Indice

1. NUOVI SOCI

Hanno aderito al Clusit:

- ACHAB (Milano)
- CSQA Certificazioni (Thiene - VI)
- Ente Nazionale per l'Aviazione Civile (Roma)
- Promotion Digitale (Merate - LC)

2. ETICA DELLA SICUREZZA

Etica della sicurezza.

La soluzione è un modello collaborativo che esca dai confini dell'azienda.

Dall'epoca "cavalleresca" degli hacker alla ricerca del gesto éclatante, siamo passati alla criminalità organizzata che vede nella rete un campo d'azione particolarmente allettante. Alla vulnerabilità per gli attacchi si associa una vulnerabilità dovuta alla complessità di un vero e proprio ecosistema fatto di milioni di macchine e milioni di utenti con l'aggiunta della totale mobilità. É difendibile un sistema simile? Quali sono i principi della sicurezza che rimangono validi e quali i miti da sfatare? Quali cambiamenti dopo l'11 settembre e, soprattutto, quali strategie adottare per difendere il valore dell'informazione? Sappiamo per certo che l'informazione è un bene prezioso e che potrà essere difeso solo con uno sforzo collaborativo che superi l'egoismo dei singoli e consideri la rete un patrimonio comune.

Con la diffusione pervasiva di sistemi informativi in rete, il tema della sicurezza informatica, da materia esoterica per addetti ai lavori è diventata argomento di interesse comune e fonte di giusta preoccupazione dei singoli individui oltre che di aziende ed enti pubblici. A fronte di una situazione in continuo mutamento, ci sono aspetti legati alla sicurezza delle informazioni che non sono cambiati e che vale la pena di conoscere, come è bene sfatare alcuni concetti che sono del tutto infondati.

Il bisogno di sicurezza è un bisogno primario che viene subito dopo il soddisfacimento dei bisogni fisiologici, è la condizione necessaria perchè si possano stabilire relazioni con gli altri perchè in un ambiente "insicuro" non siamo a nostro agio e le emozioni hanno il sopravvento sulla ragione. Viviamo

in un mondo di incertezze, incertezze che sono cresciute e mutate con le trasformazioni sociali e chiediamo all'informatica certezze che non abbiamo nella nostra vita quotidiana. I computer sono sempre più affidabili e sicuri ma l'ecosistema in cui interagiscono li pone in una condizione di pericolo costante. Il mondo dell'informatica, presentato come il mondo binario degli 1 e degli 0 in cui non esistono sfumature, ingenera inoltre una forte aspettativa di certezza e di prevedibilità nella convinzione del totale dominio dell'uomo sulla macchina. Ricordo che il padre della cibernetica italiana Silvio Ceccato parlando del computer lo chiamava "l'idiota fulmineo" perchè se istruito dall'uomo a fare una cosa sbagliata la faceva comunque e sempre a velocità straordinaria.

Dobbiamo innanzitutto accettare serenamente il primo principio: la sicurezza non esiste. Non potremo mai essere sicuri al 100% così come non possiamo aspettarci di vivere in eterno o di essere sempre in buona salute. La sicurezza deve conciliare aspetti tra loro conflittuali: le reti vogliono far comunicare liberamente e velocemente persone e imprese, la sicurezza vuole chiudere e controllare tutto. Se è vero che non esiste in assoluto, la sicurezza è la ricerca di un equilibrio dinamico, cioè sempre in movimento, tra apertura e chiusura, tra improvvisazione e regole, tra costi e danni.

Il secondo principio dice che la sicurezza è un'emozione: non è una condizione oggettiva uguale per tutti ma fa entrare in gioco importantissimi fattori emotivi e di vissuto personale, che a parità di situazione portano ad azioni molto diverse fra loro. La sicurezza riguarda quindi i comportamenti e non solo le tecnologie e richiede una forte coerenza nell'interazione fra i due: che senso ha una porta blindata se lascio la chiave nella toppa? Che senso ha una password lasciata in chiaro sul tavolo? Il terzo principio dice che la sicurezza è la gestione di un rischio e in sostanza riassume i primi due: dobbiamo scegliere fino a che punto "sentirci" sicuri e quanto investire economicamente, in rinunce, in regole, in prodotti, per raggiungere questa condizione emotiva e oltre tale soglia accettare il rischio.

La sicurezza dovrebbe quindi ridurre il rischio in termini accettabili o sostenibili economicamente dall'impresa, per poi lasciare il "rischio residuo" al mondo delle assicurazioni. Qual'è, sempre parlando di principi, il più grande nemico della sicurezza? É l'abitudine. Dopo un attentato i controlli sono rigorosissimi e diventa particolarmente sicuro viaggiare, anche se logisticamente più problematico, mentre a distanza di qualche mese, quando l'allarme rientra e i controlli si attenuano, sale proporzionalmente il rischio di subire un nuovo attacco. La sicurezza vive di routines e controlli, pensate al check che fanno i piloti prima di tutti i decolli, ma guai se vengono fatti distrattamente e senza la consapevolezza di compiere un gesto importante per la propria vita e quella degli altri. Da queste considerazioni deriva il pilastro principale su cui poggia la sicurezza: il backup, la copia di sicurezza, il sistema d'emergenza.

Se si parte dall'assunto che non esiste la sicurezza assoluta non ci si deve domandare cosa fare SE avremo un guasto o un incidente, bensì cosa fare DATO CHE prima o poi avremo un guasto o un incidente.

Il brano è tratto dal saggio “Etica della sicurezza” di Gigi Tagliapietra, pubblicato integralmente sul secondo volume di Nòva24 Review, il bimestrale di ricerca, innovazione e creatività del Sole 24 ORE. Per ulteriori informazioni: www.ilsole24ore.com/nova.

3. CYBERCRIME

Perché non ci sono più attacchi massicci di virus?

Vi ricordate i tempi di NIMDA, CODE RED, GAOBOT, e così via? Perché non si bloccano più le aziende? Perché milioni di computer non si fermano più, tutti assieme, un dato giorno? Ci sono tanti virus, tanti computer ogni giorno si bloccano, ma non è un attacco preoccupante. Almeno come in passato.

I giornali ne parlano poco. I possessori di computer dormono sonni tranquilli. Sono convinti di essere protetti. Lo sono veramente? Hanno l'ultima versione dell'antivirus? Siamo certi?

Una nostra indagine ha rivelato che su 100 utenti che hanno a casa il personal computer, tutti hanno un antivirus, ma solo il 45% si ricorda di quando ha scaricato l'ultimo aggiornamento! Il 5% è caduto dalle nuvole ed ha chiesto addirittura spiegazioni!

Hanno tutti un personal firewall attivato? Sono state inserite delle regole per impedire l'uscita dal pc di informazioni personali? Il 75% ha risposto di no.

Allora una domanda viene spontanea: non è che questa apparente "tranquillità" sta progressivamente indebolendo le difese? Non delle aziende, ma bensì di coloro che utilizzano il computer a casa, dove tengono dati personali e da dove fanno transazioni su Internet.

Abbiamo accennato tempo fa alla nostra preoccupazione: non si sta preparando un attacco massiccio?

Correggiamo la domanda: non è che criminali (non trascurando i terroristi) stanno installando "trojans" sui computer e da lì si preparano a prelevare dati o ad attaccare le aziende? Milioni di computer potrebbero diventare dei temibili nemici.

Ecco allora l'invito nuovamente ai media: sensibilizzate, nel dovuto modo, i consumatori.

Come il Cliente aggiunge l'olio al motore per evitare di perdere l'auto ed i soldi, così aggiunga sicurezza al computer.

Ne basta poca: quella suggerita dal venditore o dal negoziante sotto casa. Nulla di più.

Noi chiaramente siamo sempre disponibili a fornire informazioni ed aiuto.

Anthony Cecil Wright, Presidente ANSSAIF - www.anssaif.it

4. QUANDO IL PIN LO DIGITA IL TOPO

Quanti di noi hanno un conto bancario online (ed ormai siamo in tanti), e` probabile che negli ultimi mesi abbiano dovuto far l'abitudine al cosiddetto "tastierino".

E` questo il caso, per esempio, dei clienti di Deutsche Bank e di ING Direct, ma la pratica si sta diffondendo. In che cosa consiste? Il PIN necessario per accedere ai servizi non viene piu` digitato tramite la tastiera, bensi` l'utente deve cliccare con il mouse su una serie di pulsanti che rappresentano un tastierino numerico, la cui disposizione cambia ad ogni accesso.

L'operazione e` una discreta seccatura: nel caso conserviate, come il sottoscritto, tutte le password in un archivio criptato (p.es. utilizzando Password Safe [1]) facendone copia e incolla ogni volta che ne avete bisogno, dovrete cambiare le vostre abitudini: il PIN va inserito infatti un numero alla volta riconoscendo i pulsanti corretti e operando unicamente con il mouse.

Ma la sicurezza, lo sappiamo tutti, richiede qualche piccolo sacrificio, giusto? Certamente, quando l'efficacia di una misura e`proporzionata al costo che impone.

Quali sono dunque le minacce da cui il "tastierino" ci difende? Essenzialmente dovrebbe costituire una protezione contro i cosiddetti "keylogger", programmi maligni che intercettano l'input della tastiera, spedendo poi le informazioni rilevate al malintenzionato di turno. Si tratta percio` di un classico attacco di /eavesdropping/ (intercettazione) seguito dal riutilizzo non autorizzato (replay) dei dati rilevati.

Il tastierino e` efficace contro questo attacco? La mia risposta e`no. Lasciamo pure perdere il fatto che l'intercettazione puo` avvenire tramite un agente umano che ci scruta alle spalle, e in questo caso l'azione del mouse e` senz'altro assai piu` evidente di un veloce digitare da tastiera o, meglio, un copia e incolla criptato.

Ma anche nel caso del programma maligno la protezione e` soltanto apparente. In effetti la presenza di un keylogger significa che la macchina e`compromessa ossia che non ci si puo` piu` fidare del suo comportamento. Nulla vieta (non certo il sistema, ormai, abbiamo detto, compromesso), che anziche` le operazioni da tastiera vengano intercettate le schermate e le coordinate dei clic dei mouse, informazioni del tutto sufficienti al malintenzionato attaccante per ricostruire il PIN dell'utente.

Si conoscono misure alternative piu` efficaci? Contro l'eavesdropping-replay si`. E` possibile per esempio utilizzare One Time Password (OTP) che funzionano per una sola transazione. L'OTP puo` essere generata da un dispositivo hardware separato oppure richiesta preventivamente tramite un canale differente, per esempio via SMS (che, per inciso, non sara`piu` un canale differente quando la "convergenza" ci avra` abituati a navigare col telefonino). Oppure e` possibile che la banca ci chieda solo /una parte,/ ogni volta diversa, della password: se la password e` sufficientemente lunga, l'attaccante e` costretto a intercettare molto traffico prima di riuscire a ricostruire il dato privato. Fra l'altro questo e` proprio il meccanismo utilizzato da una delle due banche citate all'inizio (Deutsche Bank) per autenticare le operazioni piu` critiche, come i bonifici. Perche` non adottare la stessa strategia, imperfetta ma piu` efficace, anche per il login?

Concludo precisando che, come ha spiegato bene Bruce Schneier [2], le tecniche di cui sopra non ci difendono comunque dai due attacchi piu` insidiosi: il "man in the middle", in cui l'utente viene ingannato in maniera tale che l'autenticazione avvenga su di un sito approntato dall'attaccante (il quale poi riutilizza i dati così raccolti per un'autenticazione reale) e il "trojan attack", in cui l'attaccante manipola una sessione /dopo/ che l'utente si e` gia`autenticato (compiendo poi operazioni all'insaputa dell'utente).

I cattivi, dice Woody Allen, hanno spesso capito qualcosa che i buoni ignorano. Non lasciamoglielo sfruttare.

[1] http://passwordsafe.sourceforge.net/

[2] B. Schneier, "Two-Factor Authentication: Too Little, Too Late", Communication of the ACM, April 2005, Vol. 48, n. 4

Autore: Mattia Monga, Ricercatore presso il Dipartimento di Informatica e Comunicazione dell'Università degli Studi di Milano, membro del Comitato Direttivo del Clusit

5. L'ACQUISIZIONE DELLA DIGITAL EVIDENCE DA PARTE DELLA POLIZIA GIUDIZIARIA

Riportiamo un articolo dell'Avv. Andrea Monti, socio fondatore e membro del CD Clusit, tratto dal terzo numero di ICTLEX BRIEFS

www.ictlex.com - http://www.ictlex.com/?p=48

Il concetto, in sintesi

- Non sempre la polizia giudiziaria acquisisce l'elemento di prova informatica secondo le regole della computer forensics.
- L'esperienza dimostra che ciò accade per una sorta di sottovalutazione della delicatezza delle attività che si stanno compiendo.

- Questo si traduce in comportamenti che possono pregiudicare l'utilizzabilità e il valore probatorio delle informazioni, sia nella fase delle indagini, sia in quella del dibattimento.
- I problemi aperti riguardano la documentazione dei contenuti di una risorsa o di un servizio di rete (web, newsgroup, chat), l'acquisizione dei contenuti dei supporti di memorizzazione, l'accesso alle informazioni generate da sistemi che non possono essere spenti (es.: server di internet provider, sistemi di contabilità).
- La magistratura non ha ancora assunto un orientamento condiviso sul punto. Ma prevale la posizione di chi non attribuisce particolare rilevanza giuridica al rispetto delle regole dettate dalla computer forensics.
- Nell'acquisizione degli elementi di prova informatica presso ISP e operatori telefonici, la polizia giudiziaria non ha l'obbligo di seguire procedure particolari.
- Questo significa che l'acquisizione materiale di quanto necessario può avvenire ordinando all'operatore la semplice consegna dei dati, senza che la polizia esegua alcun controllo.
- L'operatore si assume in proprio la responsabilità giuridiche di eventuali discordanze fra quanto consegnato alla polizia giudiziaria e quanto effettivamente dovesse risultare dalle proprie infrastrutture.

Il concetto, in teoria

1. Case history

Negli ultimi anni si è registrata una vera e propria proliferazione di file, tabulati telefonici (call data record) o altri "oggetti digitali" presentati come prove nei processi penali. Questo ha indotto il pubblico ministero e il difensore (più il secondo che il primo, per la verità) a porsi il problema dei limiti di ammissibilità degli elementi di prova informatica raccolti dalla polizia giudiziaria. Non sempre quest'ultima opera in modo da consentire alla difesa di verificare a posteriori la genuinità di quanto viene presentato al processo, come dimostra la breve case history che segue. Volendo classificare alcuni dei casi in cui l'informatica ha giocato un ruolo centrale, si può dire che le attività di indagine della polizia giudiziaria si sono tradotte in:

- stampa di pagine web residenti su server localizzati al di fuori della giurisdizione italiana (Trib. penale Teramo, sent. 112/02, ma anche Trib. penale Pescara, sent. 6 ottobre 2006 relativa al p.p. n. 7320/ 02, in attesa di motivazione);
- ricorso a dichiarazioni di fonti confidenziali non utilizzabili, senza riscontri indipendenti (Trib. penale Pescara, sent. 1593/05);
- acquisizione di file di log tramite mera consegna dei dati da parte dell'internet provider, senza verifi- carne le modalità di conservazione in rapporto alla loro genuinità e attendibilità nel tempo (Trib. penale Chieti, sent. 175/05);
- invio al potenziale indagato, in chat pedopornografiche e durante attività sotto copertura, di immagini senza adottare adeguate cautele per dimostrare che quanto rinvenuto successivamente sul computer dell'indagato, fosse proprio ciò che l'operatore di PG aveva inviato (Trib. penale Civitavecchia, sent. 1277/04);
- sequestro di interi elaboratori, senza alcuna preventiva (o immediatamente successiva) selezione del materiale rilevante ai fini della prova (Trib. riesame Torino, Ord. 7 febbraio 2000);
- accesso remoto della polizia giudiziaria alla porzione di hard disk condivisa, durante una sessione peer-to-peer, senza specifico decreto di perquisizione

del computer stesso, sul presupposto che l'area in questione fosse aperta a chiunque (Trib. riesame Venezia, Ord. 62/05);

- perquisizioni e analisi tecniche dei contenuti di un disco rigido senza adottare modalità che garantissero la ripetibilità dell'atto (Trib. penale Bologna, sent. 1823/05);
- ispezioni compiute sul posto dall'ausiliario di polizia giudiziaria, senza alcuna documentazione delle attività svolte (Trib. penale Savona, sent. 844/04).

Il dato comune che emerge dai casi appena citati è il ruolo centrale della polizia giudiziaria nella raccolta degli elementi di prova. Spesso, infatti, il pubblico ministero tende a delegare il compimento di atti investigativi alla polizia giudiziaria che, a sua volta, può anche sub-delegare l'esecuzione degli ordini del magistrato. Il risultato di questo progressivo smagliamento del controllo sulle componenti tecnologiche dell'indagine, fa si che non sempre l'ultimo anello della catena abbia le necessarie competenze.

2. La gatta frettolosa…

A prescindere da come siano andati a finire i singoli processi (alcuni, fra i casi citati, si sono conclusi con assoluzioni, altri con delle condanne), un altro elemento ricorre molto di frequente nel corso dei processi che coinvolgono i computer: la tendenza della polizia giudiziaria ad affidarsi sempre di più alla sola indagine informatica, trascurando metodi più tradizionali, ma non per questo privi di efficacia.

Dalla prospettiva degli inquirenti, questo "sbilanciamento investigativo" fa sicuramente muovere più in fretta il procedimento penale e con minore impiego di risorse e rischio per il personale. Ma, dal punto di vista del difensore, questo approccio è anche un valido strumento sia per ottenere informazioni con largo anticipo rispetto ai tempi stabiliti dal codice di procedura penale, sia per rilevare, in dibattimento, errori tecnici che, non essendo supportati da altre attività di indagine, provocano l'impossibilità per la polizia giudiziaria di riferire sugli accertamenti eseguiti vanificando di fatto l'indagine. Il ricorso indiscriminato ed eccessivamente esteso al sequestro probatorio di materiale informatico, per esempio, consente all'indagato di presentare una richiesta di riesame al tribunale della libertà.

Grazie a questa richiesta egli avrà il diritto di ottenere tutte gli atti che, secondo il pubblico ministero, avrebbero giustificato l'emissione del provvedimento di sequestro. Spesso, a questi atti non se ne aggiungono altri, e quindi l'indagato sa già dalla fase iniziale dell'indagine (quella, cioè, in cui il segreto è, o sarebbe, essenziale), quali siano gli "assi" in mano alla pubblica accusa. Anche l'adozione di "scorciatoie procedimentali" come la perquisizione autorizzata verbalmente dal magistrato, o l'analisi del computer dell'indagato senza adottare alcuna cautela per evitare l'alterazione anche accidentale dei dati, possono compromettere (dal punto di vista dell'accusa) l'esito del processo.

E' vero che ci sono state decisioni secondo cui la mancata adozione da parte della polizia giudiziaria delle cautele richieste dalle best practice di computer forensics non è di per sé causa di esclusione del valore probatorio (vedi la sentenza del Tribunale di Bologna, appena citata, o quella del Tribunale penale di Milano, 4 settembre 2006, relativa al p.p. n. 12803/03, in attesa di motivazione). Come è anche vero, però, che in altri casi proprio l'inosservanza da parte della polizia giudiziaria dei più elementari requisiti tecnici in fase di acquisizione degli elementi di prova informatica, ha consentito di far escludere dalle indagini del materiale già acquisito al fascicolo del pubblico ministero (vedi la sentenza, qui citata, del Tribunale di Chieti), o di annullare un sequestro probatorio (come nel caso dell'ordinanza 9 ottobre 2006 del Tribunale del riesame di Brescia, relativa al procedimento penale n.121/06, inedita).

3. "Chi" deve provare "cosa"?

Il problema fondamentale del ruolo della computer forensics nel procedimento penale è sintetizzato in un passo della già citata sentenza n. 1823/05 del Tribunale penale di Bologna: … non è permesso al Tribunale escludere a priori i risultati di una tecnica informatica utilizzata a fini forensi solo perché alcune fonti ritengono ve ne siano di più scientificamente corrette, in assenza della allegazione di fatti che suggeriscano che si possa essere astrattamente verificata nel caso concreto una qualsiasi forma di alterazione dei dati e senza che venga indicata la fase delle procedure durante la quale si ritiene essere avvenuta la possibile alterazione.

In pratica, dice il Tribunale, tocca alla difesa dimostrare che le operazioni tecniche della polizia giudiziaria hanno alterato i dati. Senza questa prova non si può mettere in discussione il valore probatorio di quanto acquisito dalla polizia giudiziaria. A meno di errori clamorosi commessi dalla polizia giudiziaria, quindi, non ha particolare importanza il metodo con il quale viene raccolto l'elemento di prova informatica, purché appaia attendibile (qualsiasi cosa questo significhi).

Benché rinforzata da un illustre precedente secondo il quale eccepire semplicemente la possibilità che le prove siano state alterate non è sufficiente a rendere le prove inammissibili (Corte Suprema degli Stati Uniti, USA vs Allen, 106, F3d 695, 700 - 6th Cir. 1997), la posizione del Tribunale di Bologna non è condivisibile.

Molto raramente (quasi mai) le attività di acquisizione dell'elemento di prova digitale avvengono alla presenza del difensore e se in quel momento vengono commessi errori, sarà praticamente impossibile dimostrare che si sono verificati. In altri termini: se acquisendo dei file di log tramite un banale "copia-e-incolla" i dati vengono modificati (per esempio, perché invece di un text-editor, si utilizza un word processor con il correttore ortografico attivo), una volta giunti al processo non c'è modo, per la difesa, di dimostrare il contenuto originale di quanto presentato al giudice.

Ma prima ancora di questa considerazione pratica, ne viene una di ordine generale: è onere del pubblico ministero dimostrare positivamente la "bontà" delle sue prove, e non obbligo della difesa farsi carico di dimostrare il contrario.

4. Conseguenze pratiche per ISP e operatori telefonici

Benché discutibile, è probabile che si consolidi l'orientamento di ammettere come prova nel processo un "oggetto informatico" acquisito senza particolari cautele.

Dunque la polizia giudiziaria che richiede dati di traffico o altre informazioni legate all'uso che un certo soggetto abbia fatto dei servizi offerti dall'ISP, continuerà a non avere l'obbligo di seguire particolari procedure o di osservare specifiche cautele tecniche. Potrà infatti limitarsi a chiedere all'operatore di consegnare le informazioni di cui dispone, lasciando all'operatore stesso la scelta di come comportarsi.

Se dal punto di vista della polizia giudiziaria il rispetto delle best practice di computer forensics potrebbe essere facoltativo, nel caso dell'operatore sarebbe opportuno che queste regole tecniche fossero, al contrario, seguite con scrupolo per evitare, proprio malgrado, di essere coinvolti nelle fasi successive del processo.

Se, infatti, la polizia giudiziaria dichiara di essersi limitata a ricevere un supporto contenente i dati di interesse, è praticamente automatico che il difensore dell'indagato chiamerà a testimoniare il personale dell'operatore che ha materialmente eseguito le operazioni. O, se l'identità non è nota, verrà chiamato il legale rappresentante dell'azienda che poi dovrà dichiarare l'identità del dipendente.

Per evitare, o comunque limitare al massimo l'invio di personale in giro per le città giudiziarie italiane, è quindi necessario adottare delle procedure di estrazione e memorizzazione dei dati, con documentazione delle attività svolte da allegare al supporto contenente i dati richiesti.

In questo modo l'operatore potrà supplire alla frequente "sintesi" di verbalizzazione degli operatori di polizia giudiziaria, evitando così di essere chiamato a testimoniare, magari dopo anni, su fatti di cui non conserva nemmeno memoria.

Il concetto, in pratica

- E' opportuno che il fornitore di servizi di comunicazione elettronica predisponga una postazione collegata ai sistemi informativi interni e dotata di: stampante, scanner, masterizzatore, disco rigido esterno, lettore di smart-card per firma digitale, software di computer forensics da mettere a disposizione della polizia giudiziaria.
- E' preferibile che i software di forensics utilizzati siano open source e che venga certificata la non alterazione dei sorgenti, in modo da evitare contestazioni sull'attendibilità dei risultati. _ Le operazioni di estrazione di dati, quando sono svolte da personale del fornitore di servizi di comunicazione elettronica, devono essere estremamente dettagliate.
- Documentare le attività svolte mette in condizione l'operatore di fornire le informazioni richieste dalla difesa dell'imputato anche a distanza di tempo e nel caso in cui non sia più reperibile il soggetto che aveva compiuto le attività richieste dalla polizia giudiziaria.
- Quando è necessario masterizzare o comunque duplicare file su un supporto non riscrivibile, è opportuno estrarre una hash dei file in questione, da confrontare con quella della copia masterizzata.
- Per evitare che il rappresentante legale dell'operatore sia chiamato in giro per l'Italia a comunicare il nominativo di chi ha materialmente svolto le operazioni di ricerca ed estrazione dei dati, è necessario far risultare sempre l'identità della risorsa impiegata.

6. PERCEZIONI E COMPORTAMENTI DEI TELELAVORATORI: FATTORI CHIAVE PER LA SICUREZZA AZIENDALE

Un recente studio commissionato da Cisco e realizzato a livello globale da Insight Express - importante società di ricerca indipendente - ha mostrato che sebbene i telelavoratori affermino di essere a conoscenza delle problematiche di sicurezza, il loro comportamento - che include la condivisione dei computer aziendali con persone al di fuori dell'ambito lavorativo, l'apertura di e-mail di dubbia provenienza e l'utilizzo non autorizzato di reti wireless altrui - lascia supporre il contrario, ovvero che non sia del tutto noto quale sia potenzialmente l'impatto negativo dei loro comportamenti sulla sicurezza aziendale. Tale ricerca, effettuata in tre fasi, evidenzia inoltre le percezioni dei telelavoratori nei confronti dell'IT manager, e viceversa come l'IT manager pensa di essere considerato dal telelavoratore.

Al fine di comprendere al meglio come le percezioni e il comportamento dei telelavoratori vadano ad intensificare i rischi di sicurezza per l'intera comunità in rete, le aziende IT e le organizzazioni per cui lavorano, la ricerca è stata condotta, in una prima fase, su un campione complessivo di 1.000 telelavoratori e nella seconda e terza fase, su un ulteriore campione di 1.000 IT decision maker nei seguenti 10 Paesi: Stati Uniti, Inghilterra, Francia, Germania, Italia, Giappone, Cina, India, Australia, e Brasile. I risultati di tale studio mettono in

luce le problematiche che i dipartimenti IT si trovano ad affrontare a seguito dei comportamenti pericolosi o a rischio dei dipendenti che lavorano al di fuori dell'ufficio (telelavoro) - una pratica lavorativa che può accrescere la produttività ma che allo stesso tempo può compromettere la sicurezza aziendale.

Prima fase: percezioni e comportamento dei telelavoratori

Lo studio ha rilevato che la maggior parte dei lavoratori mobili è convinta di operare in modo sicuro, nonostante continui ad attuare comportamenti on-line potenzialmente pericolosi. Alcune evidenze:

· Shopping online: Circa il 40% dei telelavoratori intervistati (il 47% in Italia) ha affermato di utilizzare il proprio computer aziendale per fare shopping su Internet. La metà ha affermato di fare personalmente gli acquisti on-line perché "alla loro società non dà fastidio che lo facciano" (41% in Italia).

· Condivisione dei computer con persone esterne all'azienda: Il 21% degli intervistati (il 31% in Italia) ha affermato di permettere ad altre persone di utilizzare il proprio computer aziendale. Un intervistato su quattro (il 50% in Italia) afferma di "non vedere niente di sbagliato in questo comportamento" e di essere convinto che l'utilizzo condiviso dei computer "non aumenta i rischi alla sicurezza" (il 13% in Italia).

· Comportamento wireless pericoloso: Un intervistato su dieci (il 18% in Italia) ha dichiarato di aver utilizzato la connessione Internet di un vicino, mentre lavorava in remoto. La maggioranza ha affermato di agire in tal modo perché "era una situazione di emergenza." Il 18% degli intervistati (il 21% in Italia) ha affermato "i miei vicini non lo sanno, quindi va bene così."

· Dispositivi personali: Circa la metà degli intervistati ha dichiarato di utilizzare i propri dispositivi elettronici personali per accedere alle risorse aziendali.

Tuttavia solo la metà degli intervistati (il 29% in Italia) ha detto di avere un software antivirus o di sicurezza installato sul proprio computer.

· Scaricamento delle e-mail: Il 38% degli intervistati (il 34% in Italia) ha affermato di aprire e-mail di provenienza sconosciuta ma non gli allegati.

Nonostante i telelavoratori comprendano l'importanza che la sicurezza ricopre per la propria azienda, il loro comportamento suggerisce ai dipartimenti IT aziendali di aumentare il proprio impegno e gli investimenti nella formazione e nella collaborazione con gli utenti. Incoraggiando attivamente una comunicazione bi-direzionale con gli utenti, l'IT manager può compiere un importante passo avanti verso una maggiore comprensione delle strategie di sicurezza aziendali da parte degli utenti.

Seconda fase: Il ruolo dell'IT manager

Sulla base dei dati emersi dal precedente studio, la seconda fase della ricerca ha analizzato due importanti aspetti: le percezioni dei telelavoratori nei confronti dell'IT manager, e -viceversa? come l'IT manager pensa di essere considerato dal telelavoratore. In sei Paesi su dieci tra quelli sopra citati, i telelavoratori riconoscono ai loro superiori, invece che al dipartimento IT, l'autorità di controllare i loro comportamenti informatici.

In generale, il 13% dei telelavoratori dichiara che nessuno all'interno all'azienda ha l'incarico di controllare i dispositivi informatici. L'Italia è fra le eccezioni: il 49% si affida all'IT manager, il 16% al proprio superiore mentre il 35% dichiara che non è compito di nessuno.

Tali risultati, non hanno invece stupito i professionisti IT intervistati, che dichiarano di essere consapevoli della percezione che i telelavoratori hanno del loro ruolo. Secondo il 53% dei professionisti IT intervistati (il 42% in Italia), gli utenti non riconoscono ai dipartimenti IT la responsabilità di controllare il modo con cui vengono utilizzati gli strumenti informatici dell'azienda.

Terza fase: Gli investimenti nella sicurezza

La terza fase della ricerca, ha invece analizzato l'andamento delle chiamate agli help desk IT e la propensione ad effettuare investimenti nella sicurezza.

Globalmente, il 38% dei decision-maker intervistati (il 42% a livello italiano) ha registrato una crescita delle chiamate all'help-desk per incidenti relativi alla sicurezza che coinvolgono gli utenti e i loro dispositivi informatici utilizzati per lavoro. Tra le principali cause di tale aumento compaiono: attacchi di virus e/o worm (48% globalmente, 35% in Italia), spyware e/o adware (47% globalmente, 40% in Italia), spam e/o phishing (52% globalmente, 49% in Italia), furto di identità (26% globalmente, 12% in Italia), hacking (28% globalmente, 14% in Italia). A fronte di tutto ciò, il 67% degli intervistati (il 66% a livello italiano) ha dichiarato di prevedere maggiori investimenti in sicurezza nel corso del prossimo anno, e di questi il 41% (il 34% in Italia) prevede un aumento della spesa superiore al 10%.

"Questi dati sono una chiamata alle armi per i dipartimenti IT e Sicurezza," ha affermato Jeff Platon, vice president of security solutions marketing di Cisco. "La ricerca mostra chiaramente che la consapevolezza dimostrata dagli utenti non risulta sempre in un comportamento sicuro, e dal momento che molti utenti rigettano l'autorità dell'IT, non danno credito al proprio team IT né si rivolgono ad esso. Analizzando questi dati, non sorprende quindi che i dipartimenti IT stiano registrando un numero più elevato di chiamate all'helpdesk e che ci sia una maggiore propensione agli investimenti in sicurezza. Comprendere le motivazioni che sottostanno a tali trend, significa che i responsabili IT devono adottare con urgenza un approccio più progressivo per proteggere i dati aziendali e gli impiegati."

"La tecnologia è un importante elemento nella sicurezza, ma non è tutto", ha aggiunto John N. Stewart, chief security officer di Cisco. "La sicurezza è in primo luogo un esercizio umano. Vi è un aspetto interpersonale che coinvolge la comunicazione e un impegno costante nella formazione, educazione e riconoscimento.

Creare delle solide relazioni all'interno dell'azienda permette ai responsabili IT di essere percepiti dall'utenza come una presenza strategica e consulenziale in grado di favorire una cultura aziendale consapevole in fatto di sicurezza. Quando ciò avviene, i CIO e i CSO sono in grado di massimizzare il ritorno dagli investimenti effettuati in soluzioni di sicurezza e di prevenire i pericoli che insidiano la produttività".

"Mai come oggi, la Sicurezza è di così fondamentale importanza per le organizzazioni: le reti rappresentano per qualsiasi impresa lo strumento più importante per ottenere vantaggi competitivi, raggiungere nuovi mercati, creare nuove fonti di reddito e migliorare i livelli di produttività. Tale trasformazione è possibile solo se le infrastrutture e i sistemi informatici sono in grado di garantire adeguati livelli di Sicurezza. Protezione e integrità della rete sono infatti componenti essenziali di ogni strategia di e-business", ha affermato Roberto Mircoli, Security Business Development Manager di Cisco e membro del Comitato Direttivo del CLUSIT.

"Sicurezza, infatti, è molto più che prodotti o tecnologie, ed è questo il principio ispirativo dell'impegno dimostrato e mantenuto elevato negli anni da Cisco per la diffusione della cultura della Sicurezza in Italia."

La ricerca è disponibile al seguente indirizzo:
www.cisco.com/application/pdf/en/us/guest/netsol/ns413/c654/cdccont_0900aecd8056e783.pdf

7. INFOSECURITY ITALIA 2007

Riportiamo il programma aggiornato al 31.12.2006 dei convegni che abbiamo contribuito ad prganizzare nell'ambito di Infosecurity Milano (6-8 febbraio).

6 Febbraio Pomeriggio

IDENTITÀ DIGITALE: UNA SFIDA PER IL FUTURO

Ogni utente della rete possiede molteplici identità digitali, anche nell'ambito della stessa organizzazione. Ciò rende estremamente problematica e spesso inefficente la gestione delle identità digitali, sia per gli utenti che per gli amministratori di sistema. Il problema non è purtroppo di facile soluzione. Solo recentemente sono state messi a punto metodologie e prodotti che possono contribuire ad una soluzione radicale.

In questo convegno, alcuni rappresentanti delle Istituzioni e esperti del settore illustreranno le iniziative più significative in ambito nazionale.

Alcuni fornitori leader di mercato illustreranno alcuni esmpi reli in cui il problema è stato risolto con successo.

Nel corso del convegno si discuterà anche del problema del furto di identità digitale.

Chairman: GIGI TAGLIAPIETRA, Presidente CLUSIT

Relatori:

- GIOVANNI MANCA - Responsabile Ufficio Standard e tecnologie d'identificazione del CNIPA

L'identità digitale nell'e-government europeo

In Italia ed Europa l'e-government continua la sua evoluzione per offrire servizi ai cittadini e alle imprese. In Italia proseguono le esperienze della Carta d'Identità Elettronica e della Carta Nazionale dei Servizi per l'accesso ai servizi in rete della PA. Ma il "cittadino europeo" quante identità digitali dovrà avere ? Quale sarà la situazione nei prossimi mesi ed anni ? Quale è il futuro della ECC (European Citizen Card) ?

- LORENZO GRILLO - Country Manager VeriSign Italy

Un approccio integrato al furto di identità. L'esperienza CREDEM

L'Internet Banking ha raggiunto un alto livello di qualità e gli utenti di servizi online stanno crescendo, anche se le frodi online continuano ad aumentare. CREDEM ha seguito l'approccio integrato di VeriSign, per fornire ai clienti, durante le loro attività di online banking, un alto livello di protezione delle proprie credenziali e delle informazioni personali contro i furti di identità

- GIOVANNI ANASTASI - ICT Manager Arthis

Gestire in sicurezza l'accesso ai dati e ai sistemi IT

Sarà presentata l'esperienza di Arthis, che ha scelto la soluzione ORACLE Identity Management Suite per accrescere i propri livelli di sicurezza in termini di accesso ai dati e ai sistemi IT da parte degli utenti interni ed esterni. Arthis, fondata dal Gruppo Rinascente e da Accenture, gestisce tutte le funzioni di back office della grande distribuzione, dai servizi di account al reporting finanziario, consentendo al gruppo di aumentare l'efficienza operativa e nel contempo di operare in conformità al dlg 196/03 sulla privacy.

- DOMENICO VULPIANI - Direttore Servizio Polizia Postale e delle Comunicazioni

Il furto di identità digitale

Il furto di identità digitale è sicuramente la minaccia emergente che sta caratterizzando qust'ultimo periodo di evoluzione della rete e delle forme di attacco informatico. In questo intervento si delineeranno i contorni di questa forma di attacco rifacendosi a casi reali riscontrati a livello nazionale ed internazionale.

- CASE STUDY (in fase di definizione)
- CASE STUDY (in fase di definizione)

STORAGE/INFOSECURITY 7 Febbraio

TECNOLOGIE, NORME E STANDARD PER LA SICUREZZA DELLE INFORMAZIONI

È sempre più vasto il repertorio di norme e Standard in ambito Security che un'azienda è chiamata a soddisfare:Testo Unico sulla Privacy, Legge sulla Data Retention, Legge sul Diritto d'Autore, Legge sulla Pedofilia online, Basilea 2, norme ISO. Common Criteria, ecc.

Il corretto uso di tecnologie di Storage e di Security possono facilitare notevolmente le attività che un'azienda deve intraprendere per far fronte a tali esigenze.

Nell'ambito di questo convegno, alcuni massimi esperti in ambito legale e normativo esporranno lo stato dell'arte in materia; i fornitori leader di mercato illustreranno casi reali in cui le tecnologie hanno aiutato le aziende a raggiungere i livelli di conformità richiesti.

MATTINO

Chairman: MARCO GATTI - Direttore Responsabile WEEK.it

Relatori:

- GIOVANNI ZICCARDI - Università degli Studi di Milano
- CASE STUDY a cura di ISS
- CASE STUDY a cura di NetApp
- FRANCO GUIDA - Fondazione Ugo Bordoni - Vice-Direttore dell'Organismo di Certificazione della Sicurezza Informatica (OCSI)
- CASE STUDY a cura di ACHAB

POMERIGGIO

Chairman: GIGI BELTRAME - Responsabile ICT & tech solutions - il Sole 24 Ore

Relatori:

- ANDREA MONTI - Socio fondatore e membro del CD Clusit

Privacy, informazioni segrete in aziende e ICT: problemi e soluzioni

Lo scopo di questo intervento è fornire indicazioni chiare e concrete su come tutelare gli asset immateriali dell'impresa, nel rispetto della legge ma, sopratutto, di quello degli azionisti. Sempre piu' spesso la sicurezza ICT in azienda e' identificata con la "messa a norma" della normativa sui dati personali. In realtà la protezione degli asset immateriali dell'azienda è un argomento ben più ampio e complesso. Questo, anche per via di leggi - come il codice della proprietà industriale - tanto importanti quanto trascurate e a causa di recenti sentenze che hanno tracciato, finalmente, degli indirizzi chiari sui poteri di controllo delle imprese sull'uso delle risorse di comunicazione da parte dei dipendenti.

- CASE STUDY a cura di EMC
- CASE STUDY a cura di DELL
- PAOLO MACCARRONE - MIP School of Management del Politecnico di Milano
- CASE STUDY in fase di definizione
- CASE STUDY in fase di definizione

INFOSECURITY 8 Febbraio Mattino

LA SICUREZZA DELLE APPLICAZIONI WEB

Il web è ormai diventato l'ambito di riferimento per lo sviluppo di tutte le applicazioni di rete, quali ad esempio home banking, e-commerce, e-government, e-health, ecc. La stragrande maggioranza di tali applicazioni richiede spesso il. soddisfacimento di requisiti di sicurezza molto stringenti.

Scopo del presente convegno è illustrare le metodologie e le tecnologie oggi presenti sul mercato per la realizzazione o la messa in sicurezza di applicazioni web.

Alcuni fornitori illustreranno le tecniche utilizzate in casi concreti.

Chairman: JOY MARINO

Relatori:

- DAVE WICHERS keynote speaker

Dave Wichers is the COO and cofounder of Aspect, where he is responsible for running daily operations of the company. Prior to founding Aspect, Dave started and ran the application security practice at Exodus Communications, which provided a full suite of application security consulting services to Fortune 500 and other commercial companies starting in1998.

Dave has focused on information security during his entire career, starting in 1988. His information security background spans the entire security engineering lifecycle, including software development, system security requirements, security architectures, secure designs, security policies, models, and system testing.

He has supported the design and development of trusted operating systems, trusted databases, secure routers, multilevel secure guards, and large integrated systems for a wide variety of customers, including NSA, DoD, and Fortune 500 vendors and end customers.

Dave is a primary author of the OWASP Top 10 Web Application Security Vulnerabilities and is the OWASP Conferences Chair. He was also a primary contributor to the group responsible for creating ISO 21827, the Systems Security Engineering Capability Maturity Model (SSE-CMM).

Dave earned a B.S. summa cum laude in Computer Systems Engineering from Arizona State University and an M.S. summa cum laude in Computer Science from the University of California at Davis. Dave holds both CISSP and CISM certifications.

- CASE STUDY a cura di ONE ANS
- CASE STUDY in fase di definizione
- CASE STUDY in fase di definizione

8. SEMINARI CLUSIT 2007

È in fase di definizione il calendario 2007 dei seminari Clusit.

Segnaliamo che è in funzione un nuovo sistema che gestisce le registrazioni ai seminari Clusit online.

Registrazione

Le registrazioni ai seminari d'ora in avanti avvera' solo online, dopo essersi registrati come utente (non saranno piu' accettate le registrazioni con fax).

La registrazione sarà immediatamente confermata dopo l'invio.

La conferma di partecipazione sarà inviata la settimana precedente il seminario all'indirizzo e-mail indicato.

Prerequisiti

- Per usufruire del diritto di partecipazione gratuita ai seminari il Socio deve essere in regola con la quota sociale per l'anno in corso.
- Le Aziende associate, possono inviare un numero massimo di tre delegati per ciascun seminario.
- Per iscriversi in seguito ad un invito o ad una convenzione indicare il Codice Convenzione o Invito di 5 caratteri di cui si e' in possesso.

- Sono accettate fino a 3 iscrizioni di studenti a titolo gratuito per ogni seminario. Sarà considerato valido ai fini dell'iscrizione l'ordine d'arrivo delle registrazioni. Uno stesso studente può partecipare gratuitamente fino a 3 seminari nel corso di un anno solare. Lo studente dopo ogni registrazione deve inviare il certificato di frequenza rilasciato dall'Università per fax al numero 02.700440.496 o la scansione per email a: edu@clusit.it. In caso di mancato invio entro i 5 giorni successivi, la registrazione sarà cancellata. Non sono accettati altri tipi di documenti quale libretto, ricevute di pagamento, ecc.; *non sara' data risposta a richieste di ogni forma di deroga*.

Cancellazione

In qualunque momento è possibile cancellare la registrazione inviando un messaggio a edu@clusit.it, per dare così la possibilità di partecipare ad altri Soci.

Riprese video e/o audio

E' possibile che per alcuni seminari sia predisposta la registrazione video e/o audio allo scopo di rendere il materiale fruibile sul web o con altri mezzi di diffusione.

Su https://edu.clusit.it sono disponibili maggiori informazioni e sono aperte le iscrizioni ai primi 2 seminari, che si terranno in ambito Infosecurity Milano, nei giorni 6 e 8 febbraio.

Coloro che si iscrivono ai seminari di febbraio, possono richiedere a info@clusit.it un invito valido per l'ingresso gratuito a Infosecurity Italia.

9. NOTIZIE DAI SOCI

Una primaria Banca situata nel Veneto ricerca un Senior Security Officer per la gestione e implementazione del proprio sistema di sicurezza informatica.

Il profilo ideale è quello di un laureato in Scienze dell'Informazione (o cultura equivalente), in grado di conversare agevolmente in inglese, disponibile a brevi e frequenti trasferte in Europa, con pluriennale esperienza sulle tecnologie e metodologie sulla sicurezza IT quali: tecniche di Risk Management, webserver security, firewalls, networks, encryption, PKI. Il possesso di certificazione (CISSP-CISA-CISM) costituisce elemento preferenziale.

E' prevista l'assunzione con contratto a tempo indeterminato nel CCNL delle Aziende del Credito come Quadro Direttivo.

Chi fosse interessato può scrivere a info@clusit.it.

CLUSIT
ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA*
Dipartimento di Informatica e Comunicazione
Università degli Studi di Milano
Via Comelico 39 - 20135 MILANO - cell. 347.2319285
* associazione senza fini di lucro, costituita il 4 luglio 2000