate ad ottenere un conto in banca? Come dimostrate la vostra identità quando entrate in un'area protetta? Come venite identificati per gli esami universitari? Con la patente di guida? E che succede se non ne possiedo una? Con una firma? Non riesco a fare la stessa firma due volte di fila (ogni tanto la mia banca si rifiuta di darmi i miei soldi per questo motivo). La mia fidanzata è in grado di fare la mia firma meglio di me. Che altro?

Noi in Europa (beh, almeno nell'Europa Centrale e dell'Est) possediamo dei documenti di identità (un'eredità dell'epoca "comunista") e non credo che la nostra sicurezza o privacy sia più compromessa. Devo dimostrare la mia identità se entro in un hotel, ma il proprietario dell'hotel è tenuto a giustificare il perché vuole i miei dati personali, e li deve distruggere una volta che ho lasciato l'hotel dopo aver pagato il conto. Se devo fare un prelievo bancario, devo presentare un documento con la mia fotografia. Si tratta forse di un'inutile seccatura? Non penso proprio. Io la vedo come una misura per proteggere il mio denaro (chiunque voglia derubarmi deve prima rubare o contraffare il mio documento d'identità). Se voglio prendere un'auto o un'imbarcazione in affitto, devo presentare un documento d'identità. È una misura che consente a me di riportare indietro il veicolo, oppure di essere denunciato se lo rubo.

Non sto dicendo che tutti i tentativi di identificazione siano legittimi. Il caso della farmacia nel suo articolo può essere un esempio, ma dato che non ho a disposizione tutti i dettagli, non me la sento di giudicare. Giudizi repentini senza prima avere delle informazioni dettagliate possono essere molto pericolosi.

A mio avviso, il vero problema è che l'uso di uno pseudonimo (come si può vedere in certi sistemi di identità digitale) non è (ancora) possibile nella vita reale. E troppo spesso dobbiamo presentare la nostra completa identità. Ma rifiutando indiscriminatamente ogni tipo di tentativo di identificazione senza distinguere quelli legittimi da quelli che non lo sono, può essere molto dannoso.

Da: Richard Kay <rich@copsewood.net>
Oggetto: Come reagire

Per quanto riguarda la questione di divulgare dati personali in presenza di impiegati ligi alle regole, ho sviluppato l'abitudine di fornire dettagli mescolati ove appropriato, per esempio il mio numero di telefono se non voglio che il mio vero numero venga inserito nel database. Mi sembra sia più semplice incoraggiare un sufficiente numero di persone a seguire l'esempio, che non sensibilizzarle politicamente su una cosa che può apparire, ai non-geek, come una causa tecnica e oscura.

Anche invertire un paio di cifre in un numero di telefono o in un codice di avviamento postale è sufficiente a ridurre la validità di un database, e se sono in tanti a fare così, quei bravi sostenitori del mercato, creatori di regole che obbligano gli impiegati a raccogliere queste informazioni, si ritroveranno con dati inaffidabili e inservibili. Anche nel caso di quei documenti ufficiali dove è reato penale indicare informazioni false, è molto difficile che in tribunale si possa dimostrare come intento volontario di dichiarare il falso quella che può apparire come una piccola e casuale dislessia. E così si possono mettere i bastoni fra le ruote di tutta quella burocrazia indesiderata.

Da: "bill" <bill@strahm.net>
Oggetto: I livelli di allarme nazionale

I suoi commenti in merito ai livelli di allarme nazionale non mi sembrano molto accurati. Lei scrive: "L'esercito degli Stati Uniti possiede un sistema simile: DEFCON 1-5 corrisponde ai cinque livelli di allarme: Verde, Blue, Giallo, Arancio, e Rosso. La differenza sta nel fatto che il sistema DEFCON è legato a particolari procedure; le unità militari hanno delle azioni specifiche da compiere ogni volta che il livello DEFCON sale o scende. Il sistema di allarme cromatico, invece, non è legato ad alcuna azione specifica. Si lascia che la gente si preoccupi, oppure vengono date assurde istruzioni di acquistare rivestimenti plastici e nastro adesivo. Persino i dipartimenti di polizia e le organizzazioni governative locali non hanno idea di cosa fare quando cambia il livello di allarme".

Accadono cose assai specifiche almeno nel caso dei due livelli di allarme che abbiamo visto (giallo e arancio). Anzitutto, durante un allarme arancio posso rendermi conto di come siano aumentate le procedure di sicurezza; vi sono molte più forze dell'ordine all'interno e nei pressi di un aeroporto, vi sono maggiori controlli, ecc. Mi ha molto sorpreso il fatto che non sia stato innalzato il livello di allarme durante il fine settimana della festività del 4 luglio, come è sempre accaduto per tutte le altre festività. Tuttavia quel che ho visto agli aeroporti è stato un livello di allarme "arancio" per la sicurezza. Mi piacerebbe sapere se quelle procedure di sicurezza negli aeroporti sono state silenziosamente aumentate, se è stata una decisione a livello locale (dei due aeroporti che ho visto) o se vi è stato un innalzamento della sicurezza a livello nazionale.

Da: Bron Gondwana <brong@brong.net>
Oggetto: Nascondere gioielli nel vino rosso

Si tratta di una soluzione molto furba, ma qui purtroppo siamo di fronte a un esempio strepitoso di come possa funzionare la sicurezza attraverso l'oscurità (o meglio la sicurezza attraverso l'eccezionalità o attraverso la diversità).

Finché i ladri saranno all'oscuro di questa tecnica, essa continuerà a funzionare; ma nel momento in cui divenisse molto comune -- o fosse sufficientemente divulgata -- essa non funzionerebbe più. I ladri romperebbero tutti quei bicchieri di vino abbastanza prossimi a una signora.

Se il ristorante offrisse un economico rosso della casa per questo scopo, allora il ladro dovrebbe essere cieco (o non molto bravo a fare il suo mestiere) per lasciarsi sfuggire questa possibilità.

Suppongo che le più intelligenti fra quelle donne stiano già pensando ad un nuovo sistema per proteggere i propri averi -- un sistema che non sia ancora diventato di moda e quindi noto. Se fossi una di quelle donne, di certo non parlerei a nessuno della mia tecnica.

Da: "Steven Alexander" <alexander.s@mccd.edu>
Oggetto: Insegnare a scrivere virus

Allan Dyer ha scritto: "Abbiamo bisogno di più persone che siano in grado di capire e di combattere i virus, ma non è necessario creare un virus per questo".

Invece è necessario. Certo, l'idea che sta alla base di un virus o di un worm può essere compresa senza scriverne uno. Tuttavia, per capire veramente come funzionano i virus, diventa necessario scriverne uno. Realizzare un programma che aggiunge un altro programma a se stesso non è la stessa cosa. Infettare nuovi file partendo da eseguibili già infetti è decisamente più difficile perché occorre progettare un programma che possa gestire un caso generale invece di uno specifico.

I virus devono fare cose come rilevare tipi eseguibili ed estrarre il loro codice dal programma infetto in cui stanno girando. A volte, prima di potersi diffondere, devono fare una sorta di

escalation dei privilegi. Copiare un altro programma nel proprio normalmente non richiederebbe una cosa del genere, anche se si potrebbe tentare di aggiungere un programma sul quale non si ha il permesso di lettura. Per essere un esperto del campo occorre conoscere la differenza tra l'infettare un eseguibile .COM, .EXE, Windows PE o ELF; occorre conoscere come le differenze nell'organizzazione della memoria in Windows e Unix influiscono sui virus. Queste sottigliezze saranno destinate a sfuggire se non ci si è mai dedicati alla scrittura di un virus vero e proprio.

Da: "Singer, Nicholas" <nick.singer@us.army.mil>
Oggetto: American Express e la sicurezza

Quando ho telefonato per l'attivazione di una carta di credito American Express che avevo ricevuto per posta, il sistema automatizzato mi ha informato che avrei dovuto associarvi un codice PIN. Il sistema ha aggiunto che ad altri utenti piaceva l'idea di usare il compleanno della propria madre come codice PIN a quattro cifre. Dopo qualche esperimento, ho scoperto che il sistema avrebbe accettato solo quei PIN a quattro cifre che corrispondevano a date: "0229" era ammesso, ma non "0230" e di certo non "3112" (l'ultimo dell'anno, scritto all'europea). In questo modo gli amministratori della condotta del sistema avevano ridotto le possibili combinazioni di PIN a quattro cifre da 10.000 a 366.

Quando ho domandato ad una persona dell'American Express se mi era consentito di usare un PIN dissimile da una data, non ci sono stati problemi, anche se mi è stato detto che non sarebbero stati in grado di fornirmi un indizio nel caso mi fossi poi scordato il codice.

Da: Phil Stripling <philip@civex.com>
Oggetto: "[Non ne ho la più pallida idea]"

Per quanto riguarda la lettera che le è pervenuta "da qualche parte", devo dire di essere sorpreso che lei l'abbia pubblicata e che la tratti come fonte di intrattenimento per i suoi lettori. A me sembra (come a lei, del resto), che provenga da una persona mentalmente malata, e mi spiace dire che non vedo dove sia l'intrattenimento nel vedere quanto soffre questa poveretta. Credo che lei abbia commesso un errore di valutazione.

Da: Andy Brown <logic@warthog.com>
Oggetto: "[Non ne ho la più pallida idea]"

Le scrivo in riferimento al messaggio apparso nella sezione Commenti dei lettori della sua Crypto-Gram del 15 luglio 2003, con intestazione: "Da: Qualcuno, da qualche parte / Oggetto: [Non ne ho la più pallida idea]". Nell'introduzione a questo messaggio, lei dichiara: "La trascrivo qui a solo scopo di intrattenimento".

Con tutto il rispetto, devo dirle che non ho trovato questa lettera per nulla divertente; al contrario, l'ho trovata sgradevole e inquietante nel suo contenuto, nonché fastidiosa, visto che lei ha scelto di divulgarla. Forse, come lei suggerisce, chi ha scritto questa missiva potrebbe soffrire di stati allucinatori. Se fosse così, di sicuro l'autore o l'autrice meriterebbe comprensione -- ma non certo un'esibizione pubblica; e in nessun caso sta a lei (o a me) decidere di attribuirsi il ruolo da psicanalista onnisciente. ("... paranoia depressiva..."? Si tratta di un'etichetta molto forte, che persino gli "esperti" non usano volentieri).

Da: Andy Brown <logic@warthog.com>
Oggetto: "[Non ne ho la più pallida idea]"

La paranoia, in piccole dosi, è una virtù per un diligente professionista della sicurezza. La convinzione errata è fra i vizi peggiori. Vedere come queste due si siano scontrate nell'ultimo

numero di Crypto-Gram è stato affascinante. Ancor di più dopo aver speso qualche minuto cercando su Google e trovando qualche collegamento con la realtà da parte della lettera di quella povera donna.

Nella posizione in cui lei si trova, immagino riceva tutta una serie di lettere bizzarre. Ma sono sicuro di non essere l'unico suo lettore che vorrebbe vedere altre lettere come questa pubblicate su Crypto-Gram, anche omettendo l'identità degli innocenti. Trovo che il rapporto fra crittografia e psicologia sia importante all'atto pratico, e che spinga alla riflessione. Lei si trova in una posizione davvero speciale per condividere queste misture interessanti (anche se a volte inquietanti), e la incoraggio in questa direzione.

Da: Alexandre <salexru2000@sympatico.ca>

Data: Friday, August 08, 2003 1:53 PM

A: info@counterpane.com

Oggetto: "[Non ne ho la più pallida idea]"

Avendo familiarità con alcuni aspetti della paranoia, questa lettera ha destato il mio interesse, poiché è noto che in molti casi la paranoia persecutoria è causata da motivi reali. L'aggressore deve solo essere tenace ed avere abbastanza risorse per squilibrare l'universo della sua vittima. Potrebbe essere attraverso una droga, indotta tramite l'ambiente e/o in maniera motivazionale.

Questo fa sorgere una questione interessante e ancora non risolta: quali tecniche potrebbero essere usate per differenziare la realtà dall'immaginazione, sempre che esista davvero una realtà? In che modo la realtà potrebbe venire "autenticata"?

Questa donna non sembra essere molto divertita dalla sua situazione -- di certo si sta "autenticando" in maniera sbagliata. Potrebbe già essere troppo tardi per lei. Ad ogni modo, quando si riceve un messaggio e-mail da una fonte nota o sconosciuta, che pare inneschi o stimoli il processo nel caso di questa donna, come si può essere sicuri dell'autenticità delle informazioni? Forse ci sono state rubate o forzate password, chiavi, o altri segreti, e sono state usate contro di noi e ancora non lo sappiamo. Forse la persona che ci chiama al telefono è solo una sintesi vocale computerizzata o una voce registrata. Il futuro potrebbe anche essere peggiore, in questo senso -- come la mettiamo con i cloni e l'intelligenza artificiale, che inganneranno qualsiasi dispositivo biometrico?

Non si possono combattere le allucinazioni o le convinzioni errate e non è possibile nemmeno ignorarle, specie quando non si è in grado di distinguere fra allucinazioni e realtà. Nella vita quotidiana ci affidiamo a criteri di "buonsenso". Se accade qualcosa che è insolito/dannoso? Insolito è un segnale d'allarme. Dannoso anche. Allora diventiamo cauti. E il buonsenso ci aiuta a fermarci prima di essere sommersi da un'ondata di "che succederebbe se...". Purtroppo questo approccio non funziona molto bene su vasta scala -- non possiamo prevedere con un certo margine di sicurezza se le nostre azioni saranno dannose alla lunga, e a scapito di chi -- come nell'episodio dei dati del passaporto fasulli che lei ha raccontato. Magari l'anno prossimo lei potrebbe essere scartato in quanto "persona sospetta", o forse peggio, giusto?

La crittografia trasuda paranoia -- può contribuire a combatterla? O sta soltanto contribuendo ad alimentare tendenze paranoiche? Più si è al corrente di come "loro" possono ingannarci, più si diventa sospettosi, giusto?

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

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

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.

Inoltrate liberamente CRYPTO-GRAM a colleghi ed amici che possano trovare la rivista interessante. Viene concessa l'autorizzazione a ristampare CRYPTO-GRAM, a condizione che sia stampata integralmente.

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è il fondatore e CTO di Counterpane Internet Security, Inc., autore di "Secrets and Lies" e di "Applied Cryptography" e inventore degli algoritmi Blowfish, Twofish e Yarrow. È membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla crittografia.

Counterpane Internet Security, Inc. è leader mondiale nel monitoraggio guidato della sicurezza informatica. Gli analisti esperti in sicurezza di Counterpane proteggono reti per aziende inserite nella Fortune 1000 a livello mondiale.

Copyright (c) 2003 by Counterpane Internet Security, Inc.